Quantum resource-saving protocols for early quantum networks

Lipinska, V.

DOI
10.4233/uuid:0da54248-4739-4bd2-af52-08109aa37113

Publication date
2020

Document Version
Final published version

Citation (APA)
Lipinska, V. (2020). *Quantum resource-saving protocols for early quantum networks*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:0da54248-4739-4bd2-af52-08109aa37113

QUANTUM RESOURCE-SAVING PROTOCOLS FOR EARLY QUANTUM NETWORKS

QUANTUM RESOURCE-SAVING PROTOCOLS FOR EARLY QUANTUM NETWORKS

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus Prof. dr. ir. T. H. J. J. van der Hagen
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op 8 september 2020 om 12:30 uur

door

Victoria LIPINSKA

Master of Science in Theoretical Physics,
Stockholm University, Stockholm, Sweden,
geboren te Slawno, Poland.

Dit proefschrift is goedgekeurd door de

promotor: prof. dr. S. D. C. Wehner

Samenstelling promotiecommissie:

Rector Magnificus	voorzitter
Prof. dr. S. D. C. Wehner,	Technische Universiteit Delft
Onafhankelijke leden:	
Prof. dr. W. Tittel,	Technische Universiteit Delft
Prof. dr. L. M. K. Vandersypen,	Technische Universiteit Delft
Prof. dr. E. Kashefi,	Sorbonne Université
Dr. D. Elkouss Coronas,	Technische Universiteit Delft

Keywords: quantum networks, quantum internet, quantum cryptography, quantum communication, distributed quantum computation

Printed by: Gildeprint - www.gildeprint.nl

Front & Back: Luuk Platschorre

ISBN 978-94-6402-485-2

An electronic version of this dissertation is available at
http://repository.tudelft.nl/.

To my parents.

CONTENTS

SUMMARY

The Internet as we know it has had an immense impact on the way we communicate. We can now do it faster and more securely than ever before. Enabling quantum communication between any two points on Earth is the next step towards even more secure communication. This is the goal of the quantum internet. Although it is hard to predict all of the applications for the quantum internet, many protocols running on a network connecting nodes able to process qubits have already been identified. Typically, these applications require many qubits to be realized, a requirement which will not likely be met in the early quantum internet.

For this reason, in this thesis we take two main directions in investigating applications for near-term quantum internet. First, we study existing network protocols and analyze how quantum resources necessary to realize them could be scaled down, while keeping the same security requirements. What is more, we analyze the quantum resource states for certain network protocols in terms of robustness to common types of noise. Second, we design a testing protocol which provides a certificate for the quantum network to achieve a certain stage of development on the path to becoming a large-scale quantum internet.

In our first direction of study we investigate three tasks. The first of them is the task of anonymously transmitting a quantum message in a network. We present a protocol that accomplishes it using the W state and we analyze its performance in a quantum network where some form of noise is present. We then compare the performance of our protocol with other protocols developed for anonymous transmission. We show that, in many regimes, our protocol tolerates more noise and achieves higher fidelities of the transmitted quantum message than the other ones.

Next, we discuss sharing a secret quantum state in a n-node quantum network in a verifiable way. We propose a protocol that achieves this task, while reducing the number of required qubits, as compared to the existing protocols. To achieve this, we combine classical encryption of the quantum secret with an existing verifiable quantum secret sharing scheme based on quantum error correcting codes. In this way we obtain a verifiable hybrid secret sharing scheme for sharing qubits, which combines the benefits of quantum and classical schemes. Moreover, for sharing a one-qubit state, each node needs a quantum memory to store n single-qubit shares, and requires a workspace of at most $3n$ qubits in total to verify the quantum secret. Importantly, in our scheme an individual share is encoded in a single qubit, as opposed to previous schemes requiring $\Omega(\log n)$ qubits per share.

What is more, we consider the task of secure multi-party distributed quantum computation on a quantum network. We propose a protocol based on quantum error correction which reduces the number of necessary qubits, as compared to the prior approach. In our protocol each of the n nodes requires an operational workspace of n^2+4n qubits. To achieve universal computation, we develop a distributed procedure for veri-

fying magic states, which allows us to apply distributed gate teleportation. We showcase our protocol on a small example for a 7-node quantum network.

Finally, in the second direction of study, we test the ability of quantum network nodes to execute multi-round quantum protocols. Specifically, we examine protocols in which the nodes are capable of performing quantum gates, storing qubits and exchanging the said qubits over the network a certain number of times. We propose a simple ping-pong test, which provides a certificate for the capability of the nodes to run certain multi-round protocols. We first show that in the noise-free regime the only way the nodes can pass the test is if they do indeed possess the desired capabilities. We then proceed with considering the case where operations are noisy, and provide an initial analysis showing how our test can be used to estimate parameters that allow us to draw conclusions about the actual performance of such protocols on the tested nodes.

SAMENVATTING

Het internet zoals we het kennen, heeft een enorme impact gehad op de manier waarop we communiceren. We kunnen nu sneller en veiliger communiceren dan ooit tevoren. Het mogelijk maken van kwantumcommunicatie tussen twee willekeurige punten op aarde is de volgende stap naar nog veiligere communicatie. Dit is het doel van het kwantuminternet. Hoewel het moeilijk is om alle toepassingen voor het kwantuminternet te voorspellen, zijn er al veel protocollen bekend die draaien op een netwerk van partijen die kwantumbits kunnen verwerken en uitwisselen. Meestal vereisen deze toepassingen echter dat veel kwantumbits beschikbaar zijn, een vereiste waaraan waarschijnlijk niet zal worden voldaan in het vroegtijdige kwantuminternet.

Om deze reden onderscheiden we in dit proefschrift twee hoofdlijnen in het onderzoek naar toepassingen voor het kwantuminternet op de korte termijn. Ten eerste bestuderen we bestaande netwerkprotocollen en analyseren we hoe de kwantumresources die nodig zijn om ze te realiseren, kunnen worden verkleind met behoud van de beveiligingsvereisten. Bovendien analyseren we de kwantumtoestanden die nodig zijn voor bepaalde netwerkprotocollen in termen van robuustheid tegen veelvoorkomende soorten ruis. Ten tweede ontwerpen we een testprotocol dat een certificaat levert dat een kwantumnetwerk een bepaalde ontwikkelingsfase heeft bereikt op weg naar een grootschalig kwantuminternet.

In onze eerste hoofdlijn onderzoeken we drie verschillende taken op een kwantumnetwerk. De eerste is het anoniem versturen van een kwantumbericht in een netwerk (anonieme transmissie - anonymous transmission). We presenteren een protocol dat deze taak volbrengt met behulp van de W-toestand en we analyseren de prestaties hiervan in een kwantumnetwerk waar enige vorm van ruis aanwezig is. Vervolgens vergelijken we de prestaties van ons protocol met andere protocollen die zijn ontwikkeld voor anonieme transmissie. We laten zien dat ons protocol in veel regimes meer ruis tolereert en dat het ontvangen kwantumbericht een betere kwaliteit (fidelity) heeft dan in andere protocollen.

Vervolgens bespreken we het op een verifieerbare manier delen van een geheime kwantumtoestand in een kwantumnetwerk met n partijen (verifieerbare kwantumgeheimdeling - verifiable quantum secret sharing). We presenteren een protocol voor deze taak waarin het aantal benodigde kwantumbits wordt verminderd ten opzichte van de bestaande protocollen. Om dit te bereiken combineren we klassieke versleuteling van het kwantumgeheim met een bestaand protocol voor verifieerbare kwantumgeheimdeling gebaseerd op kwantumfoutcorrectiecodes. Op deze manier verkrijgen we een hybride protocol voor het delen van kwantumbits dat de voordelen van de kwantum- en klassieke protocollen combineert. Voor het delen van een geheim van één kwantumbit, heeft elke partij bovendien slechts n kwantumbits aan geheugen nodig om zijn n aandelen van het geheim op te slaan en nog eens maximaal $3n$ extra kwantumbits om het geheim te verifiëren. Belangrijk is dat in ons schema een individueel aandeel is gecodeerd

in een enkele kwantumbit, in tegenstelling tot eerdere schema's die $\Omega(\log n)$ kwantumbits per aandeel gebruiken.

Daarnaast beschouwen we de taak van het veilig uitvoeren van een kwantumberekening met meerdere partijen in een kwantumnetwerk (veilige meerpartijen-kwantumberekening - secure multi-party quantum computation). We presenteren een protocol op basis van kwantumfoutcorrectie waarin het aantal benodigde kwantumbits minder is dan in eerdere protocollen. In ons protocol heeft elk van de n partijen slechts een operationele werkruimte van $n^2 + 4n$ kwantumbits nodig. Om te zorgen dat universele kwantumberekeningen mogelijk zijn, ontwikkelen we een gedistribueerde procedure voor het verifiëren van magische toestanden. Daardoor kunnen we gedistribueerde versie van circuit teleportatie toepassen. We demonstreren ons protocol op een klein voorbeeld netwerk met 7 partijen.

Ten slotte testen we in de tweede hoofdlijn van ons onderzoek het vermogen van kwantumnetwerken om kwantumprotocollen van meerdere communicatierondes uit te voeren. We onderzoeken in het bijzonder protocollen waarin de partijen lokaal kwantumoperaties kunnen uitvoeren, kwantumbits kunnen opslaan en de kwantumbits een bepaald aantal keren via het netwerk kunnen uitwisselen. We stellen een eenvoudige pingpongtest voor om te certificeren dat de partijen in het netwerk de capaciteit hebben om bepaalde protocollen van meerdere rondes uit te voeren. We laten eerst zien dat de test in het ruisvrije regime alleen succes geeft als de partijen inderdaad de gewenste capaciteiten hebben. Daarna bekijken we het geval waarin de kwantumoperaties imperfect zijn en geven we een eerste analyse die laat zien hoe onze test kan worden gebruikt om parameters te schatten die iets zeggen over de daadwerkelijke prestaties van dergelijke protocollen op het geteste netwerk.

1

INTRODUCTION

This is an introductory chapter meant to provide a high-level overview and motivation for this thesis. We discuss two directions we take in the thesis: first, reducing quantum resources necessary to realize tasks on a quantum network and second, certification of an aptitude of a quantum network. We also present chapter-by-chapter overview of the contents of this thesis.

1

At the moment of writing this it is 2020, which means I have been studying quantum information for 8 years now. Although, in the early 2010s I could still hear a question "quantum what?" asked with a hint of condescension, I am happy to report that there is a lot more quantum awareness in the mind of the general public. And as much as I love "quantum" being a synonym for "magic", I am also very positively surprised when I find out people heard about qubits or superposition, be it from YouTube or a newspaper.

Most of the online pop-science sources talk about how quantum computers can help us solve problems which are unattainable for a classical computer, for example simulating molecules. This thesis won't be about that. Some other sources talk about how quantum computers can break the encryption schemes we use today when we browse the internet. This thesis won't be about that either. In fact, it will not talk about quantum computers at all. Instead, it will consider a domain of quantum science which remains a bit misunderstood, that is *quantum communication*. In quantum communication we use quantum technology to communicate with each other. The information that is sent, instead of regular 0 and 1 bits, can also be quantum – we will send quantum bits or "qubits". In this thesis I will talk about what can we do when we have just a few of these qubits available, and what happens when there are some bad guys around. Hopefully, by the time we are done, I will have convinced you why we should do this and why it makes sense at all.

If you are holding this thesis, dear reader, it means that you are somewhat interested in quantum technology (or you are in my thesis committee). In this chapter I will try my best to give you a general and somewhat subjective overview of the state-of-the-art on quantum networks. I will also refer to myself as "we". I promise it will make sense in the following chapters where I would like to credit my excellent co-authors for the effort they put in in our collective work. However, in this introductory chapter, please, bear with us.

1.1. APPLICATIONS FOR NEAR-TERM QUANTUM INTERNET

It is not much of a stretch to say that the internet revolutionized the way we communicate. It enables any two points on Earth to send messages faster and more securely than ever before. To take this a step further would be to enable quantum communication between any two points. This is exactly the vision of the so called *quantum internet*. We disclaim here that the quantum internet is not meant to work as an individual entity or replace the internet we have today. On the contrary, it is meant to support and enhance the "classical" internet, achieving even more secure communication and enabling tasks impossible to achieve in the regular internet.

In a quantum internet we envision connecting small quantum processors, i.e. processors which are able to control a few qubits, in a network. We will refer to such processors as *end nodes* or simply *nodes* [1]. This is, however, not just a theoretical consideration anymore. At QuTech we collectively work towards a real-life demonstration of a quantum internet, which might become world's first.

It is quite a challenge to anticipate all future use cases of the quantum internet, which is the case with any entirely new technology. However, many major applications have already been identified, including secure communication, extending baseline of telescopes [2], clocks synchronization [3], anonymous transmission [4], position verification [5, 6] and quantum computation on a remote server [7]. Perhaps the most famous

application is the quantum key distribution, often referred to as QKD [8, 9]. Its task is to distribute a key between two nodes of a network in a completely secure way, such that an eavesdropper can always be detected. It is also the application which received the most attention from the community. Many variants of QKD have been considered so far, with [9] and without entanglement [8], with [8, 9] and without [10–12] trusted devices and thus achieving weaker or stronger versions of security. Many variants were also demonstrated experimentally [13–15] and many major conferences discuss QKD in great depth.

As much as it may seem that way, QKD is not a synonym for quantum cryptography. However, other cryptographic applications for the quantum internet which we listed before, were mostly analyzed in the context of a theoretical concept, we might even say briefly compared to QKD. On the other hand, near-term quantum networks will likely have limited quantum resources, being able to control up to a few qubits. This opens up a possibility for a new direction in quantum cryptography: What other applications can we realize on a small quantum internet, while using as few qubits as possible and achieving comparable security guarantees? This is the first direction we will take in this thesis. We will analyze a few quantum protocols beyond quantum key distribution in the context of quantum resource reduction. We will see that some tasks can be achieved using far less qubits than what was known before, at the same time keeping the security guarantees.

1.2. TESTING QUANTUM NETWORKS

We can define stages of development of a quantum internet, depending on the difficulty and technological complexity of the application we wish to run. Ref. [1] identifies those stages and unifies the framework for future development. For example, if an application only requires preparing single-qubit states, sending them and measuring right after, it will define an early stage of development. This is because preparing and measuring single qubits is relatively "easy". For comparison, if an application requires simultaneous control over multiple qubits, multi-qubit operations and long-time storage of said qubits, it defines an advanced stage of development. Generally speaking, controlling and storing qubits at the same time is way "harder" than just sending them one by one.

A naive way to say that a quantum internet achieved a certain stage of development would be to try to run all of the applications within that stage. This solution quickly becomes intractable. First of all, it requires a lot of resources and time to run all of the applications. Second of all, we are not even sure whether applications we know today are *all* of the applications potentially in that stage (most likely, they are not). Finally, it does not give us a measure of how well the quantum internet performs at a particular stage. For this reason, it is important to come up with a certification procedure which would measure a general aptitude of a quantum network for realizing certain tasks. In the second part of this thesis we take the first step towards that. We define a certification protocol verifying that a quantum network achieved a *quantum memory network* stage of development. That means, that each node is able locally manipulate a few qubits and store them for time long enough to account for communication delays in the network.

1

1.3. CHAPTER OVERVIEW

This thesis consists of 7 chapters. The first two chapters, including this one, serve as an overview and set the framework for the rest of the thesis. The following chapters consist of original work: Chapters 3, 4 and 5 talk about reducing quantum resources in applications for a near-term quantum internet. In chapter 6 we certify that a quantum internet achieves a certain stage of development.

In **Chapter 2** we provide mathematical preliminaries, set the notation and explain terminology commonly used in quantum cryptography which we will employ throughout the rest of this thesis. In **Chapter 3** we consider quantum anonymous transmission and present a protocol that accomplishes this task using a different resource state than what is known to date. In a quantum network where noise is present, we analyze its performance and then compare it with other protocols developed for the task. In **Chapter 4** we discuss sharing a secret quantum state in a quantum network in a verifiable way. We propose a protocol that achieves this task, while reducing the number of required qubits, as compared to the prior protocols. Our solution combines an existing verifiable quantum secret sharing scheme with classical encryption of the secret state. In this way we obtain a verifiable hybrid secret sharing scheme for sharing qubits. In **Chapter 5** we study the task of secure multi-party distributed quantum computation on a quantum network. We propose a protocol which reduces the number of necessary qubits, as compared to the existing approach. This makes our protocol suited for near-term quantum networks. We also showcase our protocol on a small example for a 7-node network. In **Chapter 6** we consider testing the ability of quantum network nodes to execute protocols in which the nodes are capable of performing quantum gates, storing qubits and exchanging the said qubits over the network a certain number of times. We propose a simple ping-pong test, which provides a certificate for the capability of the nodes to run such protocols. Finally, in **Chapter 7** we provide conclusions for the entire thesis.

REFERENCES

[1] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead,* Science **362** (2018), 10.1126/science.aam9288.

[2] D. Gottesman, T. Jennewein, and S. Croke, *Longer-baseline telescopes using quantum repeaters,* Physical Review Letters **109** (2012), 10.1103/physrevlett.109.070503.

[3] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, *Quantum clock synchronization based on shared prior entanglement,* Physical Review Letters **85**, 2010 (2000).

[4] M. Christandl and S. Wehner, *Quantum anonymous transmissions,* in *Advances in Cryptology - ASIACRYPT 2005*, edited by B. Roy (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 217–235.

[5] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, *Position-based quantum cryptography: Impossibility and constructions,* SIAM Journal on Computing **43**, 150 (2014).

[6] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, *Position-based quantum cryptography,* (2010).

[7] J. F. Fitzsimons, *Private quantum computation: an introduction to blind quantum computing and related protocols,* npj Quantum Information **3** (2017), 10.1038/s41534-017-0025-3.

[8] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[9] A. K. Ekert, *Quantum cryptography based on bell's theorem,* Phys. Rev. Lett. **67**, 661 (1991).

[10] D. Mayers and A. Yao, *Quantum cryptography with imperfect apparatus,* in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)* (IEEE Comput. Soc, 1998).

[11] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *Device-independent quantum key distribution secure against collective attacks,* New Journal of Physics **11**, 045021 (2009).

[12] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical device-independent quantum cryptography via entropy accumulation,* Nature Communications **9** (2018), 10.1038/s41467-017-02307-4.

[13] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, *Long-distance quantum key distribution in optical fibre,* New Journal of Physics **8**, 193 (2006).

[14] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Provably secure and practical quantum key distribution over 307 km of optical fibre,* Nature Photonics **9**, 163 (2015).

[15] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, *Satellite-relayed intercontinental quantum network,* Physical Review Letters **120** (2018), 10.1103/physrevlett.120.030501.

2

PRELIMINARIES

In this chapter we discuss useful notions from quantum mechanics and quantum information theory. Specifically, we talk about quantum states and measurements, quantum operations and measures of quality whenever some form of noise is present. We also review the language used in quantum cryptography. This chapter is by no means exhaustive. Its purpose is to serve as an overview of different aspects of quantum information we will put together in the following chapters.

In this chapter we introduce the basic definitions, notation and formalism which will be useful in the following chapters. We assume that the reader is already familiar with the basic notions of linear algebra and probability theory. The concepts discussed here are merely an overview. For a much more comprehensive and didactic introduction to quantum information theory we refer the reader to the famous book of Nielsen and Chuang [1], or to much more mathematically detailed book by Watrous [2]. We start, in Section 2.1 with defining quantum states and measurements, and consequently, a probability of obtaining a certain measurement outcome upon measuring a quantum state. In Section 2.2 we discuss quantum gates and channels and look at useful properties of Pauli and Clifford groups. In Section 2.3 we consider how to quantify the quality of quantum states and operations in the case when some sort of noise is present in the quantum system. Finally, in Section 2.4 we introduce some basic notions of quantum cryptography, which will be particularly useful throughout this thesis. We recommend that a reader already familiar with these definitions skips this chapter and resumes reading in Chapter 3.

2.1. QUANTUM STATES AND MEASUREMENTS

2.1.1. QUANTUM STATES

Pure states. Consider a quantum system, described in terms of a complete complex vector space with a Hermitian inner product, i.e. the Hilbert space $\mathscr{H}$. The first postulate of quantum mechanics states that the state of a qauntum system is completely specified by its state vector in a Hilbert space. This vector is commonly denoted as $|\psi\rangle$ and called a *ket*. Its complex conjugate $\langle\psi| = (|\psi\rangle)^\dagger$ is called a *bra*. Although, in principle, in quantum mechanics such spaces can be treated as infinite-dimensional, in this thesis we will restrict ourselves to finite-dimensional cases with dimension d. The simplest quantum system exists for $d = 2$ and determines a physical quantum bit or a *qubit*. One can identify it with a two-level quantum system, such as the polarization of a photon, presence and absence of a photon, the spin of an electron or an atom with a ground and excited state.

Formally, we write the qubit state as

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle , \tag{2.1}$$

where $\{|0\rangle , |1\rangle\}$ form an orthonormal basis for the Hilbert space $\mathscr{H}$ (sometimes called the "standard" or "computational" basis), and α_0 and α_1 are complex numbers. The choice of basis is completely arbitrary and a qubit can be represented in any basis. Moreover, a state vector is a unit vector and therefore, the normalization condition $\langle\psi\rangle = 1$ implies that $|\alpha_0|^2 + |\alpha_1|^2 = 1$. In principle, one can define quantum states with $d > 2$. Quantum states that can be written in a form of a vector, for example (2.1), are referred to as *pure*.

Mixed states. More generally, one can also consider a statistical mixture of pure states, which we refer to as *mixed* states. This is particularly useful if one does not have the full knowledge about the quantum state: suppose a quantum system is in one of the possible states $\{|\psi_i\rangle\}$ with some probability $p_i \geq 0$, $\sum_i p_i = 1$. Then we call the set $\{p_i, |\psi_i\rangle\}$ an

ensemble, which defines a density matrix of the quantum state,

$$\rho = \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|. \tag{2.2}$$

Every density matrix ρ must *(i)* be positive semi-definite and *(ii)* have the trace equal to one, $\mathrm{tr}\{\rho\} = 1$. Finally, note that every state that is not pure is a mixed state.

Composite systems. To describe a combined system of two or more physical systems one uses the tensor product of the state spaces of each of the physical systems. In other words, the representation space of the system composed of n qubits is a tensor product individual Hilbert spaces, $\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \cdots \otimes \mathscr{H}_n$. Whether two or more qubits are entangled is determined by whether their joint state ρ can be written as a convex combination of tensor products. That is, whenever a state of n qubits cannot be written as

$$\rho \neq \sum_{i_1,\ldots,i_n} p_{i_1,\ldots,i_n} \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}, \tag{2.3}$$

we call it *entangled* and otherwise it is separable.

2.1.2. MEASUREMENTS AND PROBABILITIES

The measurement problem in quantum mechanics is quite a controversial topic. Many notions have been introduced, depending on the interpretation of quantum mechanics [3]. We will follow the commonly accepted interpretation where a measurement is a process with an intrinsically random outcome subject to given probabilities.

A postulate of quantum mechanics states that quantum measurements are characterized by a collection of measurement operators $\{M_m\}$, which act on the Hilbert space $\mathscr{H}$ of the measured system. By m we denote the measurement outcome, which assumes a real value. Let the measured system be in a state ρ before performing the measurement. In this case, the probability that the outcome m occurs, according to Born rule is expressed as

$$p(m) = \mathrm{tr}\big[M_m \rho\big], \tag{2.4}$$

where we have that $p_m \geq 0$ and $\sum_m p_m = 1$. From this we get two conditions that any measurement needs to satisfy: $M_m \geq 0$ (positivity) and $\sum_m M_m = \mathbb{1}$ (completeness). The above conditions describe general quantum measurements called positive operator-valued measurements (POVM). This measurement, although very useful in many applications, will not be our concern here. Instead, we will use a so called *projective* measurement, which additionally satisfies the orthonormality condition, $M_m M_n = \delta_{mn} M_m$.

2.2. QUANTUM OPERATIONS

A quantum state can be subject to changes. On an elementary level, the simplest change (rotation of a qubit) can be described with a unitary operation, also called a quantum gate. We discuss this in Section 2.2.1. We also discuss more general changes to the quantum state described by quantum channels, see Section 2.2.2.

2.2.1. QUANTUM GATES

The way that one pure quantum state changes into another pure quantum state is described with a unitary operation U. In the quantum computing domain these are often called quantum gates, or just gates. Importantly, these unitary operations are linear and preserve the inner product between states. That is, given two states $|\psi\rangle_1$ and $|\psi_2\rangle$, we have that $\langle\psi_1|U^\dagger U|\psi_2\rangle = \langle\psi_1\rangle\psi_2$, from which it follows that $U^\dagger U = \mathbb{1}$. Here $U^\dagger$ denotes the hermitian conjugate of U. What is more, if U and V are both unitary then their composition UV is also a unitary. A unitary operation can also be applied to the mixed state which we write as $U\rho U^\dagger = \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger$, where we use Equation (2.2) defining mixed states. In particular, from this equation we see that unitary transformations preserve the probabilities associated with pure states in the mixed state. Some of the most common examples of quantum gates are:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.5}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, \tag{2.6}$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.7}$$

Pauli and Clifford group. As stated before, the set of unitaries has a notion of inverse, $U^\dagger U = \mathbb{1}$, and it is closed under composition. In fact, the set of unitaries forms a group. Some of the gates stated above form subgroups of the unitary group with useful properties. We define two of those subgroups below.

Definition 1 (Pauli group)**.** The Pauli group P_1 on one qubit is a 16-element subgroup of the unitary group, generated by the 2×2 identity matrix $\mathbb{1}$ and all of the Pauli matrices X, Y, Z, i.e.

$$\mathsf{P}_1 = \langle X, Z, i\mathbb{1}\rangle, \tag{2.8}$$

where $\langle\cdot\rangle$ denotes a set of the group generators. Similarly, the n-qubit Pauli group P_n consists of all n-fold tensor products of n elements of P_1.

Definition 2 (Clifford group)**.** The n-qubit Clifford group Cliff_n is a subgroup of the unitary group generated by H, P and CNOT gates,

$$\mathsf{Cliff}_n = \langle i\mathbb{1}, H_i, P_j, CNOT_{kl} : \quad i, j, k, l \in [1, n], k \neq l\rangle, \tag{2.9}$$

where H_i denotes a Hadamard gate on the i-th position in the n-element Clifford string.

The Pauli group and the Clifford group are closely related. In fact, any Clifford gate maps an element of the Pauli group to an element of the Pauli group under conjugation. This is an equivalent definition of the Clifford group, however formally, it requires more involved structures from algebra. We refer an interested reader to [4] for a more comprehensive overview.

2.2.2. CHANNELS

So far we discussed the changes to the quantum state when subjected to a unitary operation. As we saw, unitary operations preserve the probabilities in mixed states. What if, however, we had an interaction which changes those probabilities? In this case, one can describe the changes made to the quantum state with a quantum channel. More specifically, quantum channels map linear operators (for example density operators) to linear operators acting on some Hilbert space. For this reason, they are sometimes called "superoperators", since they are operators acting on linear operators. Additionally, we would like that when a quantum channel acts on a quantum state, it transforms it into another valid quantum state. Quantum channels are formally described with a completely positive trace preserving (CPTP) maps, which we define below.

Definition 3 (Quantum channel)**.** A quantum channel is a completely positive trace preserving linear map Λ transforming linear operators in $\mathscr{L}(\mathscr{H}_{\mathscr{A}})$ acting on the Hilbert space $\mathscr{H}_A$, to linear operators in $\mathscr{L}(\mathscr{H}_{\mathscr{A}'})$ acting on the Hilbert space $\mathscr{H}_{A'}$,

$$\Lambda_{A\to A'} : \mathscr{L}(\mathscr{H}_A) \to \mathscr{L}(\mathscr{H}_{A'}), \tag{2.10}$$

with the following properties:

1. (trace preserving) $\forall\ \rho \in \mathscr{L}(\mathscr{H}_A):\quad \mathrm{tr}\big[\Lambda_{A\to A'}(\rho)\big] = \mathrm{tr}\big[\rho\big]$.
2. (completely positive) $\forall\ \rho \in \mathscr{L}(\mathscr{H}_A \otimes \mathscr{H}_B), \rho \geq 0:\quad \Lambda_{A\to A'} \otimes \mathbb{1}_{B\to B'}(\rho) \geq 0$

Property 1 guarantees that quantum states are normalized after the action of the channel, and property 2 guarantees that if the channel is applied on a part of a larger system it outputs a quantum state whose eigenvalues can still be interpreted as probabilities. To wrap up the considerations about channels, let us give two examples of quantum channels, which we will be using throughout this thesis.

Depolarizing channel. The depolarizing channel, parametrized with parameter $p \in [0,1]$ acts as follows on a single-qubit state ρ,

$$\Lambda_p(\rho) = p\rho + (1-p)\frac{\mathbb{1}}{2}. \tag{2.11}$$

This means that with probability p the input state remains unchanged and with probability $(1-p)$ it is substituted for a maximally mixed state, and therefore erases all the information about the quantum state. For this reason, the depolarizing channel is often viewed as the worst case scenario for a noise on a quantum state.

Dephasing channel. The dephasing channel is a special case of the depolarizing channel, where the depolarization happens in only one basis, for example the Z basis,

$$\Lambda_p(\rho) = p\rho + (1-p)Z\rho Z. \tag{2.12}$$

Therefore, with probability $p \in [0,1]$ the state remains unchanged and with probability $1-p$ the state is affected by the noise in the Z basis.

2.3. MEASURES OF QUALITY

In this section we will discuss how to measure "closeness" of two quantum states. That is, how to quantify the quality of a quantum state when we aim to produce ρ_{ideal} but in a physical process we produce ρ_{real}.

2.3.1. TRACE DISTANCE

Intuitively, we would like that if two states ρ_{ideal} and ρ_{real} are nearly indistinguishable, then the probability of guessing which of the states is which should be really close to a random guess. We will now see how to make this intuition concrete.

Suppose that we are given ρ_{ideal} and ρ_{real}. Without any additional knowledge about the states, our best guess to tell them apart is 50-50. We may however, measure the states to improve our odds. Let the measurement operators be denoted with M_{real} and M_{ideal}, such that $M_{ideal} = \mathbb{1} - M_{real}$. Then our probability of successfully identifying the states is,

$$p_{succ} = \frac{1}{2}\operatorname{tr}\left[M_{ideal}\rho_{ideal}\right] + \frac{1}{2}\operatorname{tr}\left[M_{real}\rho_{real}\right] = \frac{1}{2} + \frac{1}{2}\operatorname{tr}\left[M_{real}(\rho_{real} - \rho_{ideal})\right]. \quad (2.13)$$

We can of course optimize over the measurements picking the best possible one, such that

$$p_{succ}^{max} = \frac{1}{2} + \frac{1}{2}\max_{0\leq M\leq\mathbb{1}} \operatorname{tr}\left[M(\rho_{real} - \rho_{ideal})\right]. \quad (2.14)$$

This operational meaning of distinguishing two quantum states is precisely captured by the so called trace distance.

Definition 4 (Trace distance)**.** We define the trace distance between two states ρ_{ideal} and ρ_{real}, as

$$D(\rho_{ideal}, \rho_{real}) = \max_{0\leq M\leq\mathbb{1}} \operatorname{tr}\left[M(\rho_{real} - \rho_{ideal})\right]. \quad (2.15)$$

2.3.2. FIDELITY

While trace distance is a nice theoretical tool, particularly used in cryptographic proofs, there exists another measure of quality of two states, which has a more practical meaning. We will see that it is related to the inner product of the states.

Definition 5. We define fidelity between two quantum states ρ_1 and ρ_2 as

$$F(\rho_1, \rho_2) = \operatorname{tr}\left[\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right]^2. \quad (2.16)$$

In particular, when one of the states is pure $\rho_1 = |\psi_1\rangle\langle\psi_1|$ the fidelity has the form $F(|\psi_1\rangle, \rho_2) = \langle\psi_1|\rho_2|\psi_1\rangle$. When both of the states are pure then the fidelity is exactly the inner product between them, $F(|\psi_1\rangle, |\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|^2$.

Often it is also useful to define the so called average fidelity $\bar{F}$, where we average the "regular" fidelity, Definition 5, over the space of all states. As such, the average fidelity quantifies how close a channel Λ acting on a quantum state is to the identity channel $\mathbb{1}$.

Definition 6 (Average fidelity)**.** The average fidelity of the channel Λ (to $\mathbb{1}$) acting on a pure state $|\psi\rangle$ is defined as

$$\bar{F} = \int \mathrm{d}\psi \, \mathrm{tr}\left[\Lambda\left(|\psi\rangle\langle\psi|\right)|\psi\rangle\langle\psi|\right] \tag{2.17}$$

where $\mathrm{d}\psi$ is the Haar measure on pure states.

2.4. QUANTUM CRYPTOGRAPHY

In this section we review terminology commonly used in the realm of quantum cryptography that will be relevant throughout this thesis. We also list the assumptions that we will put on our quantum network in order to realize useful applications.

2.4.1. TERMINOLOGY AND ADVERSARY

Throughout this thesis we consider protocols that take place between multiple participants. Since our protocols are presented in the context of a quantum network, every participant of a protocol is an end *node* of the network, possibly with a small quantum processor. Usually, we will say that n denotes the number of nodes in the network. All nodes have also access to a classical computer which can perfectly perform classical computation. This is a somewhat simplifying assumption, albeit well justified, since current classical computers are far more reliable than their quantum counterparts.

Each node can input both quantum and classical data into a protocol. We call this input *private* if no other node knows anything about the input. For comparison we talk about a *public* data if every node has full knowledge about it.

When the nodes follow the set of instructions defined by a protocol exactly, then we say that they act *honestly*. However, not all of the nodes need to act honestly. Notably, if it was the case, there would be no need for cryptography in the first place. Those nodes who try to gain additional information about the data in the protocol by, for example, following an arbitrary set of instructions, are called *cheaters*. They are allowed to collaborate with one another. It is very common to consider that the cheaters are controlled by an entity outside of the protocol, called *adversary*. This makes it easier to consider possible malicious strategies when designing a security proof. If the set of cheaters is determined at the beginning of the protocol and stays fixed throughout its execution, we talk about a *non-adaptive* adversary.

We can further classify the cheaters, depending on what they aim to achieve. When the cheaters follow the protocol honestly, but only collect and store all the information available throughout the protocol, we call them *passive* (sometimes also "honest-but-curious") cheaters. Passive cheaters can collaborate to use the collected classical data in order to learn as much about other nodes as possible, without disrupting the execution of the protocol. On the other hand, if the cheaters can perform arbitrary joint quantum operations on their collective state during the execution of the protocol and have unlimited quantum resources (so called *quantum side information*), then we talk about *active* cheaters. This is the most malicious type of cheaters one can consider. One can also define an intermediate stage, where the cheaters are active, but some elements of the protocol, for example the resource state preparation, is trusted. In this case we

talk about *semi-active* cheaters, see Chapter 3 for details. We say that a protocol *tolerates* cheaters if at the end of the protocol an outcome can be determined despite of the presence of the cheaters.

2.4.2. ASSUMPTIONS ON THE QUANTUM NETWORK

Our concern is to design and analyze protocols for small quantum networks. For this reason we assume that a quantum network operates together with an underlying classical network. We will follow a common assumption that classical computation can be performed with subroutines that work perfectly. In each chapter we make this assumption more specific, depending on the protocol we consider.

Importantly, we consider that each pair of nodes is connected via private and authenticated classical channels [5]. This assumption allows us to reliably transmit classical information without worrying about additional security claims. Additionally, we assume that the nodes have access to an authenticated classical broadcast channel [6] and a public source of randomness. The latter can be realized, for example, by running a classical verifiable secret sharing protocol or multi-partite coin flipping [7]. Last, throughout this thesis we will often talk about information-theoretical security, which means that a protocol remains secure even if the adversary is given unlimited (quantum) computational power. For comparison, there also exists the notion of computational security which means that the security achieved relies on assumptions about computational complexity of a particular problem.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, USA, 2011).

[2] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[3] M. Schlosshauer, *Decoherence, the measurement problem, and interpretations of quantum mechanics,* Reviews of Modern Physics **76**, 1267 (2005).

[4] D. Gottesman, *Stabilizer codes and quantum error correction,* (1997).

[5] R. Canetti, *Universally composable signature, certification, and authentication,* in *Proceedings. 17th IEEE Computer Security Foundations Workshop, 2004.* (2004) pp. 219–233.

[6] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, *Multicast security: a taxonomy and some efficient constructions,* in *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, Vol. 2 (1999) pp. 708–716 vol.2.

[7] T. Rabin and M. Ben-Or, *Verifiable secret sharing and multiparty protocols with honest majority,* in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89 (ACM, New York, NY, USA, 1989) pp. 73–85.

3

ANONYMOUS TRANSMISSION WITH THE W STATE

We consider the task of anonymously transmitting a quantum message in a network. We present a protocol that accomplishes this task using the W state and we analyze its performance in a quantum network where some form of noise is present. We then compare the performance of our protocol with some of the existing protocols developed for the task of anonymous transmission. We show that, in many regimes, our protocol tolerates more noise and achieves higher fidelities of the transmitted quantum message than the other ones. Furthermore, we demonstrate that our protocol tolerates one nonresponsive node. We prove the security of our protocol in a semiactive adversary scenario, meaning that we consider an active adversary and a trusted source.

This chapter has been published, with minor changes, in V. Lipinska, G. Murta, and S. Wehner, *Anonymous transmission in a noisy quantum network using the W state*, Phys. Rev. A 98, 052320 (2018).

3.1. INTRODUCTION

In cryptographic scenarios we are often concerned with hiding the content of the messages being exchanged. However, sometimes the identity of the parties who communicate may also carry relevant information. Examples of tasks where the identities of the ones who communicate carry crucial information are voting, electronic auctions [1] or, more practically, sending a message to a secret beloved [2]. Therefore, the establishment of anonymous links in a network, where identities of connected parties remain secret, is an important primitive for both classical [**?**] and quantum communication.

In this chapter we consider a task of anonymously transmitting a quantum message in a network. To define the task more precisely, consider a quantum network with N nodes. One of the nodes, sender S, would like to communicate a quantum state $|\psi\rangle$ to a receiver R in a way that their identities remain completely hidden throughout the protocol. In particular, for S it implies that her identity remains unknown to all the other parties, whereas for R it implies that no one except S knows her identity. The essence of the protocol is to create an entangled link between S and R by performing local operations on the other nodes of the network. Such a link is called *anonymous entanglement* (AE) [3], since the identities of the nodes holding the shares of the entangled pair is kept anonymous. After anonymous entanglement is created, S and R use it as a resource for teleporting the quantum information $|\psi\rangle$. Note that the main goal of anonymous transmission is to fully hide the identities of the sender and the receiver; it does not aim at guaranteeing the reliability of the transmitted message.

A number of protocols have been proposed to tackle this task, which was first introduced in [3]. There, the authors present a protocol which makes use of a given multipartite Greenberger-Horne-Zeilinger (GHZ) state as a quantum resource, i.e., $|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\ldots0\rangle + |1\ldots1\rangle)$. The problem was subsequently developed to consider the preparation and certification of the GHZ state [4, 5]. In [5], it was first shown that the proposed protocol is information-theoretically secure against an active adversary. What is more, other protocols were proposed, which do not make use of multipartite entanglement, but utilize solely Bell pairs to create anonymous entanglement [6]. Yet, so far, it has not been discussed whether multipartite states other than the GHZ allow for anonymous transmission of a quantum state. Moreover, nothing is known about the performance of such protocols in a realistic quantum network, where one inevitably encounters different forms of noise.

Here we design a protocol for quantum anonymous transmissions which uses the W state, $|\mathrm{W}\rangle_N = \frac{1}{\sqrt{N}}(|10\ldots0\rangle + \cdots + |0\ldots01\rangle)$. Just like other existing protocols, our protocol is based on establishing anonymous entanglement between S and R. We prove the security of our protocol in a semiactive adversary scenario, meaning that we consider an active adversary and a trusted source, as in [3]. We also show that security is preserved in the presence of noise in the network, when all the particles are subjected to the same type of noise. What is more, we compare the performance of our protocol with previously proposed protocols that use the GHZ state and Bell pairs. We quantify the performance of protocols by the fidelity of the transmitted quantum state. We find that, in many cases, our W-state based protocol tolerates more noise than the other protocols and achieves higher fidelity of the transmitted state. Additionally, we show that our protocol can tolerate one nonresponsive node, e.g., if one of the qubits of a multipartite

state gets lost. In contrast, the protocol using the GHZ state cannot be carried out at all in this case, since the loss of a single qubit destroys the entanglement of the state. We also address the performance of the Bell-pair based protocol, presented in [6], and we show that in the presence of noise, the performance of the protocol depends on the ordering of S and R in the network. To the best of our knowledge this is the first analysis of anonymous transmission in the presence of noise. Without such an analysis the performance of near-future applications for quantum networks cannot be characterized [7].

The chapter is organized as follows. In Section 3.2, we present the protocol for anonymous transmission with the W state and discuss its correctness. In Section 3.3, we provide the security definition and prove that our protocol is secure in the semiactive and passive adversary scenario. Finally, in Section 3.4 we examine the behavior of our protocol in a noisy quantum network and compare it with the other existing protocols.

3.2. THE PROTOCOL

Our anonymous transmission protocol, Protocol 1, allows a sender S to transmit an arbitrary quantum state $|\psi\rangle$ to a receiver R in an anonymous way and uses the N-partite W state as a quantum resource. Protocol 1 is built on a number of classical subroutines – collision detection, receiver notification, veto and logical OR. Specifically: collision detection checks whether only one of the nodes wishes to be the sender; receiver notification notifies the receiver of her role in the protocol; veto announces if at least one of the parties has given input 1; and logical OR computes the XOR of the input of all the parties. In [8], protocols for implementing these classical subroutines were proposed. The protocols were proven to be information-theoretically secure in the classical regime, even with an arbitrary number of corrupted participants, assuming the parties share pairwise authenticated private channels and a broadcast channel. However, security against a quantum adversary was not analyzed. Like in related work [5], here we will assume that the protocols listed above remain secure even in the presence of a quantum adversary. We make this assumption explicit in the security proof presented in Section 3.6.2, where we assume that the classical subprotocols only act on the classical input register and create the output register, therefore, not revealing any information other than what is specified by the protocol.

The main concern of any anonymous transmission protocol is to hide the identities of sender S and receiver R. Nonetheless, it is also desired that, in the case in which all the parties act honestly, no information about the transmitted message is revealed. In order to achieve this functionality we add the step where R randomizes the output of the logical OR in Step 6 of Protocol 1. In that way, the classical outcome of the teleportation, m, is sent from S to R in a secret way. Indeed, even though the classical bit m could be sent by a simple anonymous broadcast protocol, the probability of obtaining a particular outcome m can depend on which state is teleported if the established anonymous entanglement is not a maximally entangled state. This is the case especially in the presence of noise in the network (for more details see Section 3.6.3).

Note that our protocol is probabilistic, as the parties may abort in Step 5. However, since the measurement outcomes are announced, the creation of anonymous entanglement is heralded. Hence, S and R know when the anonymous entanglement failed to be established before they initiate the teleportation, so in the case in which the protocol

Protocol 1: Anonymous transmission with the W state.

Goal: Transmit a quantum state $|\psi\rangle$ from the sender S to the receiver R, while keeping the identities of S and R anonymous.

1. *Collision detection.*
   Nodes run the classical collision detection protocol [8] to determine a single sender S. All nodes input 1 if they do wish to be the sender and 0 otherwise. If a single node wants to be the sender, continue.

2. *Receiver notification.*
   Nodes run the classical receiver notification protocol [8], where the receiver R is notified of her role.

3. *State distribution.*
   A trusted source distributes the N-partite W state.

4. *Measurement.*
   $N-2$ nodes (all except for S and R) measure in the $\{|0\rangle, |1\rangle\}$ basis.

5. *Anonymous announcement of outcomes.*
   Nodes use the classical veto protocol [8] which outputs 0 if all the $N-2$ measurement outcomes are 0, and 1 otherwise. If the output is 0 then anonymous entanglement is established, else abort.

6. *Teleportation.*
   Sender S teleports the message state $|\psi\rangle$ to the receiver R. Classical message m associated with teleportation is sent anonymously. The communication is carried out using the classical logical OR protocol [8] which computes $m \oplus \text{rand}$, where rand is a random 2-bit string input by the receiver R.

aborts, S keeps the state $|\psi\rangle$. In the following we first state the correctness of the protocol and then elaborate on the probability of success in the protocol, as a function of the number of parties in the network N.

Lemma 1 (correctness)**.** *If all the parties act honestly and Protocol 1 does not abort, the state $|\psi\rangle$ is transferred from the sender S to the receiver R, except with probability ϵ_{corr}, where ϵ_{corr} is an exponentially vanishing function of the number of rounds used to implement the classical subroutines.*

Proof. First, recall that Protocol 1 is built on several classical subroutines and in [8], protocols to implement these subroutines were presented. The protocols were proven to be correct except with a probability that vanishes exponentially with the number of rounds n_{class} used to implement the subroutines. Secondly, conditioned on the fact that the classical subroutines are correct and the parties act honestly, the measurement in the $\{|0\rangle, |1\rangle\}$ basis can lead to two situations: *(i)* all parties obtain measurement outcome 0, in which case the anonymous entangled state between S and R is $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, or *(ii)* a single party obtains a measurement outcome 1 and then the state between S and R is $|00\rangle$, in which case they abort the protocol. If the parties do not abort the protocol in Step 5, then the state shared by S and R is the maximally entangled state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, which is then used to perfectly teleport state $|\psi\rangle$ from S to R. Altogether, this implies that Protocol 1 is correct except with probability ϵ_{corr} which vanishes exponentially with n_{class}.

□

Lemma 2 (probability of success)**.** *Given sender S and receiver R, the probability of obtaining the anonymous entangled state $|\psi^+\rangle$ in Step 4 of Protocol 1 is $\frac{2}{N}$.*

Proof. Let $|\vec{0}\rangle\langle\vec{0}|_{N-2}$ denote the projection on the $|0\rangle$ state of $N-2$ parties. The probability P_{ψ^+} of obtaining this state can be expressed as $P_{\psi^+} = \text{Tr}\left[|\text{W}\rangle\langle\text{W}|_N \cdot \left(\mathbb{1}_{SR} \otimes |\vec{0}\rangle\langle\vec{0}|_{N-2}\right)\right] = \frac{2}{N}\text{Tr}\left[|\psi^+\rangle\langle\psi^+|\right] = \frac{2}{N}$. □

Lemma 2 states that in the honest implementation, the probability of not aborting in Step 4 of Protocol 1 decreases with the number of parties. Protocols based on the GHZ state [3, 5], on the other hand, are deterministic in creating anonymous entanglement. However, we remark that a fair comparison between the success rate of the two protocols should also take into account the rate of state generation. Note that recently, a linear optical setup for generating the W state in nitrogen-vacancy systems was proposed [9], which could offer a potential advantage in generation rates of the W state, over the GHZ state.

3.3. SECURITY

As discussed in the previous section, in the task of anonymous transmission the main goal is to keep the identities of sender S and receiver R secret. In this section we present the security definitions and prove the security of Protocol 1 against a semiactive adversary.

Let $[N] = \{1, \ldots, N\}$ be the set of nodes. We say that dishonest nodes are a subset $\mathscr{A} \in [N]$, with $|\mathscr{A}| = t$. This set is defined at the beginning of the protocol, which is known as a *nonadaptive* adversary.

Definition 7 (semiactive adversary)**.** We define the *semiactive adversary* scenario as one in which the adversaries are active, i.e., can perform arbitrary joint operations on their state during the execution of the protocol, but the source distributing a quantum state is trusted.

In particular, for Protocol 1 this means that the state in Step 3 is exactly the W state. This adversarial model is stronger than a *passive* adversary, where it is assumed that the parties follow all the steps of the protocol and only collect the available classical information. However, note that a fully active adversarial scenario would allow the cheating participants to corrupt the source.

We define security in terms of the guessing probability, i.e., the maximum probability that adversaries guess the identity of the S or R given all the classical and quantum information they have available at the end of the protocol. Intuitively, we say that the protocol is secure when the guessing probability is no larger than the uncertainty the adversaries have about the identity of the sender before the protocol begins. This uncertainty is defined by the prior probability, $P[S = i | S \notin \mathscr{A}]$. For example, in the case where all the nodes are equally likely to be the sender, the prior probability is uniform and, therefore, $P[S = i | S \notin \mathscr{A}] = \frac{1}{N-t}$.

In Protocol 1 it is assumed that the message $|\psi\rangle$ to be sent carries no information about the sender's identity. We remark that anonymous transmission is concerned with ensuring anonymity and not secrecy. In the case in which secrecy of the message is required, anonymous transmission could be combined with another primitive that allows one to encrypt the message. However, here, we do not address this issue.

Definition 8 (guessing probability)**.** Let $\mathscr{A}$ be the subset of semiactive adversaries. Let C be the register that contains all classical and quantum side information accessible to the adversaries. Let $W^{\mathscr{A}}$ denote the adversaries' quantum register of the state distributed by the source. Then, the probability of adversaries guessing the sender is given by

$$\begin{aligned} &P_{\text{guess}}[S|W^{\mathscr{A}}, C, S \notin \mathscr{A}] = \\ &\quad = \max_{\{M^i\}} \sum_{i \in [N]} P[S = i | S \notin \mathscr{A}] \operatorname{Tr}\left[M^i \cdot \rho_{W^{\mathscr{A}} C | S = i} \right], \end{aligned} \tag{3.1}$$

where the maximization is taken over the set of POVMs $\{M^i\}$ for the adversaries and $\rho_{W^{\mathscr{A}} C|S=i}$ is the state of the adversaries at the end of the protocol, given that node i is the sender.

Definition 9 (sender security)**.** We say that an anonymous transmission protocol is *sender-secure* if, given that the sender is honest, the probability of the adversary guessing the sender is

$$P_{\text{guess}}[S|W^{\mathscr{A}}, C, S \notin \mathscr{A}] \leq \max_{i \in [N]} P[S = i | S \notin \mathscr{A}]. \tag{3.2}$$

In words, the protocol is sender-secure if the probability that the adversaries guess the identity of S at the end of the protocol is not larger than the probability that an honest node i is the sender, maximized over all the nodes. An analogous definition can be given for the *receiver security*.

We remark that, even if S and R are honest, it is trivially possible for the *malicious* parties to prevent S and R from exchanging the desired message. For example, the dishonest parties can measure the W state in a different basis affecting the resulting anonymous entanglement. In this sense, the correctness of Protocol 1 is not robust to malicious attacks. However, in what follows, we show that Protocol 1 is secure, and even in the presence of dishonest parties, the anonymity of S and R is preserved.

Theorem 1. *The anonymous transmission protocol with the W state, Protocol 1, is sender- and receiver-secure in the semiactive adversary scenario.*

Idea of the proof. For clarity, here we present the main idea of our security proof and we refer the reader to Section 3.6.3 for details. Note that in the semiactive adversary scenario we allow the adversaries to apply an arbitrary cheating strategy, which in particular includes not following the steps of the protocol and performing global operations on their joint state. First, let us discuss the sender security. We consider the case when R is honest, $R \notin \mathscr{A}$, as well as when she is dishonest, $R \in \mathscr{A}$. In both cases, the gist of our sender-security proof is to show that the reduced quantum state of the adversary $\rho_{W^{\mathscr{A}}C|S=i}$ at the end of the protocol is independent of the sender, i.e., $\forall\, i \notin \mathscr{A}$, $\rho_{W^{\mathscr{A}}C|S=i} = \rho_{W^{\mathscr{A}}C}$. To show it, we explicitly use the assumption that the classical protocols do not leak any information about S or R's identity even if the adversary has access to quantum correlations. Therefore, any quantum side information the adversary holds is independent of S. This, together with the fact that the state distributed by the source is permutationally invariant yields the desired equality. Since now the reduced quantum state of the adversary is independent of S we can easily upper-bound the guessing probability by $\max_{i\in[N]} P[S = i|S \notin \mathscr{A}]$. The receiver security can be proven following the same structure. □

Note that our security proof tolerates any number of cheating nodes. It is also general enough to make a security statement about any resource state that is invariant under permutation of nodes.

Let us now discuss a passive adversarial model, also called the honest-but-curious model. This is the case when the malicious parties follow all the steps of the protocol (in particular, they measure in the $\{0,1\}$ basis in Step 4), but can collaborate to compare their classical data. Note that the passive adversary model is a special case of the semiactive adversary scenario. However, this model is interesting by itself, since in the case in which the nodes build their anonymous transmission protocol using weaker versions of classical subroutines, i.e., those that are not secure against quantum adversary, the security still holds. Indeed, it restricts the power of the adversary, so that they cannot share any quantum side information. Then, the probability of the adversaries guessing the sender simplifies to $P_{\text{guess}}[S|W^{\mathscr{A}}, C, S \notin \mathscr{A}] = \sum_{a,c} P[W^{\mathscr{A}} = a, C = c] \max_{i\in[N]} P[S = i|W^{\mathscr{A}} = a, C = c, S \notin \mathscr{A}]$, where maximization is taken over all the values of the random variable S, and a, c are possible values of random variables $W^{\mathscr{A}}$ and C respectively [10]. Note that, unlike before, here $W^{\mathscr{A}}$ is a classical register of the adversary, since their

share of the W state was measured in the $\{0,1\}$ basis. An analogous expression holds for receiver-security.

Theorem 2. *The anonymous transmission protocol with the W state, Protocol 1, is sender- and receiver-secure in the passive adversary scenario.*

The proof of this statement is a special case of the proof of Theorem 1. As before, we use the fact that classical protocols do not leak identities of S and R and the permutational invariance of the resource state to conclude that the classical information generated during the protocol is independent of who is sender and receiver. For details see Section 3.6.3.

3.4. ANONYMOUS TRANSMISSION IN A NOISY QUANTUM NETWORK

Equipped with the security tools from the previous section, here we analyze the security and performance of Protocol 1 in a noisy quantum network. We consider a noise model in which each qubit is subjected to the same individual noisy channel. One can think that a trusted source prepared the multipartite state for the network, but each qubit is individually affected by a noise map Λ while being transmitted to the nodes. Note that this model can also encompass noise on the local measurements performed on the state. Therefore, in our noisy network, if $|\mathrm{W}\rangle_N$ is the perfect N-partite W state prepared by a trusted source, then

$$\omega_N^{\Lambda} = \Lambda^{\otimes N}(|\mathrm{W}\rangle\langle\mathrm{W}|_N) \tag{3.3}$$

is the state distributed to the parties at Step 3 of Protocol 1.

3.4.1. SECURITY IN THE PRESENCE OF NOISE

Perfect security. In what follows we will show that our protocol is perfectly secure in the semiactive adversary scenario in the noisy network defined by Eq. (3.3). We start by defining what it means for a map to preserve permutational invariance.

Definition 10 (Permutational-invariance preserving map)**.** Let π be a permutationally invariant state, such that for all permutations Σ, $\pi = \mathcal{V}_\Sigma(\pi)$, where $\mathcal{V}_\Sigma$ is a map that performs the permutation Σ on the subsystems. A map $\mathscr{E}$ is permutational-invariance preserving if the state after the action of the map $\pi' = \mathscr{E}(\pi)$ is permutationally invariant, i.e., $\pi' = \mathcal{V}_\Sigma(\pi')$.

Note that the noise channel of our interest, $\Lambda^{\otimes N}$, preserves permutational invariance according to the above definition, due to the tensor structure.

Theorem 3. *The anonymous transmission protocol with the W state, Protocol 1, is sender- and receiver-secure in the semiactive adversary scenario in a noisy network, where noise is defined by Eq.* (3.3).

Proof. According to Definition 10, the noise channel $\Lambda^{\otimes N}$ is permutational-invariance preserving. Therefore, the proof of Theorem 3 follows exactly the same steps as the proof

of Theorem 1, where one replaces the state distributed by the source, $|\mathrm{W}\rangle\langle\mathrm{W}|_N$, with ω_N^Λ. Therefore if $\rho^\Lambda_{W^{\mathscr{A}}C|S=i}$ is the state of the adversaries at the end of the protocol, given that node i is the sender, we have that $\rho^\Lambda_{W^{\mathscr{A}}C|S=i} = \rho^\Lambda_{W^{\mathscr{A}}C}$, for all $i \notin \mathscr{A}$, and

$$\begin{aligned} P_{\text{guess}}[S|A,C,S\notin\mathscr{A}] &:= \max_{\{M^i\}} \sum_{i\in[N]} P[S=i|S\notin\mathscr{A}]\,\mathrm{Tr}\left[M^i\cdot\rho^\Lambda_{W^{\mathscr{A}}C|S=i}\right] \\ &\leq \max_{i\in[N]} P[S=i|S\notin\mathscr{A}]. \end{aligned} \tag{3.4}$$

The same statement holds for receiver-security. □

3

ε security. In a realistic quantum network, it is quite unlikely that one will be able to control the noise channels perfectly and ensure that all qubits are subjected to the action of exactly the same noise channel. Here we would like to analyze what happens in the case when the network noise is slightly perturbed, in the sense that each qubit experiences a slightly different noise. We say that in the perturbed case, the network noise is such that each individual qubit of the multipartite W state, $|\mathrm{W}\rangle_N$, is subjected to an action of a channel Λ_i,

$$\hat{\omega}_N^\Lambda = \bigotimes_{i=1}^N \Lambda_i(|\mathrm{W}\rangle\langle\mathrm{W}|_N), \tag{3.5}$$

where $\|\Lambda-\Lambda_i\|_1 \leq \varepsilon_i$ for some map Λ, and $\|\cdot\|_1$ denotes the induced trace norm [11].

Since each channel is slightly perturbed, the state after the action of the channel, $\hat{\omega}_N^\Lambda$, is no longer perfectly permutationally invariant. Yet, intuitively, since the perturbation is small, the state $\hat{\omega}_N^\Lambda$ is ε-close to a permutationally invariant state, for some small ε, and, consequently, the protocol should be ε-secure. In the following we show that this intuition is, indeed, true. First, let us formalize the notion of ε security.

Definition 11 (ε-sender security)**.** We say that the anonymous transmission protocol is *ε-sender-secure* if, given that the sender is not the adversary, the probability of the adversaries guessing the sender is

$$P_{\text{guess}}[S|W^{\mathscr{A}},C,S\notin\mathscr{A}] \leq \max_{i\in[N]} P[S=i|S\notin\mathscr{A}] + \varepsilon. \tag{3.6}$$

And analogously for ε-receiver security.

Theorem 4. *The anonymous transmission protocol with the W state, Protocol 1, is $N\varepsilon_{\max}$-sender-secure in the semiactive adversary scenario when the noise in the network is defined by Eq.* (3.5)*, i.e.,*

$$\begin{aligned} P_{\text{guess}}[S|W^{\mathscr{A}},C,S\notin\mathscr{A}] &= \max_{\{M^i\}} \sum_{i\in[N]} P[S=i|S\notin\mathscr{A}]\,\mathrm{Tr}\left[M^i\cdot\hat{\rho}^\Lambda_{W^{\mathscr{A}}C|S=i}\right] \\ &\leq \max_{i\in[N]} P[S=i|S\notin\mathscr{A}] + N\varepsilon_{\max}, \end{aligned} \tag{3.7}$$

where $\hat{\rho}^\Lambda_{W^{\mathscr{A}}C|S=i}$ is the state of the adversaries at the end of the protocol, and $\varepsilon_{\max} = \max_{i\in[N]}\varepsilon_i$, with ε_i given by Eq. (3.5)*.*

The idea of the proof is to show that, for all $i \in [N]$, the trace $\mathrm{Tr}\left[M^i \cdot \hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]$ is upper-bounded by $\mathrm{Tr}\left[M^i \cdot \rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right] + N\varepsilon_{\max}$. Then using the fact that $N\varepsilon_{\max}$ is independent of i, the rest of the proof follows from Theorem 3. For details see Section 3.6.3.

3.4.2. PERFORMANCE IN A NOISY NETWORK

In this section we analyze the performance of Protocol 1 in a noisy quantum network. To do so reliably, we assume honest implementation; i.e., all of the parties follow the protocol. In the honest implementation, given success in the protocol, the anonymous entangled state between S and R after Step 5. is

$$\omega_{SR} = \frac{1}{\mathscr{N}} \mathrm{Tr}_{N-2}\left[\Lambda^{\otimes N}(|\mathrm{W}\rangle\langle\mathrm{W}|_N) \cdot \left(\mathbb{1}_{SR} \otimes |\vec{0}\rangle\langle\vec{0}|_{N-2}\right)\right], \tag{3.8}$$

where $|\mathrm{W}\rangle\langle\mathrm{W}|_N$ is the N-partite W state, $|\vec{0}\rangle\langle\vec{0}|_{N-2}$ is a projection onto the $|0\rangle$ state of $N-2$ parties and $\mathscr{N}$ is a normalization factor. Note that in the case where no noise is present we recover the maximally entangled state, i.e. $\omega_{SR} = \left|\psi^+\right\rangle\left\langle\psi^+\right|$, where $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |01\rangle)$.

Throughout the rest of the chapter, we will be interested in discussing the performance of anonymous transmission protocols under two types of noise:

1. Λ is the dephasing channel

$$\Lambda(\rho) = \mathscr{P}_q(\rho) = q\rho + (1-q)Z\rho Z, \tag{3.9}$$

where ρ is a single qubit state, Z is the Pauli Z gate, and $q \in [0,1]$ is the noise parameter.

2. Λ is the depolarizing channel

$$\Lambda(\rho) = \mathscr{D}_q(\rho) = q\rho + (1-q)\frac{\mathbb{1}}{2}, \tag{3.10}$$

where ρ is a single qubit state, $\frac{\mathbb{1}}{2}$ is a maximally mixed single-qubit state, and $q \in [0,1]$ is the noise parameter.

Comparison with the GHZ protocol [3]. In the following we are interested in comparing the performance of our protocol using the W state with the protocol that uses the GHZ state (for reference see [3, 5]). The main differences between our protocol and the protocol presented in [3] lie in *(i)* the initial resource state: W in our case and GHZ for [3]; *(ii)* the measurement basis: standard basis for our protocol and X basis for [3]; *(iii)* the fact that our protocol is probabilistic, whereas the one with the GHZ state continues regardless of the measurement outcome.

For the noise under consideration, all measurement outcomes in the GHZ protocol are equally likely and the resulting states are equivalent up to a local unitary operation.

Therefore, without loss of generality, we consider the state between S and R created in this protocol to be

$$\gamma_{SR} = \frac{1}{\mathcal{N}'} \mathrm{Tr}_{N-2} \Big[\Lambda^{\otimes N}(|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_N) \cdot \left(\mathbb{1}_{SR} \otimes \left|\vec{+}\right\rangle\left\langle\vec{+}\right|_{N-2}\right) \Big], \tag{3.11}$$

where $|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_N$ is the N-partite GHZ state, $\left|\vec{+}\right\rangle\left\langle\vec{+}\right|_{N-2}$ is a projection onto the $|+\rangle$ state of $N-2$ honest parties and $\mathcal{N}'$ is a normalization factor. In the case where no noise is present in the network, the ideal state of S and R is the maximally entangled state $\gamma_{SR} = \left|\phi^+\right\rangle\left\langle\phi^+\right|$, with $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Note that this is a different maximally entangled state than in our W state protocol, but both states are equally useful for teleportation.

To compare the performance of the two protocols, we fix the figure of merit to be the *fidelity* of the obtained anonymous entangled (AE) state with the ideal state that is obtained in the protocol when no noise is present,

$$F_{AE}(\omega_{SR}) = \mathrm{Tr}\left[\omega_{SR} \cdot \left|\psi^+\right\rangle\left\langle\psi^+\right|\right] \tag{3.12}$$

$$F_{AE}(\gamma_{SR}) = \mathrm{Tr}\left[\gamma_{SR} \cdot \left|\phi^+\right\rangle\left\langle\phi^+\right|\right] \tag{3.13}$$

where ω_{SR} and γ_{SR} are anonymous entangled states between S and R arising from measuring W and GHZ states subjected to the network noise.

In what follows we define what it means for an anoymous entangled state to be useful. Before that, let us motivate it twofold. First, not all states are entangled enough to be a resource for teleportation. It has been shown in [12] that any two-qubit entangled state can be used for teleportation if and only if its singlet fidelity exceeds $\frac{1}{2}$. Secondly, note that the quality of a low-fidelity anonymous entanglement could be further improved by performing entanglement distillation [13] – a protocol which creates an entangled state with high fidelity out of a few lower-fidelity states. However, entanglement distillation protocols can be carried out only when fidelities of initial states are larger than $\frac{1}{2}$. We remark that performing entanglement distillation without compromising security of anonymous transfer requires support of anonymous two-way classical communication between S and R. This can be achieved, for example, by using a classical anonymous broadcast protocol [8].

We are now ready to define what it means to say that a resource state is useful for anonymous transmission.

Definition 12 (Usefulness)**.** We say that the anonymous entangled state is a *useful* resource for transmission of a quantum message if its fidelity is strictly larger than $\frac{1}{2}$, i.e. $F_{AE} > \frac{1}{2}$. Therefore an N-partite state is a useful resource state for anonymous transmission if, upon the parties acting honestly, it can generate anonymous entanglement between any two nodes with $F_{AE} > \frac{1}{2}$.

To evaluate the behavior of the protocols, we calculate the fidelity of anonymous entanglement as a function of the noise parameter q and the number of nodes N, for the depolarizing and dephasing channels. Examples of the performance of the W and GHZ protocols for $N = \{4, 10, 50\}$ are shown in Figure 3.1.

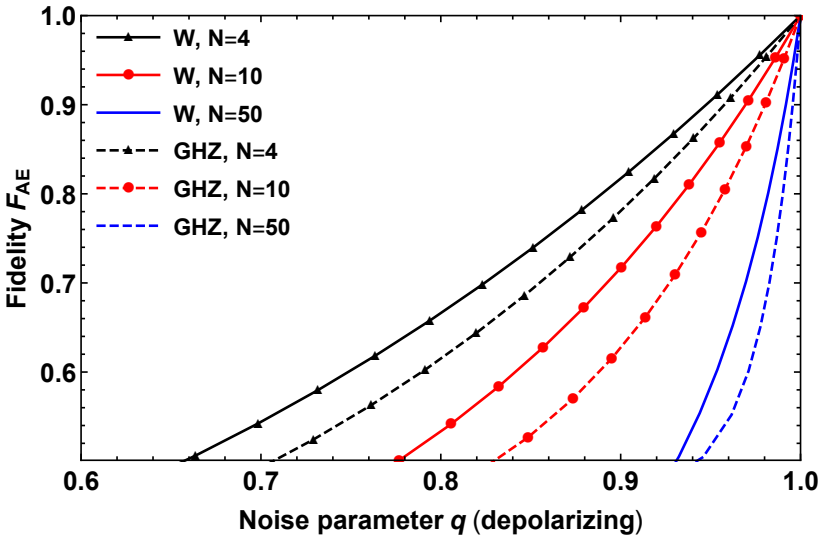


Figure 3.1: Fidelity of anonymous entanglement as a function of the noise parameter q for depolarizing network noise. Examples for $N = \{4, 10, 50\}$.

	$F_{AE}(\omega_{SR})$	$F_{AE}(\gamma_{SR})$
Dephasing noise $\mathscr{P}_q^{\otimes N}$	$1-2q(1-q)$	$\frac{1+(2q-1)^N}{2}$
Depolarizing noise $\mathscr{D}_q^{\otimes N}$	$\frac{(1+q)(N(q-1)^2+4q(1+q))}{4(N(1-q)+4q)}$	$\frac{2q^N+q^2+1}{4}$

We can now ask ourselves which of the states, GHZ or W, tolerates more noise. Note that if one has access to both parameters of the network, noise parameter q and number of nodes N, it is easy to determine which of the states would perform better by simply looking at values of F_{AE} calculated from our analytical expressions.

We start by looking at the dephasing noise. Observe that in this case the fidelity of anonymous entanglement created with the W state $F_{AE}(\omega_{SR})$ is constant in N. Specifically, this implies that when fixed dephasing noise is present in the network, the quality of the anonymous link is always the same, regardless of the number of nodes N. Moreover, for the dephasing noise, one can observe that $F_{AE}(\omega_{SR}) \geq F_{AE}(\gamma_{SR})$ for all $N \geq 2$ and all q, which implies that our Protocol 1 tolerates more noise than the GHZ-based protocol [3, 5].

When depolarizing noise is present in the network, unlike for the dephasing noise, the fidelity of the anonymous entanglement generated by Protocol 1 decreases as the number N of parties increases. Let us define the noise threshold q^* as the minimum value of noise parameter q for which the anonymous entangled state is still useful in the sense of Def. 12. One can see that, for small networks (e.g., $N < 50$), the threshold q^* is

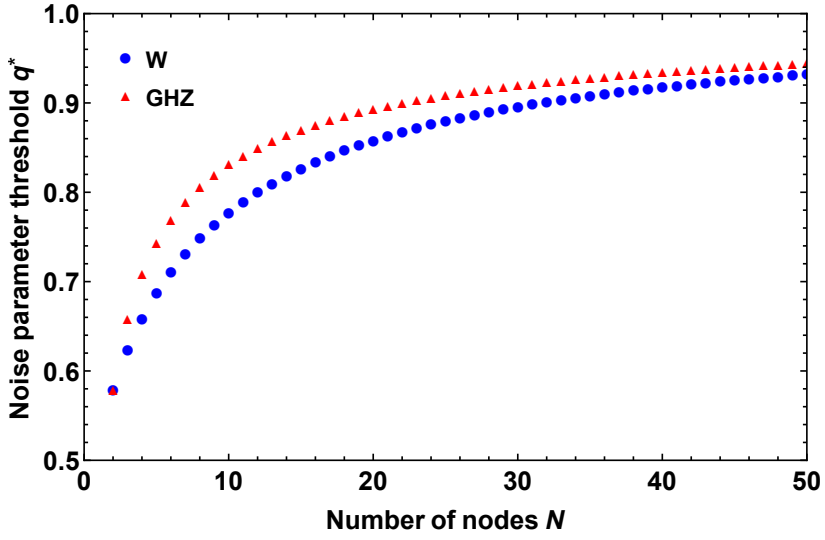


Figure 3.2: Depolarizing parameter thresholds for fidelity of anonymous entanglement $F_{AE} = \frac{1}{2}$.

lower for the W state than for the GHZ state $q^*_W < q^*_{GHZ}$, see Fig. 3.2, which implies that the W state tolerates more noise in these cases. However, for $N \geq 182$ one finds that the converse is true, $q^*_W > q^*_{GHZ}$, and therefore the GHZ-based protocol tolerates more noise in this regime. Nevertheless, in Section 3.7.2 we show that for $N \geq 182$ and larger values of q, $q > q^*_W$, we still recover the behavior $F_{AE}(\omega_{SR}) \geq F_{AE}(\gamma_{SR})$. Lastly, we remark that the challenge to create a multipartite state scales with the number of parties. Therefore, applications of anonymous transmission of interest in the near future will likely be in the range of $N < 50$, in which case Protocol 1 has proven to be the most noise-tolerant.

Let us also comment on the probability of success of our protocol in the presence of noise. Recall that a round of the protocol only succeeds if in Step 3 the measurement outcome of the $N-2$ measuring parties is 0. For the dephasing noise the probability of success in our protocol remains $\frac{2}{N}$, which is due to the fact that the noise commutes with the measurement basis. However, for the depolarizing noise the probability of success drops exponentially in N. In contrast, for the GHZ state, the outcomes do not need to be post-selected, therefore the protocol [3] remains deterministic.

Comparison with the relay protocol [6]. We now compare our protocol to a scheme proposed in [6], which only requires the creation of local Bell pairs and therefore could potentially offer an advantage for a quantum network implementation. The main idea of the relay protocol [6] is to locally prepare and transmit Bell pairs in order to create a four-partite GHZ state, which will then be turned into anonymous entanglement.

In the protocol proposed in [6], the nodes are consecutively ordered and each node locally prepares a Bell pair. The first node sends half of her Bell pair to the second node. The second node performs entanglement swapping with a half of her own Bell pair and

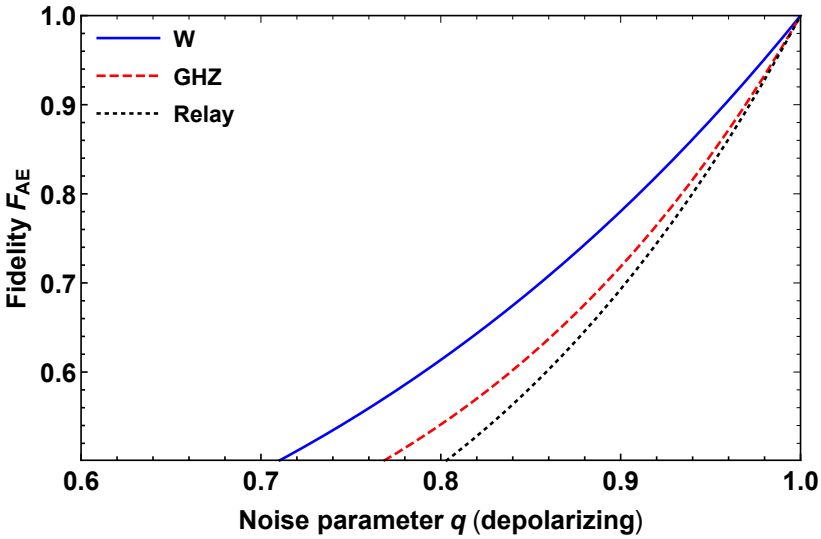


Figure 3.3: Comparison of the fidelity of anonymous entanglement F_{AE} for the W state protocol (Protocol 1), the GHZ protocol [3] and the relay scheme [6] for $N = 6$ nodes.

sends the other half of the state to the next node. This relay continues until the last N-th node is reached. S and R, however, perform an additional CNOT operation, where they locally entangle the state received from another node with an additional qubit initiated in $|0\rangle$. At the end of this relay a four-partite GHZ state is created among S, R, the first and the last node. Finally, anonymous entanglement is established after the first and the last node perform a measurement.

We explore a scenario for $N = 6$ nodes, assuming that the network is such that quantum channels between parties are depolarizing channels $\Lambda = \mathscr{D}_q$; i.e., whenever a qubit is sent from one party to another it is subject to depolarization. We calculate fidelities of anonymous entanglement for different locations of the S and R in the network. Our results are summarized in Section 3.7.2. The numerical evidence shows that in the presence of the depolarizing noise in the network, the fidelity of anonymous entanglement is different depending on the ordering of S and R in the network. Note that this does not necessarily imply that the security of the protocol is broken, in the sense that nodes can learn the identity of S and R. However, we can see that the performance of the protocol strongly depends on who is sender and receiver, which is not a desirable feature for the anonymous transmission task.

With this in mind, we define the usefulness of the anonymous entanglement created with the relay scheme as the worst case fidelity achieved by the scheme. This is practical if one wants to make sure that the scheme achieves at least a certain fidelity threshold. We then compare the behavior of the relay scheme with the behavior of Protocol 1 in the presence of depolarizing noise. In Fig. 3.3 one can see that in the presence of the depolarizing noise in the network the relay protocol achieves lower fidelity than both the GHZ and the W state protocols.

Nonresponsive nodes. Finally, let us consider the scenario where some of the nodes, that are neither S nor R, stop responding. This can happen, for example, due to particle losses in the multipartite state. Note that if S or R lose their particle the teleportation cannot be carried out and, therefore, the protocol is not correct.

Let us consider that the resource state prepared by the source suffers from the action of a noise channel where particles might get lost. Then, with some probability k out of N nodes experience particle loss. Here we ask the question of how many particles losses can be tolerated in an anonymous transmission protocol. Say that a protocol tolerates k' particle losses. After the distribution of the state, if k particles are lost: *(i)* the nodes abort the protocol if $k > k'$, or *(ii)* the remaining $N-k$ parties proceed with the protocol if $k \leq k'$.

It is known that the entanglement of the GHZ state is not robust to particle losses; *i.e.*, if one particle is lost the remaining $N-1$ parties are left with a separable state. On the other hand, if the W state is subjected to $N-2$ particle losses the remaining bipartite state is still entangled. In fact, the W state is the most robust to particle losses among all N qubit states [14]. Motivated by this property of the W state, we show that Protocol 1 can tolerate one nonresponsive node. Observe that the N-partite W state has the following form after tracing out k out of N parties,

$$\mathrm{Tr}_k |\mathrm{W}\rangle\langle\mathrm{W}|_N = \frac{N-k}{N} |\mathrm{W}\rangle\langle\mathrm{W}|_{N-k} + \frac{k}{N} |\vec{0}\rangle\langle\vec{0}|_{N-k} \tag{3.14}$$

where $|\mathrm{W}\rangle\langle\mathrm{W}|_{N-k}$ is the W state of $N-k$ parties.

In the following theorem we show that Protocol 1 tolerates one particle loss.

Theorem 5. *Protocol 1 tolerates one nonresponsive node $i \in [N] \setminus \{S, R\}$ to produce useful anonymous entanglement, regardless of the number of parties.*

Proof. The proof of the above theorem involves two steps. We first show the correctness of Protocol 1 when one of the nodes stopped responding, and then show that the created entangled link between S and R is in fact anonymous, i.e. that the security is preserved.

Let us look at the correctness. The measurement of the state (3.14) in the standard basis and after obtaining all 0 outcomes on $N-k-2$ parties yields a normalized state

$$\tilde{\omega}_{SR} = \frac{2}{2+k} \left|\psi^+\right\rangle\!\left\langle\psi^+\right| + \frac{k}{2+k} |00\rangle\langle 00| \tag{3.15}$$

which has entanglement fidelity $F_{AE}(\tilde{\omega}_{SR}) = \frac{2}{2+k}$. By Definition 12 the state $\tilde{\omega}_{SR}$ is useful for anonymous transmission if $\frac{2}{2+k} > \frac{1}{2}$ which implies $k < 2$. This yields the desired result.

To show that the created entanglement is anonymous, observe that when one of the nodes stops responding the resource state is the state from Eq. (3.14) with $k = 1$. This state is invariant under permutations of nodes and, therefore, we can treat it as a new resource state. Then the security proof follows the same pattern as the proof of Theorem 1. □

For completeness, in Section 3.7.2 we provide analytical expressions for the fidelity of anonymous entanglement when the W state is subjected to one particle loss, as well as

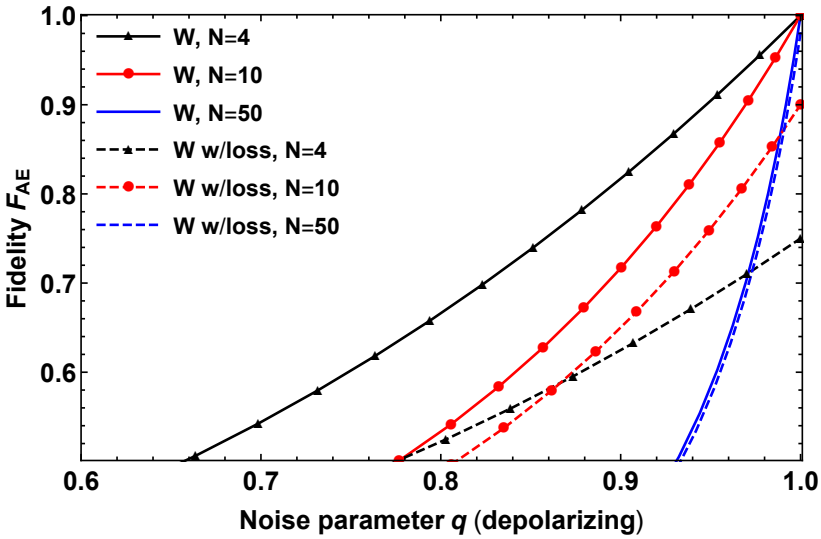


Figure 3.4: Fidelity of anonymous entanglement as a function of the noise parameter q for depolarizing network noise when the resource W state is subjected to one particle loss. Examples for $N = \{4, 10, 50\}$.

dephasing and depolarizing noise. Figure 3.4 shows the comparison of anonymous entanglement fidelity of Protocol 1 under depolarizing noise without particle loss, $F_{AE}(\omega_{SR})$, and when one particle is lost, $F_{AE}(\tilde{\omega}_{SR})$, for $N = \{4, 10, 50\}$ nodes. Note that with the growing number of nodes the fidelity of anonymous entanglement in the lossy case approaches the one with no-loss. Indeed, the larger N the smaller the admixture of the $|\vec{0}\rangle\langle\vec{0}|_{N-1}$ term in Eq. (3.14), and so, with growing N the fidelity is less affected by the loss of a particle. On the other hand, for a larger number of nodes more than one particle loss is more likely to occur. Therefore, the probability that the protocol aborts also increases with the number of nodes.

Lastly, we point out that when one particle is lost in the protocol of [6], the relay cannot be completed. Therefore, much like the GHZ protocol, the relay protocol also cannot be used to create anonymous entanglement whenever one of the nodes is not responsive.

3.5. OUTLOOK

We presented a protocol for quantum anonymous transmission using the W state, and proved its security in the semiactive adversary scenario, i.e. when the adversary is active and the source of a quantum state is trusted. Moreover, we analyzed the behavior of our protocol under the action of common noise models that occur in a realistic quantum network. An important question is whether our security proof can be extended to the case where the source might be corrupted, i.e. the fully active adversary scenario. Note that to achieve full security in the noiseless case for the GHZ protocol, Refs. [5, 15] introduced a certification step of the resource state shared by the trusted parties. We remark

that for the noiseless W state protocol, it may be possible to achieve full security in a similar way by employing self-testing techniques [16, 17]. The problem of certifying the resource state in the presence of noise in the network remains an open question.

We have also analyzed the security of our protocol when each qubit suffers the action of a noise channel with slightly different parameters. This bound, however, may not be tight, so another interesting question is whether the security proof can be improved and a stronger bound can be derived for this case.

Finally, we have seen that in many instances our W-state based protocol outperforms the GHZ-state and Bell-pair based protocols. For the values of parameters N and q, where all the protocols produce useful anonymous entanglement, we remark that a more refined comparison of their performance should take into account the generation rates and resources required to produce the states in every particular experimental setup.

3.6. TECHNICAL STATEMENTS - SECURITY

3.6.1. CLASSICAL SUBROUTINES

Our anonymous transmission protocol, Protocol 1, is built on a few classical subroutines. As mentioned, in [8], protocols for implementing these classical subroutines were proposed. Here we list the protocols which we will use as building blocks of our anonymous transmission protocol:

Theorem 6 (collision detection [8])**.** *There exists an information-theoretically secure collision detection protocol that takes as input the classical register Cd_{in} of all the participants, $Cd^i_{\text{in}} = 1$ if node i wishes to be a sender and $Cd^i_{\text{in}} = 0$ otherwise, and outputs $Cd_{\text{out}} = 0$ if only one register wants to be the sender and $Cd_{\text{out}} = 1$ otherwise.*

Theorem 7 (receiver notification [8])**.** *There exists an information-theoretically secure receiver notification protocol that takes as input the classical register Rn_{in} of the participants and outputs Rn_{out}, where $Rn^R_{\text{out}} = 1$ for the receiver, and all the other parties get output 0.*

Theorem 8 (veto [8])**.** *There exists an information-theoretically secure veto protocol that takes as input the classical register O_{in} of the parties and outputs $O_{\text{out}} = 0$ if all the parties input 0, $O_{\text{in}} = \vec{0}$, and $O_{\text{out}} = 1$ otherwise.*

Theorem 9 (logical OR [8])**.** *There exists an information-theoretically secure logical OR protocol that takes as input the classical register T_{in} and publicly outputs $T_{out} = \oplus_{i=1}^{N} T^i_{\text{in}}$.*

The protocols are information-theoretically secure, in the sense that they do not reveal any classical information other than the one specified by the protocol. The security holds even with an arbitrary number of corrupted participants, assuming the parties share pairwise authenticated private channels and a broadcast channel. However, security against a quantum adversary was not analyzed. Here we assume that the protocols listed above remain secure even in the presence of a quantum adversary. This assumption is made explicit in Section 3.6.2 where we assume that the classical subprotocols only act on the classical input register and create the output register, therefore not revealing any information other than what is specified by the protocol, also in the quantum setting.

3.6.2. STATES AND REGISTERS

In what follows we make a detailed description of the state in each step of Protocol 1. Our main goal is to show that the quantum state of the adversary at the end of the protocol does not depend on who is the sender or the receiver. We will later use this fact in the security proof in Section 3.3.

Here we adopt the notation that A denotes registers held by the adversary $\mathscr{A}$, and $\bar{A}$ denotes all the other registers, i.e., of the honest parties (including the sender and the receiver). After Step 2, i.e., once S and R are defined, we distinguish S and R registers from the registers of honest parties $\mathscr{H}$.

Table 3.1: Registers available to parties at each step of the Protocol 1. All registers are classical unless specified otherwise.

Step	Available registers	Description
0.	$A_0, \bar{A}_0$	Quantum side information of dishonest and honest parties before the beginning of Protocol 1.
1.	$Cd^A_{\text{in}}, Cd^{\bar{A}}_{\text{in}}$	Private input of the parties in the collision detection protocol. The node which wants to be a sender inputs 1, the rest 0.
	$Cd^A_{\text{out}}, Cd^{\bar{A}}_{\text{out}}$	Outputs of the collision detection protocol.
2.	$Rn^A_{\text{in}}, Rn^{\bar{A}}_{\text{in}}$	Private input of the receiver notification protocol. S inputs the identifier of R, everyone else 0.
	$Rn^A_{\text{out}}, Rn^{\bar{A}}_{\text{out}}$	Private outputs of receiver notification protocol. Output 0 for R, 1 for everyone else.
	$D^{\mathscr{A}}, D^{\mathscr{H}SR}$	Redefined register of dishonest parties $D^{\mathscr{A}} = \{A_0 Cd^A_{\text{in}} Cd^A_{\text{out}} Rn^A_{\text{in}} Rn^A_{\text{out}}\}$ and honest parties $D^{\mathscr{H}SR} = \{\bar{A}_0 Cd^{\bar{A}}_{\text{in}} Cd^{\bar{A}}_{\text{out}} Rn^{\bar{A}}_{\text{in}} Rn^{\bar{A}}_{\text{out}}\}$ after Step 2.
3.	$W^{\mathscr{H}}, W^{\mathscr{A}}, W^S, W^R$	Quantum registers of the state prepared by the source.
4.	$W^{\mathscr{H}}, W^{\mathscr{A}}, W^S, W^R$	Quantum registers of the state prepared by the source.
5.	$O^{\mathscr{H}}_{\text{in}}$	Private input of the honest parties to the veto protocol. Represented by a string of measurement outcomes $\vec{\nu}$.
	$O^{\mathscr{A}}_{\text{in}}$	Private input of dishonest parties to the veto protocol. Represented by a string of measurement outcomes $\vec{\mu}$.
	O_{out}	Public output of the veto protocol. 0 if all entries of strings $\vec{\nu}$ and $\vec{\mu}$ are 0, 1 otherwise.
6.	Q	Quantum register of quantum message $\|\psi\rangle$ which S wants to transmit.
	$T^S_{\text{in}}, T^R_{\text{in}}$	Private inputs of S and R to the logical OR protocol. S inputs teleportation message m and R inputs random bit rand.
	$T^{\mathscr{H}}_{\text{in}}, T^{\mathscr{A}}_{\text{in}}$	Private input of the honest and dishonest parties to the logical OR protocol.
	T	Public outcome the logical OR protocol. Outputs XOR of all the inputs.

In the following we specify what are the assumptions associated with each step of the protocol. Additionally, we explicitly write out the state $\xi^{(j)}$ after each step j of the protocol, taking into account all the registers that play a role in the particular step. Therefore, we remark that our notation may be cumbersome at the first glance. However, we advise the reader to refer to Table 3.1 at any point of our proof.

STEP 1. COLLISION DETECTION.

Assumption 1. Let A_0 be the quantum side information of dishonest parties and $\bar{A}_0$ be the quantum side information of the honest parties, including sender and receiver, before the beginning of the protocol. We assume that before the start of the protocol the parties share the following state:

$$\xi^{(0)}_{A_0\bar{A}_0 Cd_{\text{in}} Rn_{\text{in}}} = \sigma^{(0)}_{A_0\bar{A}_0 Cd^A_{\text{in}} Rn^A_{\text{in}}} \otimes \sigma^{(0)}_{Cd^{\bar{A}}_{\text{in}} Rn^{\bar{A}}_{\text{in}}}. \tag{3.16}$$

In words, we assume the adversaries have a quantum side information, A_0, and classical inputs to the collision detection and receiver notification protocol, Cd^A_{in} and Rn^A_{in}, that might be correlated with some quantum side information $\bar{A}_0$ of the remaining parties. However the inputs of the honest parties $Cd^{\bar{A}}_{\text{in}}$ and $Rn^{\bar{A}}_{\text{in}}$ are uncorrelated with the adversary's state.

Assumption 2. We assume that the classical collision detection protocol is secure against a quantum adversary, that is, it acts on classical registers Cd_{in} and outputs Cd_{out} without revealing any other information to the dishonest parties. In particular, if sender and receiver are honest, it does not leak their identity.

Let $\xi^{(1)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}}}$ be the global output state after collision detection (Step 1). Ass. 2 implies that tracing out the registers of honest parties (all registers of $\bar{A}$) we obtain a partial state of the adversary (all registers of A) which is independent of the sender, if the sender is honest. That is, for all honest parties, $\forall i \notin \mathscr{A}$, the state after the collision detection step (Step 1 of Protocol 1) is

$$\begin{aligned} \text{Tr}_{\bar{A}_0 Cd^{\bar{A}}_{\text{in}} Cd^{\bar{A}}_{\text{out}} Rn^{\bar{A}}_{\text{in}}} \left((\xi^{(1)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}}|S=i} \right) &= \xi^{(1)}_{A_0 Cd^A_{\text{in}} Cd^A_{\text{out}} Rn^A_{\text{in}}|S=i} && (3.17) \\ &= \xi^{(1)}_{A_0 Cd^A_{\text{in}} Cd^A_{\text{out}} Rn^A_{\text{in}}}. && (3.18) \end{aligned}$$

STEP 2. RECEIVER NOTIFICATION.

Assumption 3. We assume that the classical receiver notification protocol is secure against the quantum adversary; that is, the protocol acts on the classical register Rn_{in} and outputs Rn_{out}, without revealing any other information to the dishonest parties. In particular, if sender and receiver are honest, it does not leak their identity.

Let the input state to the receiver notification protocol be $\xi^{(1)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}}}$ and the output state conditioned on node i being the sender be $\xi^{(2)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}} Rn_{\text{out}}|S=i}$. Ass. 3 implies that, again, tracing out the registers of honest parties (all registers of $\bar{A}$) we obtain a partial state of the adversary (all registers of A) which is independent of the sender. That is, for all honest parties $\forall i \notin \mathscr{A}$, the state after the receiver notification step (Step 2 of Protocol 1) is

$$\begin{aligned} \text{Tr}_{\bar{A}_0 Cd^{\bar{A}}_{\text{in}} Cd^{\bar{A}}_{\text{out}} Rn^{\bar{A}}_{\text{in}} Rn^{\bar{A}}_{\text{in}} Rn^{\bar{A}}_{\text{out}}} (\xi^{(2)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}} Rn_{\text{out}}|S=i}) &= \xi^{(2)}_{A_0 Cd^A_{\text{in}} Cd^A_{\text{out}} Rn^A_{\text{in}} Rn^A_{\text{out}}|S=i} && (3.19) \\ &= \xi^{(2)}_{A_0 Cd^A_{\text{in}} Cd^A_{\text{out}} Rn^A_{\text{in}} Rn^A_{\text{out}}}. && (3.20) \end{aligned}$$

For clarity, we denote the state after the receiver notification (Step 2), given that node i is the sender, by

$$\xi^{(2)}_{A_0\bar{A}_0 Cd_{\text{in}}Cd_{\text{out}}Rn_{\text{in}}Rn_{\text{out}}|S=i} \equiv \sigma_{D^{\mathscr{A}}D^{\mathscr{H}SR}|S=i} \tag{3.21}$$

where $D^{\mathscr{A}} = \{A_0 Cd^A_{\text{in}} Cd^A_{\text{out}} Rn^A_{\text{in}} Rn^A_{\text{out}}\}$ denotes all the registers in possession of the adversary at the end of Step 2. And similarly, $D^{\mathscr{H}SR}$ denotes the registers of the honest parties. Note that, now that sender S and receiver R are defined, we distinguish them from the subset of honest players.

Lemma 3. *If S and R are honest, the state of the adversary at the end of the receiver notification protocol does not carry any information about their identity. Let* $\sigma_{D^{\mathscr{A}}|S=i} := \text{Tr}_{D^{\mathscr{H}SR}}[\sigma_{D^{\mathscr{A}}D^{\mathscr{H}SR}|S=i}]$*; by Ass. 2 and 3 it holds that*

$$\sigma_{D^{\mathscr{A}}|S=i} = \sigma_{D^{\mathscr{A}}|S=j} = \sigma_{D^{\mathscr{A}}} \quad \forall\, i,j \notin \mathscr{A}, \tag{3.22}$$

and

$$\sigma_{D^{\mathscr{A}}|R=i} = \sigma_{D^{\mathscr{A}}|R=j} = \sigma_{D^{\mathscr{A}}} \quad \forall\, i,j \notin \mathscr{A}. \tag{3.23}$$

STEP 3. STATE DISTRIBUTION.

Assumption 4. The N-partite state distributed by a trusted source is $|\text{W}\rangle\langle\text{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R}$. Here $W^{\mathscr{H}}$ is the *quantum* register of the honest parties, $W^{\mathscr{A}}$ is the *quantum* register of dishonest parties, and W^S and W^R are *quantum* registers of the sender and receiver.

Therefore, the global state after the source distributed the quantum state (Step 3 of Protocol 1) is

$$\xi^{(3)}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RD^{\mathscr{A}}D^{\mathscr{H}SR}|S=i} = |\text{W}\rangle\langle\text{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R} \otimes \sigma_{D^{\mathscr{A}}D^{\mathscr{H}SR}|S=i}. \tag{3.24}$$

STEP 4. MEASUREMENT.

Step 4 describes a measurement on quantum registers $W^{\mathscr{H}}W^{\mathscr{A}}$ and creates the classical registers $O^{\mathscr{H}}_{\text{in}}$ and $O^{\mathscr{A}}_{\text{in}}$. The honest parties perform a projection $\Pi^{\vec{\nu}}_{W^{\mathscr{H}}}$ on the $\{0,1\}$ basis and the string of outcomes $\vec{\nu}$ is recorded on register $O^{\mathscr{H}}_{\text{in}}$. The adversaries, however, instead of performing the measurement specified by the protocol, can apply an arbitrary map on their registers and produce a classical outcome $|\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathscr{A}}_{\text{in}}}$. This action is descried by applying a map $\mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}D^{\mathscr{A}}}$ labeled by $\vec{\mu}$, which acts on registers $W^{\mathscr{A}}D^{\mathscr{A}}$ and producing a classical outcome $|\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathscr{A}}_{\text{in}}}$ in register $O^{\mathscr{A}}_{\text{in}}$. Note that this outcome can be a strategy upon which dishonest parties agree and, in particular, it does not have to represent the actual action of the map $\mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}D^{\mathscr{A}}}$. Therefore, the state after the parties perform local measurements (Step 4 of Protocol 1) is described as,

$$\xi^{(4)}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RD^{\mathscr{A}}D^{\mathscr{H}SR}O^{\mathscr{H}}_{\text{in}}O^{\mathscr{A}}_{\text{in}}|S=i} = \sum_{\vec{\mu},\vec{\nu}} \Pi^{\vec{\nu}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(|\text{W}\rangle\langle\text{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R} \otimes \sigma_{D^{\mathscr{A}}D^{\mathscr{H}SR}|S=i}) \otimes |\vec{\nu}\rangle\langle\vec{\nu}|_{O^{\mathscr{H}}_{\text{in}}} \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathscr{A}}_{\text{in}}}, \tag{3.25}$$

where $\Pi^{\vec{\nu}}_{W^{\mathscr{H}}}$ corresponds to a projection of register $W^{\mathscr{H}}$ onto the state $|\vec{\nu}\rangle\langle\vec{\nu}|$ in the standard basis.

STEP 5. ANONYMOUS ANNOUNCEMENT OF OUTCOMES.
Each of the parties inputs their measurement outcome into the veto protocol. In particular, $O_{\text{in}}^{\mathcal{H}} = |\vec{\nu}\rangle\langle\vec{\nu}|_{O_{\text{in}}^{\mathcal{H}}}$ is a private input of the honest parties and $O_{\text{in}}^{\mathcal{A}} = \left|\vec{\mu}\right\rangle\left\langle\vec{\mu}\right|_{O_{\text{in}}^{\mathcal{A}}}$ is a private input of the dishonest parties.

Assumption 5. We assume that the classical veto protocol is secure against the quantum adversary; i.e., the veto protocol acts on the classical registers $O_{\text{in}}^{\mathcal{H}}, O_{\text{in}}^{\mathcal{A}}$, and only outputs $O_{\text{out}} = 0$ if $O_{\text{in}}^{\mathcal{H}} = O_{\text{in}}^{\mathcal{A}} = \left|\vec{0}\right\rangle\left\langle\vec{0}\right|$ and 1 otherwise, and does not reveal any other information.

Then, the state after the veto protocol, where the parties announce their outcomes (Step 5 of Protocol 1), is

$$\begin{aligned}\xi^{(5)}_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^RD^{\mathcal{H}\mathcal{A}SR}O_{\text{in}}^{\mathcal{H}}O_{\text{in}}^{\mathcal{A}}O_{\text{out}}|S=i} =& \Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^R} \otimes \sigma_{D^{\mathcal{A}}D^{\mathcal{H}}SR|S=i}) \\ & \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_{O_{\text{in}}^{\mathcal{H}}} \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_{O_{\text{in}}^{\mathcal{A}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \\ & + \sum_{\vec{\mu}\neq 0,\vec{\nu}} \Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathscr{F}^{\vec{\mu}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^R} \otimes \sigma_{D^{\mathcal{A}}D^{\mathcal{H}}SR|S=i}) \\ & \otimes |\vec{\nu}\rangle\langle\vec{\nu}|_{O_{\text{in}}^{\mathcal{H}}} \otimes \left|\vec{\mu}\right\rangle\left\langle\vec{\mu}\right|_{O_{\text{in}}^{\mathcal{A}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}} \end{aligned} \tag{3.26}$$

STEP 6. TELEPORTATION.
In Step 6., sender and receiver wish to perform the teleportation. To do so, the sender performs the Bell state measurement and communicates the classical outcome to the receiver, so that she can correct the teleported state. The classical communication is carried out by using the classical protocol logical OR.

Assumption 6. The classical logical OR protocol acts on classical registers and does not reveal any information other than the logical OR of the inputs.

Let Q denote the register of the quantum message which sender S wishes to transmit. More formally, this step consists of applying a map, a Bell state measurement, acting on the registers of the sender W^S and Q and producing a classical message in the public register T, followed by the receiver applying a unitary operation according to the outcome m of the Bell measurement. We denote the map that describes the teleportation step by $\mathcal{T}_{W^SW^RQO_{\text{out}}\to W^SW^RQO_{\text{out}}T_{\text{in}}^ST_{\text{in}}^RT}$. Its action is conditioned on the outcome of Step 5., i.e., public output of the veto protocol. We define its action on a state $\phi_{W^SW^R} \otimes \left|\psi\right\rangle\left\langle\psi\right|_Q$ as follows,

$$\begin{aligned}\mathcal{T}_{W^SW^RQ|O_{\text{out}}=0\to W^SW^RQO_{\text{out}}T_{\text{in}}^ST_{\text{in}}^RT} :=& \sum_m \mathscr{R}^m_{W^R} \circ \mathscr{B}^m_{W^SQ}(\phi_{W^SW^R} \otimes \left|\psi\right\rangle\left\langle\psi\right|_Q) \\ & \otimes \sum_{\text{rand}} \frac{1}{4} |m\rangle\langle m|_{T_{\text{in}}^S} \otimes |\text{rand}\rangle\langle\text{rand}|_{T_{\text{in}}^R} \otimes |m\oplus\text{rand}\rangle\langle m\oplus\text{rand}|_T\,, \end{aligned} \tag{3.27}$$

$$\mathcal{T}_{W^SW^RQ|O_{\text{out}}=1\to W^SW^RQO_{\text{out}}T_{\text{in}}^ST_{\text{in}}^RT} := \mathbb{1}_{W^SW^RQ}(\phi_{W^SW^R} \otimes \left|\psi\right\rangle\left\langle\psi\right|_Q) \tag{3.28}$$

$$\otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^S} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^R} \otimes |\perp\rangle\langle\perp|_T\,. \tag{3.29}$$

The map $\mathscr{B}^m_{W^S Q}$ represents the Bell state measurement, on registers $W^S Q$, with outcome m, and the map $\mathscr{R}^m_{W^R}$ corresponds to the unitary the receiver applies to correct the teleported state. The action of the map $\mathscr{T}_{W^S W^R Q O_{\text{out}} \to W^S W^R Q O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T}$ describes that the state $|\psi\rangle\langle\psi|_Q$ is either teleported to register W^R when $O_{\text{out}} = 0$ or the protocol aborts when $O_{\text{out}} = 1$, which we represent by the state $|\perp\rangle\langle\perp|_T$ in register T.

However, we note that in this step the adversaries could also deviate from the protocol. In general, they could perform an arbitrary map in their registers and input a string $\vec{\kappa} \neq \vec{0}$ to the logical OR protocol. In that case, the teleportation step can be described as

$$\begin{aligned}
&\mathscr{T}_{W^S W^R W^{\mathscr{A}} D^{\mathscr{A}} Q | O_{\text{out}}=0 \to W^S W^R W^{\mathscr{A}} D^{\mathscr{A}} Q O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T^{\mathscr{A}}_{\text{in}} T}(\xi^{(5)}_{W^{\mathscr{H}} W^{\mathscr{A}} W^S W^R Q D^{\mathscr{H}\mathscr{A}SR} O^{\mathscr{H}}_{\text{in}} O^{\mathscr{A}}_{\text{in}} O_{\text{out}} | S=i}) := \\
&\sum_{m,\vec{\kappa}} \mathscr{R}^{m \oplus_i \kappa_i}_{W^R} \circ \mathscr{G}^{\vec{\kappa}}_{W^{\mathscr{A}} D^{\mathscr{A}}} \circ \mathscr{B}^m_{W^S Q}(\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}} D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}} W^{\mathscr{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}} D^{\mathscr{H}SR} | S=i})) \\
&\otimes \sum_{\text{rand}} \frac{1}{4} |m\rangle\langle m|_{T^S_{\text{in}}} \otimes |\text{rand}\rangle\langle\text{rand}|_{T^R_{\text{in}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\text{in}}} \otimes |m \oplus \text{rand} \oplus_i \kappa_i\rangle\langle m \oplus \text{rand} \oplus_i \kappa_i|_T
\end{aligned} \tag{3.30}$$

where $\mathscr{G}^{\vec{\kappa}}_{W^{\mathscr{A}} D^{\mathscr{A}}}$ represents an arbitrary map the adversaries apply to registers $W^{\mathscr{A}} D^{\mathscr{A}}$, which is followed by the creation of classical register $T^{\mathscr{A}}_{\text{in}}$. $\mathscr{R}^{m \oplus_i \kappa_i}_R$ expresses the fact that the receiver now applies a unitary labeled by $m \oplus_i \kappa_i$ instead of m.

Note that the map $\mathscr{G}^{\vec{\kappa}}_{W^{\mathscr{A}} D^{\mathscr{A}}}$ only acts on the registers of the adversaries and after the teleportation step (Step 6) no other operations are performed by the honest parties. The security of the protocol is defined in terms of the guessing probability, which takes into account an optimization over all maps on the register of the adversary. Therefore, for the security analysis, we can, without loss of generality, neglect the map $\mathscr{G}^{\vec{\kappa}}_{AD^{\mathscr{A}}}$ in the final state, since it is taken into account in the definition of the guessing probability.

Finally, the state after the teleportation protocol (Step 6 of Protocol 1) is

$$\begin{aligned}
&\xi^{(6)}_{W^{\mathscr{H}} W^{\mathscr{A}} W^S W^R Q D^{\mathscr{H}\mathscr{A}SR} O^{\mathscr{H}}_{\text{in}} O^{\mathscr{A}}_{\text{in}} O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T^{\mathscr{A}}_{\text{in}} T | S=i} = \\
&\quad \sum_{m,\vec{\kappa}} \mathscr{R}^{m \oplus_i \kappa_i}_{W^R} \circ \mathscr{B}^m_{W^S Q}(\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}} D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}} W^{\mathscr{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}} D^{\mathscr{H}SR} | S=i})) \\
&\qquad \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{H}}_{\text{in}}} \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{A}}_{\text{in}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \\
&\qquad \otimes \sum_{\text{rand}} \frac{1}{4} |m\rangle\langle m|_{T^S_{\text{in}}} \otimes |\text{rand}\rangle\langle\text{rand}|_{T^R_{\text{in}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\text{in}}} \otimes |m \oplus \text{rand} \oplus_i \kappa_i\rangle\langle m \oplus \text{rand} \oplus_i \kappa_i|_T \\
&+ \sum_{\vec{\mu} \neq 0, \vec{\nu}} \mathbb{1}_{W^S W^R Q}(\Pi^{\vec{\nu}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}} D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}} W^{\mathscr{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}} D^{\mathscr{H}SR} | S=i})) \\
&\qquad \otimes |\vec{\nu}\rangle\langle\vec{\nu}|_{O^{\mathscr{H}}_{\text{in}}} \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathscr{A}}_{\text{in}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}} \otimes |\perp\rangle\langle\perp|_{T^S_{\text{in}}} \otimes |\perp\rangle\langle\perp|_{T^R_{\text{in}}} \otimes |\perp\rangle\langle\perp|_{T^{\mathscr{A}}_{\text{in}}} \otimes |\perp\rangle\langle\perp|_T .
\end{aligned} \tag{3.31}$$

Observe, however, that the classical registers $D^{\mathscr{H}SR}, O^{\mathscr{H}}_{\text{in}}, T^S_{\text{in}} T^R_{\text{in}}$ are not further acted upon with any map. Moreover, their content is private, as by Lemma 3 and Ass. 5 and 6 no information about it is revealed to the adversary. Since we are interested in the information available to the adversary we will trace out these subsystems.

Lemma 4. *Let $C = \{D^{\mathscr{A}}, O_{\text{in}}^{\mathscr{A}}, O_{\text{out}}, T_{\text{in}}^{\mathscr{A}}, T\}$ represent all the classical and quantum side information accessible to the adversary at the end of the protocol. The reduced output state of the anonymous transmission protocol with the W state, where we trace out all private information of the honest parties $\mathscr{H}$, S, and R, given that node i is the sender, can be described as follows,*

$$\begin{aligned}\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S}W^{R}QC|S=i} = \sum_{m,\vec{\kappa}} \mathscr{R}_{W^R}^{m\oplus_i\kappa_i} \circ \mathscr{B}_{W^SQ}^{m}(\Pi_{W^{\mathscr{H}}}^{\vec{0}} \otimes \mathscr{F}_{W^{\mathscr{A}}D^{\mathscr{A}}}^{\vec{0}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S}W^{R}} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}}}))\\ \otimes |\vec{0}\rangle\langle\vec{0}|_{O_{\text{in}}^{\mathscr{A}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T_{\text{in}}^{\mathscr{A}}} \otimes \frac{\mathbb{1}_T}{4}\\ + \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathbb{1}_{W^SW^RQ}(\Pi_{W^{\mathscr{H}}}^{\vec{\nu}} \otimes \mathscr{F}_{W^{\mathscr{A}}D^{\mathscr{A}}}^{\vec{\mu}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S}W^{R}} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}}}))\\ \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O_{\text{in}}^{\mathscr{A}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^{\mathscr{A}}} \otimes |\perp\rangle\langle\perp|_T \qquad (3.32)\end{aligned}$$

where we made use of Lemma 3 and the explicitly wrote that the state of register T is maximally mixed.

In summary, Lemma 4 represents the state at the end of the protocol, given that the adversaries might have acted arbitrarily in Step 4 and under the assumption that, in particular, the classical protocols do not reveal the identities of the sender and the receiver. We will use this state to prove security in the following section.

3.6.3. SECURITY ANALYSIS

SEMIACTIVE ADVERSARY

In this section we show that Protocol 1 is sender-secure. The key point of the proof is that security follows from permutational invariance of the state. Before proving Theorem 1, we first prove the following useful lemma.

Lemma 5. *The reduced quantum state of the adversary at the end of the protocol is independent of the sender, i.e., $\forall\, i \notin \mathscr{A}$,*

$$\rho_{W^{\mathscr{A}}C|S=i} = \rho_{W^{\mathscr{A}}C}. \qquad (3.33)$$

Proof. Let us first consider the case where the receiver is not an adversary, $R \notin \mathscr{A}$.

By tracing out we have that

$$\rho_{W^{\mathscr{A}}C|S=i} = \mathrm{Tr}_{W^{\mathscr{H}}W^{S}W^{R}Q}[\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S}W^{R}QC|S=i}], \qquad (3.34)$$

where $\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S}W^{R}QC|S=i}$ is the total state at the end of the protocol (3.32), Lemma 4, given that i is the sender. Since $\mathscr{R}_{W^R}^{m\oplus_i\kappa_i}$ and $\sum_m \mathscr{B}_{W^SQ}^{m}$ are CPTP, they do not change the trace and thus we can write the first part of Eq. (3.32) as

$$
\begin{aligned}
&\mathrm{Tr}_{W^{\mathscr{H}}W^S W^R Q}\Big[\sum_{m,\vec{\kappa}} \mathscr{R}^{m\oplus_i \kappa_i}_{W^R} \circ \mathscr{B}^{m}_{W^S Q}(\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}}}))\\
&\qquad \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4}\Big]\\
&= \mathrm{Tr}_{W^{\mathscr{H}}W^S W^R Q}\Big[\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}}})\\
&\qquad \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes \sum_{\vec{\kappa}} |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4}\Big]\\
&= \mathrm{Tr}_{W^{\mathscr{H}}}\Big[\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(\tilde{W}_{W^{\mathscr{H}}W^{\mathscr{A}}} \otimes \sigma_{D^{\mathscr{A}}})\Big] \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes \sum_{\vec{\kappa}} |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4}
\end{aligned}
\tag{3.35}
$$

where $\tilde{W}_{W^{\mathscr{H}}W^{\mathscr{A}}}$ is the reduced W state on registers $W^{\mathscr{H}}$ and $W^{\mathscr{A}}$ after tracing out W^S and W^R, i.e. $\tilde{W}_{W^{\mathscr{H}}W^{\mathscr{A}}} = \mathrm{Tr}_{W^S W^R}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^S W^R})$, and similarly for the second term of (3.32). So,

$$
\begin{aligned}
\rho_{W^{\mathscr{A}}C|S=i} = &\mathrm{Tr}_{W^{\mathscr{H}}}\Big[\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(\tilde{W}_{W^{\mathscr{H}}W^{\mathscr{A}}} \otimes \sigma_{D^{\mathscr{A}}})\Big]\\
&\otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes \sum_{\vec{\kappa}} |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4}\\
&+ \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathrm{Tr}_{W^{\mathscr{H}}}\Big[\Pi^{\vec{\nu}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(\tilde{W}_{W^{\mathscr{H}}W^{\mathscr{A}}} \otimes \sigma_{D^{\mathscr{A}}})\Big]\\
&\otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathscr{A}}_{\mathrm{in}}} \otimes |1\rangle\langle 1|_{O_{\mathrm{out}}} \otimes |\perp\rangle\langle\perp|_{T^{\mathscr{A}}_{\mathrm{in}}} \otimes |\perp\rangle\langle\perp|_T
\end{aligned}
$$

But since the state distributed by the source is permutationally invariant, it holds that

$$
\tilde{W}_{W^{\mathscr{H}}W^{\mathscr{A}}} = \mathrm{Tr}_{W^{S=i}W^R}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S=i}W^R}) = \mathrm{Tr}_{W^{S=j}W^R}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^{S=j}W^R}),\ \forall i,j \notin \mathscr{A}
\tag{3.36}
$$

Since no other part of the state $\rho_{W^{\mathscr{A}}C|S=i}$ depends on the sender, the state $\rho_{W^{\mathscr{A}}C|S=i}$ must be the same for all senders and we denote $\rho_{W^{\mathscr{A}}C|S=i} = \rho_{W^{\mathscr{A}}C}$. Note that the same statement holds when the receiver is honest since,

$$
\mathrm{Tr}_{W^S W^{R=i}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^S W^{R=i}}) = \mathrm{Tr}_{W^S W^{R=j}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^S W^{R=j}}), \quad \forall i,j \notin \mathscr{A}
\tag{3.37}
$$

and, therefore, $\rho_{W^{\mathscr{A}}C|R=i} = \rho_{W^{\mathscr{A}}C}$.

Now we proceed to the proof of this statement in the case where the receiver is an adversary.

If the receiver is dishonest then the teleportation map has to take into account the fact that the adversaries can apply an arbitrary map instead of $\mathscr{R}^{m\oplus_i\kappa_i}_{W^R}$. Also, now the output of the teleportation m is known to the adversaries and the map $\mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}D^{\mathscr{A}}}$ could initially also act on the receiver's register. Now we can model the action of the receiver after receiving m by an arbitrary map that acts on all the registers in possession of the

adversaries, i.e., $\mathscr{R}^{m\oplus_i\kappa_i}_{W^R} \longrightarrow \mathscr{R}'_{W^{\mathscr{A}}W^RCT^{\mathscr{A}}_{\text{in}}T}$ and instead of (3.32), the final state of the protocol is described by

$$\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQC|S=i} = \mathscr{R}'_{W^{\mathscr{A}}W^RCT^{\mathscr{A}}_{\text{in}}T} \circ \tag{3.38}$$

$$\circ\Big(\sum_{m,\vec{\kappa}} \mathscr{B}^m_{W^SQ}(\Pi^{\vec{0}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{0}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}}}))$$

$$\otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathscr{A}}_{\text{in}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathscr{A}}_{\text{in}}} \otimes |m\rangle\langle m|_T\Big)$$

$$+ \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathbb{1}_{W^SW^RQ} \circ (\Pi^{\vec{\nu}}_{W^{\mathscr{H}}} \otimes \mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}D^{\mathscr{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathscr{A}}}))$$

$$\otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathscr{A}}_{\text{in}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}} \otimes |\perp\rangle\langle\perp|_{T^{\mathscr{A}}_{\text{in}}} \otimes |\perp\rangle\langle\perp|_T \tag{3.39}$$

Let us look at the reduced final state of the adversary, which now includes the receiver, $\rho_{W^{\mathscr{A}}W^RC|S=i} = \mathrm{Tr}_{W^{\mathscr{H}}W^SQ}[\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQC|S=i}]$. By the permutational invariance of the state generated by the source we have that the state at the end of the protocol given that node i is the sender is equivalent to the state given that node j is the sender up to a permutation of i and j,

$$\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQC|S=i} = \mathscr{P}_{i\leftrightarrow j}(\rho_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQC|S=j}). \tag{3.40}$$

Therefore tracing out the sender and the other honest parties, the remaining states are equal

$$\rho_{W^{\mathscr{A}}W^RC|S=i} = \rho_{W^{\mathscr{A}}W^RC|S=j}, \tag{3.41}$$

which proves anonymity of the sender even if the receiver is dishonest.

□

Proof Theorem 1 (sender security). Here we focus on proving sender security. The receiver security is formally stated in Theorem 10G. iven Lemma 5, we have that

$$P_{\text{guess}}[S|W^{\mathscr{A}},C,S\notin\mathscr{A}] = \max_{\{M^i\}}\sum_{i\in[N]} P[S=i|S\notin\mathscr{A}]\,\mathrm{Tr}\Big[M^i\cdot\rho_{W^{\mathscr{A}}C|S=i}\Big] \tag{3.42}$$

$$= \max_{\{M^i\}}\sum_{i\in[N]} P[S=i|S\notin\mathscr{A}]\,\mathrm{Tr}\Big[M^i\cdot\rho_{W^{\mathscr{A}}C}\Big] \tag{3.43}$$

$$\leq \max_i P[S=i|S\notin\mathscr{A}]\max_{\{M^i\}}\mathrm{Tr}\Big[\underbrace{\sum_{i\in[N]} M^i}_{\mathbb{1}_{W^{\mathscr{A}}C}}\cdot\rho_{W^{\mathscr{A}}C}\Big] \tag{3.44}$$

$$= \max_i P[S=i|S\notin\mathscr{A}] \tag{3.45}$$

□

Analogously, we will prove the following statement for the receiver-security.

Theorem 10 (receiver security)**.** *The anonymous transmission protocol, Protocol 1, with the W state is receiver-secure in the semiactive adversary scenario, i.e.*

$$\max_{\{M^i\}} \sum_{i\in[N]} P[R=i|W^{\mathscr{A}},C,R\notin\mathscr{A}]\,\mathrm{Tr}\Big[M^i\cdot\rho_{W^{\mathscr{A}}C|R=i}\Big] \leq \max_i P[R=i|R\notin\mathscr{A}], \tag{3.46}$$

given that the receiver is honest.

Proof. By the proof of Lemma 5, it follows that the reduced quantum state of the adversary at the end of the protocol is independent of the receiver, i.e., $\rho_{W^{\mathscr{A}}C|R=i} = \rho_{W^{\mathscr{A}}C}, \forall\, i \notin \mathscr{A}$. Therefore,

$$P_{\text{guess}}[R|W^{\mathscr{A}},C,R\notin\mathscr{A}] = \max_{\{M^i\}} \sum_{i\in[N]} P[R=i|R\notin\mathscr{A}]\,\mathrm{Tr}\Big[M^i\cdot\rho_{W^{\mathscr{A}}C|R=i}\Big] \tag{3.47}$$

$$\leq \max_i P[R=i|R\notin\mathscr{A}] \max_{\{M^i\}} \mathrm{Tr}\Big[\underbrace{\sum_{i\in[N]} M^i}_{\mathbb{1}_{W^{\mathscr{A}}C}}\cdot\rho_{W^{\mathscr{A}}C}\Big] \tag{3.48}$$

$$= \max_i P[R=i|R\notin\mathscr{A}] \tag{3.49}$$

□

PASSIVE ADVERSARY

Definition 13. Let $\mathscr{H}$ be the subset of honest players, excluding S and R, and $\mathscr{A}$ be the subset of passive adversaries. Let C be the register that contains all classical information accessible to the adversaries, i.e., the public outputs of the classical subprotocols, plus all the inputs and outputs of the adversaries to these classical subprotocols, $C = \{D^{\mathscr{A}}, O_{\text{in}}^{\mathscr{A}}, O_{\text{out}}, T_{\text{in}}^{\mathscr{A}}, T\}$. Then probability of the adversaries guessing the sender is given by

$$P_{\text{guess}}[S|W^{\mathscr{A}},C,S\notin\mathscr{A}] = \sum_{a,c} P[W^{\mathscr{A}}=a,C=c] \max_{i\in[N]} P[S=i|W^{\mathscr{A}}=a,C=c,S\notin\mathscr{A}], \tag{3.50}$$

where maximization is taken over all the values of random variable S, and a and c are possible values of random variables $W^{\mathscr{A}}$ and C respectively. Note that, unlike before, here $W^{\mathscr{A}}$ is a classical register of the adversary, since their share of the W state was measured in the $\{0,1\}$ basis. An analogous expression holds for receiver-security.

The proof for the passive adversary security scenario is a special case of the proof for the semiactive adversary scenario. Indeed, it corresponds to the case where the arbitrary map of the adversary, $\mathscr{F}^{\vec{\mu}}_{W^{\mathscr{A}}\mathscr{D}^{\mathscr{A}}}$, is a measurement in the $\{|0\rangle,|1\rangle\}$ basis and $T_{\text{in}}^{\mathscr{A}} = \vec{0}$. Let us first prove the following lemma.

Lemma 6. *The probability of registers $W^{\mathscr{A}}$ and C assuming certain values a and c is independent of the sender,*

$$P[W^{\mathscr{A}}=a,C=c|S=i,S\notin\mathscr{A}] = P[W^{\mathscr{A}}=a,C=c] \tag{3.51}$$

Proof. In the passive adversary scenario, the dishonest parties follow the protocol, therefore the map $\mathscr{F}^{\vec{0}}_{W^{\mathscr{A}}D^{\mathscr{A}}}$ is replaced by a projector onto the $|\vec{0}\rangle\langle\vec{0}|_{W^{\mathscr{A}}}$ subspace, i.e. $\Pi^{\vec{0}}_{W^{\mathscr{A}}}$. By the permutational invariance argument the state, in this case classical, is independent of the sender S (or the receiver R), which completes the proof. □

Proof of Theorem 2. Let us expand the probability appearing in the security definition (3.50)

$$P[S=i|W^{\mathscr{A}}=a,C=c,S\notin\mathscr{A}]=\frac{P[W^{\mathscr{A}}=a,C=c|S=i,S\notin\mathscr{A}]P[S=i|S\notin\mathscr{A}]}{P[W^{\mathscr{A}}=a,C=c]} \tag{3.52}$$

$$=\frac{P[W^{\mathscr{A}}=a,C=c|S=i]P[S=i|S\notin\mathscr{A}]}{P[W^{\mathscr{A}}=a,C=c]} \tag{3.53}$$

$$=P[S=i|S\notin\mathscr{A}] \tag{3.54}$$

where in (3.53) we used Lemma 6. Therefore, (3.50) becomes,

$$P_{\text{guess}}[S|W^{\mathscr{A}},C,S\notin\mathscr{A}]=\sum_{a,c}P[W^{\mathscr{A}}=a,C=c]\max_{i\in[N]}P[S=i|S\notin\mathscr{A}] \tag{3.55}$$

$$=\max_{i\in[N]}P[S=i|S\notin\mathscr{A}]. \tag{3.56}$$

□

3.7. TECHNICAL STATEMENTS - NOISY QUANTUM NETWORK

3.7.1. PROOF FOR ε-SECURITY

Here we provide a proof of Theorem 4 for ε-sender security.

Proof of Theorem 4. The idea of our proof is to show that, for all i, the trace $\mathrm{Tr}\left[M^i\cdot\hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]$ can be upper-bounded by $\mathrm{Tr}\left[M^i\cdot\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]+N\varepsilon_{\max}$. Then using the fact that $N\varepsilon_{\max}$ is independent of i, the rest of the proof follows from Theorem 3.

Let us look at the following expression, $\forall i$,

$$\begin{aligned}&\left|\mathrm{Tr}\left[M^i\hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]-\mathrm{Tr}\left[M^i\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]\right|\\&\leq\left\|\hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}-\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right\|_1 \qquad (3.57)\\&\leq\left\|\xi'^{\Lambda\ (6)}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQD^{\mathscr{H}\mathscr{A}SR}O^{\mathscr{H}}_{\text{in}}O^{\mathscr{A}}_{\text{in}}O_{\text{out}}T^S_{\text{in}}T^R_{\text{in}}T^{\mathscr{A}}_{\text{in}}T|S=i}-\xi^{\Lambda\ (6)}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQD^{\mathscr{H}\mathscr{A}SR}O^{\mathscr{H}}_{\text{in}}O^{\mathscr{A}}_{\text{in}}O_{\text{out}}T^S_{\text{in}}T^R_{\text{in}}T^{\mathscr{A}}_{\text{in}}T|S=i}\right\|_1,\end{aligned}$$

where $\xi'^{\Lambda\ (6)}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQD^{\mathscr{H}\mathscr{A}SR}O^{\mathscr{H}}_{\text{in}}O^{\mathscr{A}}_{\text{in}}O_{\text{out}}T^S_{\text{in}}T^R_{\text{in}}T^{\mathscr{A}}_{\text{in}}T|S=i}$ and $\xi^{\Lambda\ (6)}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^RQD^{\mathscr{H}\mathscr{A}SR}O^{\mathscr{H}}_{\text{in}}O^{\mathscr{A}}_{\text{in}}O_{\text{out}}T^S_{\text{in}}T^R_{\text{in}}T^{\mathscr{A}}_{\text{in}}T|S=i}$ are final states of the protocol after Step 6 (defined analogously to equation (3.31)) when the network is perturbed (3.5), or not (3.3), respectively. Since the protocol is described by a CPTP map, the trace distance of the final state is upper-bounded by the trace dis-

tance of the initial state,

$$\begin{aligned}
&\left|\mathrm{Tr}\left[M^i\,\hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]-\mathrm{Tr}\left[M^i\,\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]\right| \\
&\leq \left\|\omega'^{\Lambda}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R}\otimes|\psi\rangle\langle\psi|_Q\otimes\sigma_{D^{\mathscr{H}\mathscr{A}SR}|S=i}-\omega^{\Lambda}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R}\otimes|\psi\rangle\langle\psi|_Q\otimes\sigma_{D^{\mathscr{H}\mathscr{A}SR}|S=i}\right\|_1 && (3.58)\\
&\leq \left\|\omega'^{\Lambda}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R}-\omega^{\Lambda}_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R}\right\|_1 && (3.59)\\
&\leq \left\|\bigotimes_{i=1}^N\Lambda_i(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R})-\Lambda^{\otimes N}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathscr{H}}W^{\mathscr{A}}W^SW^R})\right\|_1 && (3.60)\\
&\leq \left\|\bigotimes_{i=1}^N\Lambda_i-\Lambda^{\otimes N}\right\|_1\leq\sum_{i=1}^N\|\Lambda_i-\Lambda\|_1=\sum_{i=1}^N\varepsilon_i\leq N\varepsilon_{\max} && (3.61)
\end{aligned}$$

where we used the properties of the trace distance and the induced trace norm. Therefore we have that, $\forall i$

$$\mathrm{Tr}\left[M^i\cdot\hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]\leq\mathrm{Tr}\left[M^i\cdot\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]+N\varepsilon_{\max} \tag{3.62}$$

so using Theorem 3,

$$\begin{aligned}
P_{\mathrm{guess}}[S|W^{\mathscr{A}},C,S\notin\mathscr{A}] &= \max_{\{M^i\}}\sum_{i\in[N]}P[S=i|S\notin\mathscr{A}]\,\mathrm{Tr}\left[M^i\cdot\hat{\rho}^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right] && (3.63)\\
&\leq \max_{\{M^i\}}\sum_{i\in[N]}P[S=i|S\notin\mathscr{A}]\left(\mathrm{Tr}\left[M^i\cdot\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right]+N\varepsilon_{\max}\right) && (3.64)\\
&= \max_{\{M^i\}}\sum_{i\in[N]}P[S=i|S\notin\mathscr{A}]\,\mathrm{Tr}\left[M^i\cdot\rho^{\Lambda}_{W^{\mathscr{A}}C|S=i}\right] && (3.65)\\
&\quad+\sum_{i\in[N]}P[S=i|S\notin\mathscr{A}]N\varepsilon_{\max} && (3.66)\\
&\leq \max_{i\in[N]}P[S=i|S\notin\mathscr{A}]+N\varepsilon_{\max}. && (3.67)
\end{aligned}$$

□

The same argument holds for receiver-security.

3.7.2. PERFORMANCE IN A NOISY NETWORK

Fidelity derivation. In general, it is non-trivial to derive analytical expressions for fidelity of anonymous entanglement in the presence of noise. The most troublesome part is to obtain analytical expressions for anonymous entangled states shared between S and R, which are affected by the noise. Nevertheless, to obtain these explicit formulas, we used the fact that the noise is described by a linear map which acts on each qubit individually. We will illustrate the gist of our derivation with an example for the GHZ state, since it is easier to follow than the one for the W state.

As defined in the main text, the state shared by S and R in the noisy case is

$$\gamma_{SR}=\frac{1}{\mathscr{N}'}\,\mathrm{Tr}_{N-2}\left[\Lambda^{\otimes N}(|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_N)\cdot\left|\vec{+}\right\rangle\left\langle\vec{+}\right|_{N-2}\right], \tag{3.68}$$

where $\mathcal{N}$ is the normalization factor. Note that the GHZ state can be written as

$$|\text{GHZ}\rangle\langle\text{GHZ}|_N = \frac{1}{2}\left(|0\rangle\langle 0|^{\otimes N} + |0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N} + |1\rangle\langle 1|^{\otimes N}\right) \tag{3.69}$$

Due to the tensor structure and linearity of the noise, we can write that

$$\begin{aligned}\gamma_{SR} &= \frac{1}{2\mathcal{N}'}\,\text{Tr}_{N-2}\left[\left(\Lambda(|0\rangle\langle 0|)^{\otimes N} + \Lambda(|0\rangle\langle 1|)^{\otimes N} + \Lambda(|1\rangle\langle 0|)^{\otimes N} + \Lambda(|1\rangle\langle 1|)^{\otimes N}\right)\cdot|+\rangle\langle+|^{\otimes N-2}\right] \\ &= \frac{1}{2\mathcal{N}'}\Big(\text{Tr}[\Lambda(|0\rangle\langle 0|)]^{N-2}\Lambda(|0\rangle\langle 0|)^{\otimes 2} + \text{Tr}[\Lambda(|0\rangle\langle 1|)]^{N-2}\Lambda(|0\rangle\langle 1|)^{\otimes 2} \\ &\qquad + \text{Tr}[\Lambda(|1\rangle\langle 0|)]^{N-2}\Lambda(|1\rangle\langle 0|)^{\otimes 2} + \text{Tr}[\Lambda(|1\rangle\langle 1|)]^{N-2}\Lambda(|1\rangle\langle 1|)^{\otimes 2}\Big).\end{aligned} \tag{3.70}$$

This way one only takes the tensor product of the two terms corresponding to S and R, instead of taking the tensor of N terms. The expression for the W state follows the exact same pattern, but one has to account for all the combinations of 0's and 1's occurring in the state $|\text{W}\rangle\langle\text{W}|_N$. Let $\text{tr}_{xy} := \text{Tr}\left[\Lambda(|x\rangle\langle y|)\cdot|0\rangle\langle 0|\right]$ with $x, y = \{0,1\}$. Then the state ω_{SR} shared between S and R in the noisy implementation of Protocol 1 is

$$\begin{aligned}\omega_{SR} = \frac{1}{\mathcal{N}}\Big(&(N-2)(N-3)\text{tr}_{01}\text{tr}_{10}\text{tr}_{00}^{N-4}\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) \\ &+ (N-2)\text{tr}_{10}\text{tr}_{00}^{N-3}\left(\Lambda(|0\rangle\langle 1|)\otimes\Lambda(|0\rangle\langle 0|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 1|)\right) \\ &+ (N-2)\text{tr}_{01}\text{tr}_{00}^{N-3}\left(\Lambda(|1\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|1\rangle\langle 0|)\right) \\ &+ (N-2)\text{tr}_{11}\text{tr}_{00}^{N-3}\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) \\ &+ \text{tr}_{00}^{N-2}\left(\Lambda(|0\rangle\langle 1|)\otimes\Lambda(|1\rangle\langle 0|) + \Lambda(|1\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 1|)\right. \\ &\quad \left.+ \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|1\rangle\langle 1|) + \Lambda(|1\rangle\langle 1|)\otimes\Lambda(|0\rangle\langle 0|)\right)\Big).\end{aligned} \tag{3.71}$$

Using the explicit form of Λ for the depolarizing and dephasing noise, after easy but tedious calculations, one obtains explicit fidelity expressions derived from Eq. (3.12) and (3.13).

Dephasing and depolarizing noise. In this section we provide additional details to the noise analysis provided in the main text. First, we plot the behavior of our protocol vs. the GHZ-based protocol under the dephasing noise, for examples $N = \{4, 10, 50\}$, Figure 3.5. Note that the GHZ state is increasingly useful according to Definition 12 for $q < 0.5$. For anonymous entanglement created with the W state this is always the case, however, for the GHZ only for even N. To observe the same behavior for odd N and the GHZ state one would have to redefine Eq. (3.13) to compare the fidelity with the state $|\phi^-\rangle\langle\phi^-|$.

As discussed, the noise parameter threshold q^* for $N = 182$ nodes becomes larger for the W state: $q^*_W = 0.979057$, $q^*_{GHZ} = 0.979043$, $q^*_W > q^*_{GHZ}$. This means that for $N \geq 182$ the W state tolerates less noise than the GHZ; see Figure 3.6. However, we numerically see that there exists a value of $q > q^*_W$ for which $F_{AE}(\omega_{SR}) > F_{AE}(\gamma_{SR})$. As an example for $N = 400$ see Figure 3.7.

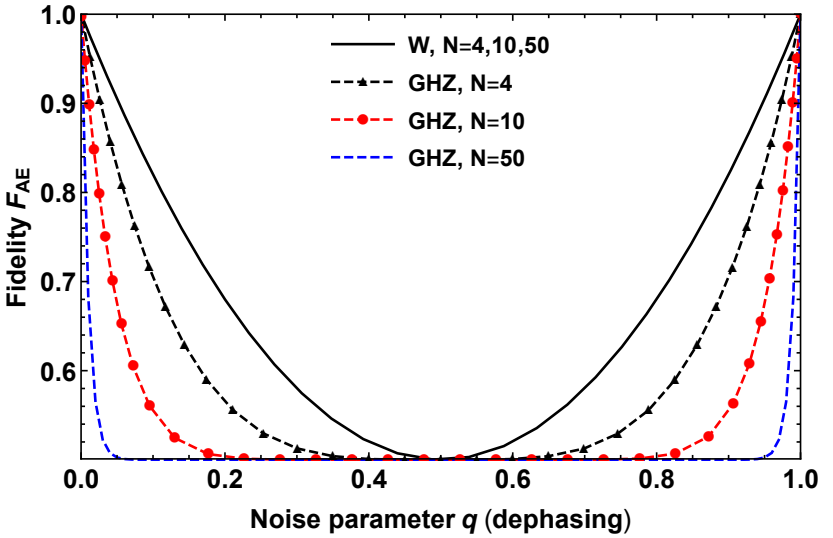


Figure 3.5: Fidelity of anonymous entanglement as a function of the noise parameter for the dephasing channel.

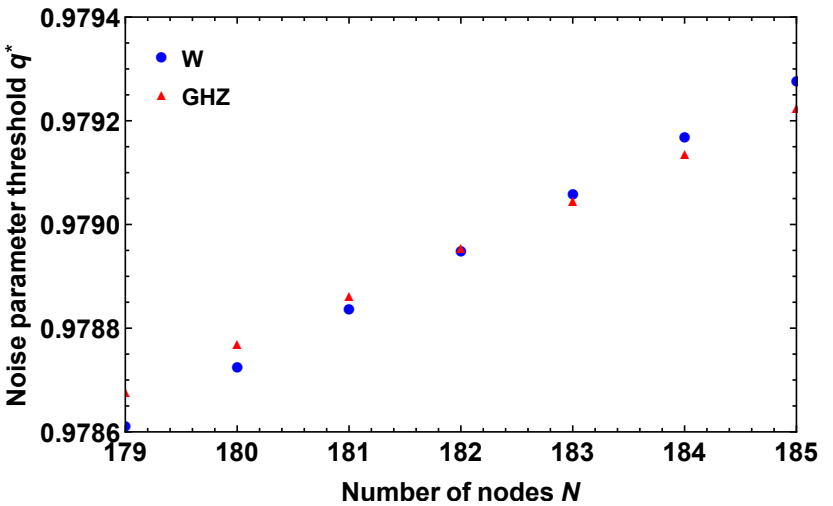


Figure 3.6: Noise parameter threshold for the depolarizing noise. Close-up to $179 \leq N \leq 185$.

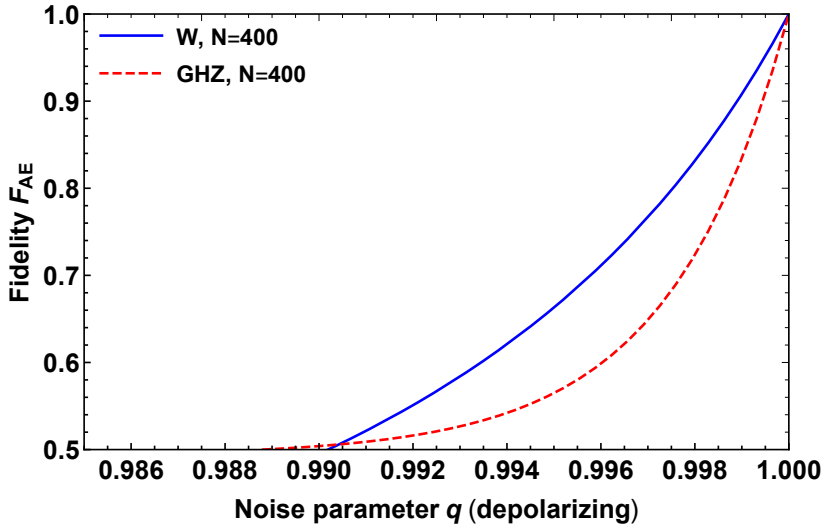


Figure 3.7: Fidelity of anonymous entanglement for $N = 400$.

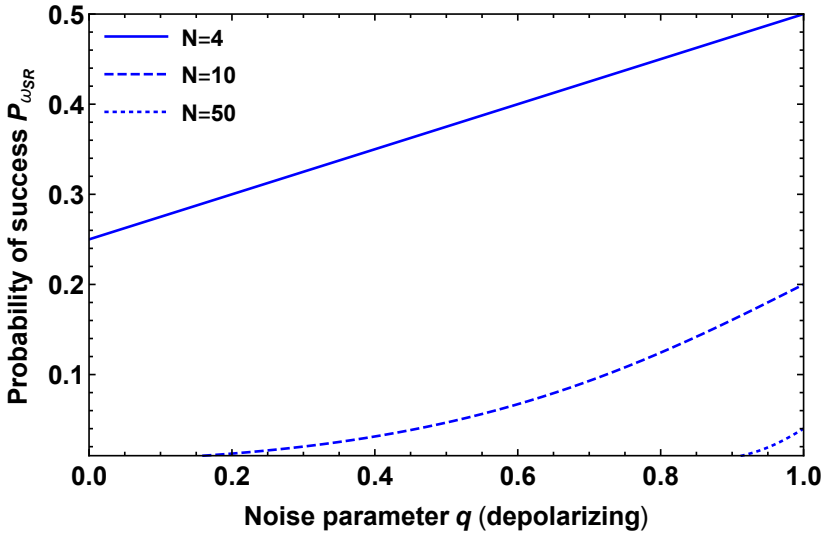


Figure 3.8: Probability of success in Protocol 1 in the presence of the depolarizing noise, $N = \{4, 10, 50\}$.

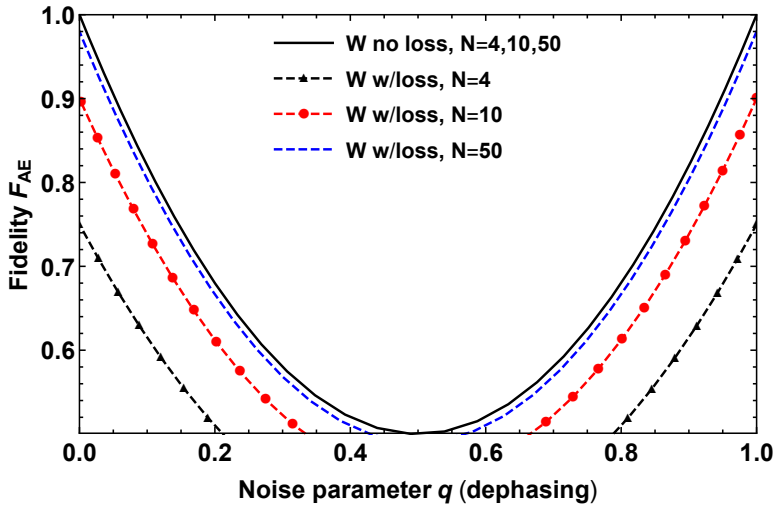


Figure 3.9: Fidelity of anonymous entanglement for Protocol 1, as a function of the noise parameter for the dephasing channel in the presence of one particle loss.

Moreover, we provide an analytical expression for the probability of success in our protocol, defined as $P_{\omega_{SR}} := \mathrm{Tr}\left[\Lambda^{\otimes N}(|\mathrm{W}\rangle\langle\mathrm{W}|_N)\cdot|\vec{0}\rangle\langle\vec{0}|_{N-2}\right]$, which for the depolarizing noise assumes the form,

$$P_{\omega_{SR}} = \frac{(q+1)^{N-3}(N(1-q)+4q)}{N2^{N-2}}. \tag{3.72}$$

Examples of $P_{\omega_{SR}}$ as a function of q for $N = \{4,10,50\}$ are plotted in Figure 3.8. Note that for the dephasing noise $P_{\omega_{SR}} = \frac{2}{N}$, since the measurement basis is not affected by the Z noise.

Particle loss. In the case when one of the particles of the W state is lost and the state is subjected to the network noise, the fidelity of anonymous entanglement can be expressed as

$$F_{AE}(\tilde{\omega}_{SR}) = \frac{(1+q)(N^2(q-1)^2 - 8q^2 + 4Nq(1+q))}{4N(N(1-q)+4q)} \tag{3.73}$$

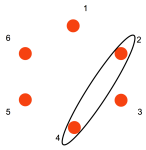
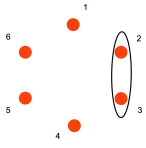
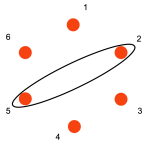
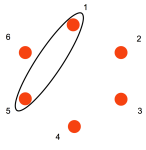
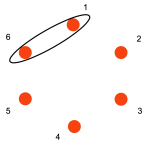
for the depolarizing noise, and

$$F_{AE}(\tilde{\omega}_{SR}) = \frac{N-1}{N}(1-2q(1-q)). \tag{3.74}$$

for the dephasing noise. In Figure 3.9 we plot the examples of F_{AE} for $N = \{4,10,50\}$ when the initial W state is subjected to one particle loss and the dephasing noise.

Relay protocol. Finally, in Tab. 3.2 we present the values for anonymous entanglement in the relay protocol [6] in the presence of the depolarizing noise.

Table 3.2: Fidelity of anonymous entanglement for the relay scheme [6] in the N-fold noisy network for the depolarizing channel. Note that for the depolarizing parameter $q = 0.8$ the anonymous entanglement created between nodes 1 and 6 is not useful in the sense of Definition 12.

Scenario	F_{AE} for $q = 0.8$	F_{AE} for $q = 0.95$
	0.5738	0.8625
	0.6138	0.8744
	0.5418	0.8512
	0.5162	0.8405
	0.4958	0.8303

REFERENCES

[1] F. Stajano and R. Anderson, *The cocaine auction protocol: On the power of anonymous broadcast,* in *Information Hiding,* edited by A. Pfitzmann (Springer Berlin Heidelberg, Berlin, Heidelberg, 2000) pp. 434–447.

[2] D. Chaum, *Untraceable electronic mail, return addresses, and digital pseudonyms,* Commun. ACM **24**, 84 (1981).

[3] M. Christandl and S. Wehner, *Quantum anonymous transmissions,* in *Advances in Cryptology - ASIACRYPT 2005*, edited by B. Roy (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 217–235.

[4] J. Bouda and J. Sprojcar, *Anonymous transmission of quantum information,* in

Quantum, Nano, and Micro Technologies, 2007. ICQNM '07. First International Conference on (2007) pp. 12–12.

[5] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, *Anonymous quantum communication,* in *Advances in Cryptology – ASIACRYPT 2007*, edited by K. Kurosawa (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007) pp. 460–473.

[6] W. Yang, L. Huang, and F. Song, *Privacy preserving quantum anonymous transmission via entanglement relay,* Scientific Reports **6**, 26762 (2016).

[7] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. F. Riedel, P. O. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F. K. Wilhelm, *The quantum technologies roadmap: a european community view,* New Journal of Physics **20**, 080201 (2018).

[8] A. Broadbent and A. Tapp, *Information-theoretic security without an honest majority,* in *Advances in Cryptology – ASIACRYPT 2007*, edited by K. Kurosawa (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007) pp. 410–426.

[9] N. Kalb, *Diamond-based quantum networks with multi-qubit nodes,* Ph.D. thesis (2018).

[10] M. Tomamichel, *A framework for non-asymptotic quantum information theory,* Ph.D. thesis (2012).

[11] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[12] M. Horodecki, P. Horodecki, and R. Horodecki, *General teleportation channel, singlet fraction, and quasidistillation,* Phys. Rev. A **60**, 1888 (1999).

[13] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Quantum privacy amplification and the security of quantum cryptography over noisy channels,* Phys. Rev. Lett. **77**, 2818 (1996).

[14] M. Koashi, V. Bužek, and N. Imoto, *Entangled webs: Tight bound for symmetric sharing of entanglement,* Phys. Rev. A **62**, 050302 (2000).

[15] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, *Multipartite entanglement verification resistant against dishonest parties,* Phys. Rev. Lett. **108**, 260502 (2012).

[16] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, *Self-testing multipartite entangled states through projections onto two systems,* New Journal of Physics **20**, 083041 (2018).

[17] M. Fadel, *Self-testing Dicke states,* (2017), arXiv:quant-ph/1707.01215 .

4

VERIFIABLE HYBRID SECRET SHARING

We consider the task of sharing a secret quantum state in a quantum network in a verifiable way. We propose a protocol that achieves this task, while reducing the number of required qubits, as compared to the existing protocols. To achieve this, we combine classical encryption of the quantum secret with an existing verifiable quantum secret sharing scheme based on Calderbank-Shor-Steane quantum error correcting codes. In this way we obtain a verifiable hybrid secret sharing scheme for sharing qubits, which combines the benefits of quantum and classical schemes. Our scheme does not reveal any information to any group of less than half of the n nodes participating in the protocol. Moreover, for sharing a one-qubit state each node needs a quantum memory to store n single-qubit shares, and requires a workspace of at most $3n$ qubits in total to verify the quantum secret. Importantly, in our scheme an individual share is encoded in a single qubit, as opposed to previous schemes requiring $\Omega(\log n)$ qubits per share. Furthermore, we define a ramp verifiable hybrid scheme. We give explicit examples of various verifiable hybrid schemes based on existing quantum error correcting codes.

This chapter has been published, with minor changes, in V. Lipinska, G. Murta, J. Ribeiro, and S. Wehner, *Verifiable hybrid secret sharing with few qubits*, Phys. Rev. A 101, 032332 (2020).

4.1. INTRODUCTION

Secret sharing is a task, which allows us to securely split a secret message among n network nodes, in such a way that at least a certain number of nodes is asked to collaborate in order to reconstruct the secret. However, one also requires that a subset with less than a certain number of nodes cannot gain any information about the secret. This way one can hide highly confidential and sensitive information from being exposed, for example missile launch codes or numbered bank accounts. The splitting and sharing of the message is often performed by one designated node – the dealer. If the nodes do not trust the dealer, but they want a guarantee that a secret was indeed distributed, then they may wish to verify that at the end of the protocol there will be one well-defined secret that they can reconstruct. In this case, the secret sharing protocol involves an additional step of verification of the shares, and one talks about *verifiable* secret sharing [1, 2].

Importantly, verifiable secret sharing is used as a subroutine for other cryptographic primitives, such as secure multipartite computation [3**?**], byzantine agreement [4], end-to-end auditable voting systems [5] and atomic broadcast [6]. Likewise, a quantum analogue, namely verifiable quantum secret sharing (VQSS), is a core subroutine for secure multiparty quantum computation [7, 8] and fast quantum byzantine agreement [9]. Verifiable schemes, similarly to their non-verifiable counterparts, have the property that they hide information from a certain number of nodes. That is, any subset with p or less nodes does not gain any information about the secret throughout the protocol. We call this property *secrecy*.

So far, many protocols have been proposed for sharing a classical secret using purely classical shares [10–12], using classical and quantum shares [13–16], as well as for sharing a quantum secret with quantum shares [13, 17–21]. This work concerns the last variant, namely schemes which share a quantum secret. Particularly, throughout this chapter we will consider that the dealer shares a pure single-qubit state $|\psi\rangle$. In this scenario, numerous schemes for both non-verifiable quantum secret sharing [13, 17, 18, 20–22] and verifiable quantum secret sharing [7, 23] are known. Fundamentally, for any scheme sharing a quantum secret with only quantum resources, there exists a limit to how many nodes p cannot gain any information about the secret. This limit is given by $p \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ and can be intuitively understood as a consequence of the no-cloning theorem [24]. Indeed, if less than half of the nodes can reconstruct the secret, then there must exist at least two groups of nodes able to reconstruct it, which violates the no-cloning theorem. Moreover, if the majority of nodes recovers the secret exactly, then the remaining nodes get no information about the secret (for more details see [18]). We will refer to schemes which saturate the above bound on p as schemes with *maximum secrecy*. In particular, for VQSS with maximum secrecy, the only current construction [7] requires that the dimension q of local shares scales with the number of nodes, $q > n$. Therefore, using the existing construction, we cannot find a non-trivial example of such a VQSS scheme where the nodes hold single-qubit shares. The reason for this scaling is that, in general, quantum secret sharing schemes are directly connected to resource-intensive quantum error correcting codes [17, 18]. Consequently, this leads to secret sharing schemes which require $\Omega(\log n)$ of qubits per share.

In the area of non-verifiable quantum secret sharing, some investigations have been performed to reduce the number of required qubits, particularly, by exploring ramp se-

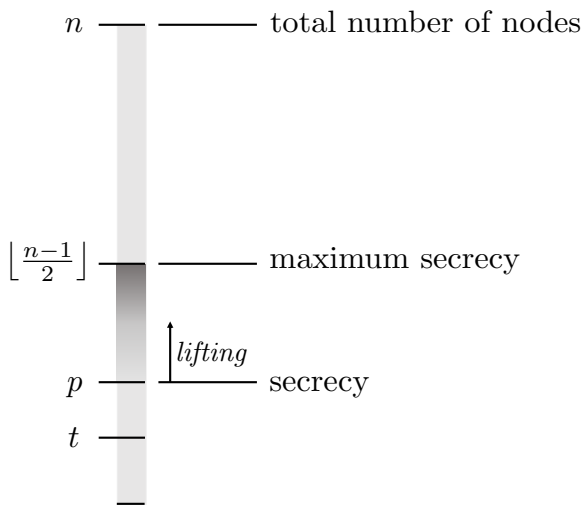


Figure 4.1: Lifting the secrecy of an n-node secret sharing scheme of a quantum state, i.e. increasing the value p of nodes which gain no information about the secret state throughout the execution of the scheme. Here t denotes the number of nodes that can perform arbitrary operations on their shares throughout the protocol, and hence corrupt the secret (active cheaters).

cret sharing schemes [20, 25] and classical encryption. In a ramp scheme one relaxes the constraint on the secrecy of the scheme, and therefore, allows some of the nodes to obtain partial information about the quantum state. This leads to schemes with less qubits per share. Additionally, the secrecy of a ramp scheme can be *lifted*, i.e. the value of p can be increased by encrypting the quantum state and then sharing the encryption key via classical secret sharing, see Figure 4.1. Such a solution was dubbed hybrid secret sharing [26–29].

In early stages of quantum network development, it would be desirable to implement VQSS on a network with ability to control only a small number of qubits. Since quantum resources are expensive, a lot of effort is being put in reducing them in many areas of quantum information field, for example quantum computing or quantum simulation [30–34]. However, reducing the resource requirements in the domain of distributed systems, and in particular verifiable secret sharing, has not been considered so far. Here we address the question of whether a verifiable secret sharing scheme with the maximum secrecy property (i.e. $p = \lfloor \frac{n-1}{2} \rfloor$) can be realized on a quantum network with less qubits. We answer this question positively by presenting a scheme which reduces quantum resources necessary for sharing a quantum secret in a verifiable way.

4.2. RESULTS

Our contribution is three-fold. First, our scheme realizes the task of verifiable secret sharing of a quantum state using a single qubit per share. Second, we show that the protocol can be realized in a setting where each node needs to store n qubits in a quantum memory and has a workspace of $3n$ qubits in total to verify the secret. For compari-

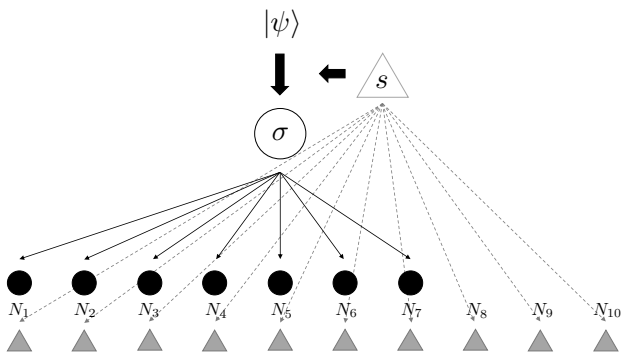


Figure 4.2: A sketch of a verifiable hybrid secret sharing (VHSS) protocol for $n = 10$ nodes denoted $N_1, \ldots, N_{10}$, with $n_q = 7$ quantum (●) and $n_c = 10$ classical (▲) shares. The quantum secret state $|\psi\rangle$ of the dealer is encrypted using a classical key s. The resulting encrypted state σ and the key s are then distributed by the dealer as quantum and classical shares respectively.

son, previous protocols [7, 35] require shares with $\Omega(\log n)$ qubits and each node having simultaneous control over $\Omega(r^2 n \log(n))$ qubits for verification, where r is the security parameter. Finally, our scheme preserves the maximum secrecy condition. This may enable qubit reductions for future implementations of cryptographic schemes, like multiparty computation or byzantine agreement, which use VQSS as a subroutine.

We extend the idea of a hybrid scheme to verifiable quantum secret sharing. Specifically, we present a protocol that achieves the task of sharing a single-qubit quantum state $|\psi\rangle$ in a verifiable way, where the dimension q of individual shares does not grow with the number of nodes n. In the spirit of [26–29], we make use of classical verifiable secret sharing [36, 37] in order to obtain a verifiable hybrid scheme where each node holds at most $3n$ single-qubit shares at a time during the verification of the secret, see Outline below. Our scheme has a variety of consequences. Thanks to the classical encryption of the quantum state via quantum one-time pad [38], our protocol can attain maximum secrecy, i.e. $p = \lfloor \frac{n-1}{2} \rfloor$. We show that by using a suitable classical scheme, one can beat the limit of maximum secrecy at the cost of tolerating less active cheaters (i.e. nodes that can perform arbitrary operations on their shares, see Adversary). Furthermore, motivated by non-verifiable schemes, we define the notion of strong threshold schemes in the context of verifiability, where any $p+1$ nodes can reconstruct the secret, any p nodes do not gain any information about it, and t nodes can actively cheat in the protocol. We then show that according to our definition, it is impossible to construct a verifiable strong threshold scheme. Finally, we show how to achieve a ramp hybrid scheme allowing for sharing secrets in a verifiable way. The security proof of our protocol expands on the approach suggested in [7, 35], see Section **??** for details.

s

Number of nodes. One key ingredient in our resource reduction is to combine quantum and classical resources in a hybrid scheme. In our model, some nodes hold quantum shares and some nodes hold classical shares. Note that nodes can have both quantum and classical shares, see Figure 4.2. We denote the number of nodes with classical

shares and the nodes with quantum shares by n_c and n_q respectively, and by n the total number of nodes.

Adversary. We allow for the existence of t malicious nodes (cheaters) in the protocol. We say that those cheaters are *active,* meaning that they can perform arbitrary joint operations on their state during the execution of the protocol, in order to learn $|\psi\rangle$. We say that a protocol *tolerates t* active cheaters if at the end of the protocol the reconstruction of the quantum state is possible despite the presence of those cheaters. The nodes who follow the protocol exactly are called honest. We follow the common assumption that the set of malicious quantum and classical nodes is determined at the beginning of the hybrid protocol and stays fixed throughout (*non-adaptive* adversary). We also assume that all nodes have access to an authenticated broadcast channel [39] and that each pair of nodes is connected by authenticated, private classical [40] and quantum [41] channels.

Definition 14 ($\{p,t,n\}$-VHSS)**.** A $\{p,t,n\}$-VHSS verifiable hybrid secret sharing scheme is an n-node protocol with three phases: sharing, verification and reconstruction, and two designated players, dealer D and reconstructor R. In the sharing phase D shares a pure single-qubit quantum state $|\psi\rangle$ using quantum and classical shares. In the verification phase all of the nodes verify that the set of shares defines a unique quantum state. In the reconstruction phase R receives all shares from all nodes, and reconstructs the unique state defined by these shares. We require that the scheme satisfies the following requirements despite of the presence of t non-adaptive active cheaters, except with probability exponentially small in the security parameter r:

- Soundness: if R is honest and D passes the verification phase, then there is a unique state $|\psi\rangle$ that can be recovered by R;
- Completeness: if D is honest then she always passes the verification phase. Moreover, if R is also honest then the reconstructed state is exactly D's state $|\psi\rangle$;
- Secrecy: if D is honest then any group of $p \geq t$ nodes cannot gain any information about the secret before reconstruction.

The parameters of the scheme are determined by an underlying quantum error correcting code which we use as a building block. In particular, a relevant variable is the distance d of the code. We remark that our results generalize to multi-qubit scenarios.

4.2.1. $\{p,t,n\}$-VHSS VERIFIABLE HYBRID SECRET SHARING PROTOCOL.

Outline of the verifiable hybrid secret sharing (VHSS) protocol (see Protocol 1).

---

1. *Sharing*

The dealer D encrypts the secret quantum state $|\psi\rangle$ using a classical key $s = ab$ and quantum one-time pad [38],

$$\sigma_{QS} = \sum_{ab=\{0,1\}^2} \frac{1}{4} X^a Z^b |\psi\rangle\langle\psi|_Q Z^b X^a \otimes |ab\rangle\langle ab|_S$$

Table 4.1: Examples of verifiable hybrid secret sharing schemes using one qubit shares coming from this work. The secret is shared among n nodes. A $\{\lfloor \frac{n-1}{2} \rfloor, t, n\}$-VHSS scheme uses shares from all of the nodes to reconstruct the secret, whereas $\{\lfloor \frac{n-1}{2} \rfloor, t, t', n\}$-ramp VHSS scheme can reconstruct the secret without any t' nodes. Both schemes tolerate t active cheaters and are based on error correcting codes of [42, 43].

Number of nodes n	$\{\lfloor \frac{n-1}{2} \rfloor, t, n\}$-VHSS		$\{\lfloor \frac{n-1}{2} \rfloor, t, t', n\}$-ramp VHSS	
	$t=2$	$t=4$	$t=1$	$t=2$
$2(t+1)^2$	$\{8,2,18\}$	$\{24,4,50\}$	$\{8,1,1,18\}$	$\{24,2,2,50\}$
$3t^2+3t+1$	$\{9,2,19\}$	$\{30,4,61\}$	$\{9,1,1,19\}$	$\{30,2,2,61\}$
$6t^2+1$	$\{12,2,25\}$	$\{48,4,97\}$	$\{12,1,1,25\}$	$\{48,2,2,97\}$
$8t^2+4t+1$	$\{20,2,41\}$	$\{72,4,145\}$	$\{20,1,1,41\}$	$\{72,2,2,145\}$

where Q is the quantum register of the dealer and S is the classical register of the encryption key. She shares the encrypted state among the nodes using the quantum protocol and the key s using the classical protocol, see Protocol 1 "Sharing".

2. *Verification*
Nodes verify whether D is honest, i.e. that the shares held by the nodes are consistent and at the end of the protocol a state will be reconstructed. For this, each node encodes the qubit received from the dealer into further n qubits and sends $n-1$ of them to other nodes. Then, each node uses at most additional $2n$ ancilla qubits for one iteration of the verification procedure. There are $\mathcal{O}(r^2)$ iterations of verification, where r is the security parameter. If the dealer passes the verification phase the protocol continues. Otherwise it aborts.

3. *Reconstruction*
One designated node R collects all shares of σ and reconstructs it. She also reconstructs the classical key s and decrypts $|\psi\rangle$.

Remark. Throughout the protocol each of the nodes needs to simultaneously store n single-qubit shares corresponding to the encoded secret state. In the verification phase each node creates at most $2n$ ancilla qubits, performs a joint operation between these ancillas and the shares of the secret, and then measures only the ancilla qubits. This means that the nodes require a workspace of at most $3n$ qubits in total for verification.

We revisit the VQSS scheme introduced in [7] and explore its extension to a verifiable scheme which uses single-qubit shares. The construction we use is based on Calderbank-Shor-Steane (CSS) error correcting codes [44, 45]. Then, we use the existing verifiable classical secret sharing schemes [36, 37] to combine classical encryption of the quantum secret with the VQSS scheme to achieve an n-node verifiable hybrid secret sharing

scheme (VHSS), see Outline. In $\{p,t,n\}$-VHSS the number p of nodes who cannot gain any information about the quantum state is determined by the classical scheme. Moreover, $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ cheaters are active and constrained by the distance d of the underlying CSS code. In our scheme the secret state of the dealer $|\psi\rangle$ is encrypted using quantum one-time pad with a classical key s, and then both objects are shared and verified in parallel. It is, therefore, impossible to reconstruct the quantum secret without reconstructing the classical key. In the case when $n = n_q = n_c$ we achieve the following functionalities:

- We construct a scheme which attains maximum secrecy using single qubit shares. Specifically, thanks to using classical encryption, we show that in our $\{p,t,n\}$-VHSS scheme any $p \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ nodes coming together before reconstructing the secret, do not gain any information about it. Our $\{p,t,n\}$-VHSS scheme tolerates up to $t < \frac{n}{4}$ active cheaters. Reconstruction of the secret occurs with all of the shares.

- We show how to achieve a $\{p,t,n\}$-VHSS scheme for $p > \left\lfloor \frac{n-1}{2} \right\rfloor$ by choosing an appropriate classical verifiable scheme [37]. In this case, however, there exists a trade-off between the number of active cheaters and secrecy, such that $n \geq p + 3t + 1$. Therefore, in order to achieve higher secrecy we tolerate less active cheaters t. As before, reconstruction of the secret occurs with all of the shares.

- We define a strong threshold scheme (see Definition 15) where shares from any group of $n - t'$ nodes are sufficient for the reconstruction, no group of $p = n - t' - 1$ nodes gains any information about the state. Importantly, we show that according to our definition, it is impossible to achieve a verifiable strong threshold scheme, namely, a scheme which satisfies the two above constraints and tolerates t active cheaters at the same time.

- We relax the secrecy constraint of the strong threshold scheme and construct a ramp VHSS scheme (see Definition 16). In our ramp verifiable scheme any $n - t'$ nodes can reconstruct the secret, but any group of at most $p \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ does not have any information about it. The scheme tolerates t active cheaters, where $t + t' \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ are constrained by the distance of the underlying quantum error correcting code. We denote it with $\{p,t,t',n\}$-ramp VHSS.

In the case when $n = n_c > n_q$, our VHSS scheme allows us to construct a scheme which extends verifiable quantum secret sharing onto nodes with purely classical capabilities, see Figure 4.2. That is, we use VQSS to share a quantum secret with n_q nodes, but we extend the sharing of the classical key s onto $n_c > n_q$ nodes. Therefore, some of the nodes hold only classical shares but still participate in hiding of the quantum secret. Due to the properties of our protocol, this scheme can also lift the secrecy, such that no set with $p \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ nodes can learn the quantum state before the reconstruction.

4.2.2. IMPLICATIONS FOR RESOURCE REDUCTION.

Our scheme allows us to exploit CSS quantum error correcting codes which encode a single-qubit quantum state into single-qubit shares. Such codes are well-studied in the

literature and therefore, numerous schemes with defined encoding and decoding exist [42, 43]. In the next section we present examples of VHSS schemes based on such codes. We remark that one could use approximate error correction codes and in this way increase the number of active cheaters to $2t$ [23, 41]. However this solution requires significantly more resources, see Section 5.4.

4.3. RESOURCE REDUCTION

Our protocol reduces the number of qubits that need to be controlled simultaneously by each node. To do so, we adapt the protocol of [7], where the verification procedure requires ancillas used in parallel, to a setting where they can be used sequentially, i.e. one by one. This way, each node needs control over $3n$ operational qubits at a time. For comparison, the parallel execution of [7] requires simultaneous control over $\Omega(r^2 n \log(n))$ qubits per node, where r is the security parameter.

Here we list a few examples of CSS codes leading to VHSS schemes with single-qubit shares (also see Table 4.1). We express our examples in terms of maximum tolerable number of active cheaters t. Note that for a particular code there exists a trade-off between the number of active cheaters and the total number of nodes.

For $t = 1$:

- $\{3,1,7\}$-VHSS. In this scheme $n = n_c = n_q = 7$ nodes hold both quantum and classical shares. The scheme achieves maximum secrecy, i.e. no group of $p = \lfloor \frac{7-1}{2} \rfloor = 3$ shares acquires any information about the secret. All of the quantum shares are single-qubit shares, and each node requires control over 21 qubits at a time for the verification procedure. This example is based on the Steane's $[[7,1,3]]_2$ code, encoding 1 qubit into 7 qubits, with distance $d = 3$ [45]. In this scheme all shares are necessary to reconstruct the secret.

  Note that the Steane's code without the classical encryption would generate a VQSS scheme, where no 2 nodes could gain any information about the secret. However, due to the properties of the code, a *specific* group of 3 nodes could still reconstruct the secret. To compare, the existing construction to achieve a purely quantum scheme with maximum secrecy, requires individual shares of dimension $q > 7$.

- $\{\lfloor \frac{n-1}{2} \rfloor, 1, n\}$-VHSS. In this scheme $n_q = 7$ out of n nodes hold quantum single-qubit shares and $n = n_c > 7$ hold classical shares. The scheme achieves maximum secrecy. For the construction we use the Steane's $[[7,1,3]]_2$ code and a classical scheme of [36]. Therefore, in our scheme only 7 nodes need to have quantum resources, but all of the n nodes can participate in verifiable secret sharing of a quantum state.

For $t \geq 1$:

- $\{\lfloor \frac{n-1}{2} \rfloor, t, n\}$-VHSS. We construct VHSS schemes which tolerate more than one active cheater and achieve maximum secrecy. All of the nodes hold both quantum and classical shares ($n_q = n_c = n$), and the quantum shares contain a single qubit. For the construction we use higher-distance quantum error correcting codes, for example toric codes and color codes [42, 43], and VCSS scheme of [36]. We present

specific examples in Table 4.1. Note that each of those schemes can be expanded onto even larger total number of nodes, by using a verifiable classical secret sharing scheme with $n_c > n_q$.

- $\{p, t, t', n\}$-ramp VHSS. Based on the same higher-distance quantum error correcting codes [42, 43], we construct examples of ramp schemes, see Tab. 4.1. All of the nodes hold quantum and classical shares, however, only $n - t'$ are used to reconstruct the secret.

4.4. METHODS

4.4.1. PROTOCOL

Our protocol is a hybrid between a classical scheme (VCSS) and a quantum scheme (VQSS) to share the classical key s and the encrypted quantum state σ_{QS}, respectively. In the following we summarize the principles of these two protocols.

VERIFIABLE CLASSICAL SECRET SHARING

A verifiable classical secret sharing scheme is a scheme which shares a classical secret of the dealer among n_c nodes in a verifiable way, using classical shares. The scheme is such that p_c nodes cannot gain any information about the classical secret after coming together (secrecy) and there are at most t_c active non-adaptive cheating nodes that the scheme tolerates. We represent the classical verifiable secret sharing protocol with a triple (p_c, t_c, n_c)-VCSS. Here we treat the VCSS scheme as a secure black box which leaks no information about the classical key s, even if the adversary has access to quantum side information during the execution of VCSS. VCSS schemes that are information theoretically secure in the context of classical adversary have been presented in for example [36**?** , 37]. Here we add it as an assumption that any VCSS protocol used to build Protocol 1 is secure against a quantum adversary in the information-theoretic sense.

Assumption 7. The VCSS scheme used to build Protocol 1, does not leak any information about the secret key s to any set of p_c nodes, except with probability exponentially small in the security parameter r, even in the presence of quantum side information. That is, the scheme is information theoretically secure in the presence of a quantum adversary.

Formally, VCSS is a classical protocol in which the dealer inputs a classical message s, which is shared among the nodes. Let P be a set of size at most p_c, and let $\mathcal{Q}_P$ denote any quantum side information held by the nodes in set P at the end of the verification phase of the VHSS. In principle, $\mathcal{Q}_P$ could be arbitrarily correlated with the classical secret key s. However, Assumption 7 implies that the state held by nodes in P carries no information about the key s, other than what was known prior to the beginning of the protocol.

To the best of our knowledge, security of protocols of [37**?**] against an adversary with quantum side information was never formalized. We note that in Theorem 13 of [46] it was proven that any classical protocol which is statistically secure in a universal composable (UC) sense, is also statistically UC-secure against a quantum adversary. Furthermore, [47, 48] discuss the possibility of strengthening the security of [36] to UC-security. As a consequence [36] could be conjectured statistically UC-secure against a quantum adversary.

In what follows, unless specified otherwise, we will consider a classical VCSS protocol of [36]. This scheme is secure with exponentially small probability of error $2^{-\Omega(r')}$, where r' is the security parameter. Here, for convenience, we choose r' such that $r' = r$, where r is the security parameter of VHSS. The protocol can tolerate up to $t_c < \frac{n_c}{2}$ malicious nodes. In particular, it also implies that $p_c = t_c < \frac{n_c}{2}$.

VERIFIABLE QUANTUM SECRET SHARING

To construct our hybrid scheme we employ a VQSS scheme which uses single-qubit shares. The VQSS scheme summarized here is based on the results of [7].

A verifiable quantum secret sharing scheme is a scheme which shares a quantum state of the dealer among n_q nodes in a verifiable way, using quantum shares. The scheme is such that p_q nodes cannot gain any information about the secret (secrecy) and there are at most t_q non-adaptive active cheating nodes that the scheme tolerates. We denote such a scheme with a triple (p_q, t_q, n_q)-VQSS. To share a pure qubit state among n_q nodes in a VQSS, the nodes agree on (an efficiently decodable) $[[n_q, 1, d]]_2$ Calderbank-Shor-Steane (CSS) error correcting code $\mathscr{C}$. Such a code encodes 1 qubit into n_q qubits and has distance d. This means that the chosen CSS code is able to correct $t_q \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ arbitrary errors and $p_q \leq d-1$ erasure errors.

The CSS code $\mathscr{C}$ used to perform the protocol, is defined through two binary classical linear codes, V and W, satisfying $V^* \subseteq W$, where V^* is the dual code. Then, $\mathscr{C} = V \cap_{\mathscr{F}} W$ is a set of states of n_q qubits which yield a codeword in V when measured in the standard basis, and a codeword in W when measured in the Fourier basis [49]. An important property of a CSS code, which is useful for the VQSS protocol, is the fact that certain logical operations $\bar{\Lambda}$ can be implemented by applying local operations Λ on the individual qubits held by the nodes and encoded with $\mathscr{C}$, i.e. $\bar{\Lambda} = \Lambda^{\otimes n_q}$. This property, called transversality, means that specific logical operations can be applied qubit-wise. In particular, the protocol uses the fact that *(i)* applying a CNOT gate is tranversal; *(ii)* applying the Fourier transform qubit-wise maps codewords of the code $\mathscr{C}$ onto codewords of the dual code $\tilde{\mathscr{C}}$; *(iii)* measurements can be performed qubit-wise, but measurement outcome of every qubit must be communicated classically to obtain the result of the logical measurement.

In the VQSS protocol the dealer D encodes the quantum secret state $|\psi\rangle$ using the code $\mathscr{C}$ and distributes it to n_q nodes. Next, each node i encodes her qubit into n_q further qubits and distributes those to every other node, see Figure 4.3. This way the nodes create two levels of encoding which can be represented as a tree. The second level of encoding gives each node some control over all the other shares, which allows honest nodes to check consistency of all the shares.

The protocol aims to verify whether the shares (the tree) create a codeword for which decoding is well-defined with respect to the code $\mathscr{C}$, without revealing any information about the secret state of the dealer. This property is formally defined in [7, 35] and is dubbed 2-GOOD. Intuitively, a 2-GOOD$_V$ tree means that for all branches of the tree which are held by honest nodes, upon measuring their shares of the tree, there exists a unique codeword in the code V that can be recovered. Since $\mathscr{C} = V \cap_{\mathscr{F}} W$, to verify that the encoded tree is 2-GOOD$_{\mathscr{C}}$, the verification procedure first verifies that the tree is 2-GOOD$_V$ when measured in the standard basis, and then that it is 2-GOOD$_W$ when

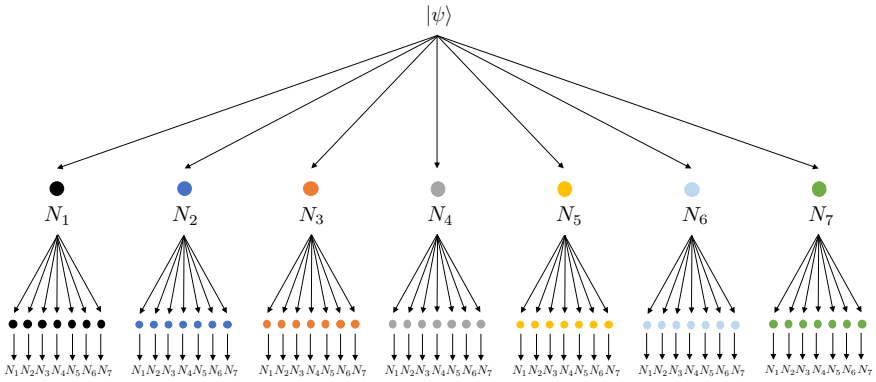


Figure 4.3: The encoding tree for (2,1,7)-VQSS protocol with 7 nodes $N_1,\ldots,N_7$, based on the Steane's $[[7,1,3]]_2$ code. The figure represents the encoding done in the sharing phase by each of the nodes.

measured in the Fourier basis.

We adapt the verification procedure from the work of [7, 35] to run in a sequential way. In our procedure, to verify that the encoded secret is 2-GOOD$_V$ in the standard basis, the dealer and the nodes create auxiliary trees initiated in a logical $|\bar{+}\rangle$ state of the code $\mathscr{C}$. Importantly, these systems are distributed one at a time. Therefore, each node needs to control $2n$ qubits at a time: n single-qubit shares for the encoded secret state, and n single-qubit shares for the auxiliary $|\bar{+}\rangle$ state. We perform r such checks, where r is the security parameter.

After this step, our protocol verifies that the encoded secret is 2-GOOD$_W$ in the Fourier basis. To do so, the dealer and the nodes create new auxiliary trees initiated in a logical $|\bar{0}\rangle$ state of the code $\mathscr{C}$. Here an important difference is that each of the auxiliary $|\bar{0}\rangle$ states is first verified to be 2-GOOD$_V$ as well, before applying the Fourier transform. This step is necessary, because one wants to make sure that the check in the Fourier basis does not introduce bit flips in the standard basis (at this point the check in standard basis for the secret state $|\psi\rangle$ has already been performed). Verifying each $|\bar{0}\rangle$ requires using extra n single-qubit shares per node and is repeated r times. Therefore, each node needs to control $3n$ qubits at this step: n single-qubit shares for the encoded secret, n single-qubit shares for a $|\bar{0}\rangle$ state, and additional n single-qubit shares for the verification of $|\bar{0}\rangle$. In comparison, in [7, 35] all of the above steps are performed in parallel, and effectively, each node needs to control $\Omega(r^2 n\log(n))$ at once.

In the verification phase the nodes publicly identify a set of *apparent* cheaters B with probability exponentially close to 1 in the security parameter r. Set B includes all of the errors introduced by the dealer and errors introduced by the cheating nodes until the end of the verification phase. Note that there is no way to distinguish the errors introduced by the dealer and those introduced by the cheaters at this point. The dealer will pass verification as "honest" if $|B| \leq t_q$. On the other hand, if $|B| \geq t_q$ then the protocol aborts.

After the verification phase, the cheating nodes can still corrupt their shares. Therefore, the reconstructor R runs an error correction circuit and measures syndromes, so

that she can correct arbitrarily located errors introduced by the cheaters after the verification. If for a branch encoded by a particular node i there have been more than t_q errors, then R adds that node to the set B of cheaters. Otherwise, R corrects errors and reconstructs branch i. After reconstructing all branches, she randomly picks $n-2t_q$ shares which she has left, and reconstructs the state of the dealer. Importantly, the size of set B cannot be larger than $2t_q$ at the end of the protocol. This is because the dealer D and cheaters can introduce at most t_q errors at the first level of encoding before verification (otherwise the protocol aborts). Before the reconstruction, the cheaters may introduce up to t_q extra errors at the second level of each branch they hold. This may create extra errors at the first level, but never more than t_q, since the cheaters have some control over at most t_q branches.

What is more, let $C_{\texttt{VQSS}}$ be the set of cheaters in the VQSS and $C_{\texttt{VCSS}}$ the set of cheaters in VCSS. We assume that if a node behaves maliciously in VQSS, it can also behave maliciously in VCSS, and moreover $C_{\texttt{VQSS}} = C_{\texttt{VCSS}}$. Therefore, we put $t = t_c = t_q$. Moreover, in our VHSS protocol we assume that the nodes have access to shared public source of randomness. This can be realized, for example, by running a classical verifiable secret sharing protocol or multipartite coin flipping. We remark that [35] points out solutions to reduce the classical communication complexity of generating public randomness. In the following we will write $[1,n]$ to denote registers of nodes from 1 to n.

Protocol 1: Verifiable Hybrid Secret Sharing (VHSS)

Input: a qubit secret system $|\psi\rangle$ to share, CSS error correcting code $\mathscr{C} = V \cap \mathscr{F}W$.

SHARING

Encryption

1. The dealer D encrypts her secret state $|\psi\rangle$ using quantum one-time pad with a classical key s, creating the state σ_{QS}, see Equation (4.5).
2. D shares the classical key s among n nodes using a verifiable classical secret sharing VCSS protocol.

Encoding

1. D encodes σ_Q using $\mathscr{C}$ into $\Phi^{0,0}_{[1,n_q]}$, where σ_Q is the reduced state of σ_{QS}.
2. for $i = 1,\ldots,n_q$:
   D sends $\Phi^{0,0}_{i}$ to node i.
   Each node i encodes received systems using $\mathscr{C}$ into $\Phi^{0,0}_{i_{[1,n_q]}}$ and sends j-th component $\Phi^{0,0}_{i_j}$ to node j.

VERIFICATION

Z basis

for $\ell = 0$, $m = 1,\ldots,r$:

1. D prepares $|\bar{+}\rangle^{0,m}_{[1,n_q]} = \sum_{v\in V}|v\rangle$ using $\mathscr{C}$.

2. for $i = 1,\dots,n_q$:
   D sends $|\bar{+}\rangle_i^{0,m}$ to node i.
   Each node i encodes received systems using $\mathscr{C}$ into $|\bar{+}\rangle_{i_{[1,n_q]}}^{0,m}$ and sends j-th component $|\bar{+}\rangle_{i_j}^{0,m}$ to node j.
3. Nodes use shared public randomness source and get public random value $b_{0,m} \in_R \{0,1\}$. Each node j:
   (a) applies the CNOT gate to her shares depending on the value of $b_{0,m}$ ($CNOT^{b_{0,m}}$). That is, for every qubit i, if $b_{0,m} = 0$ the node does nothing, and if $b_{0,m} = 1$ the node applies a CNOT gate with a qubit indexed by $m = 0$ as a control to a qubit indexed by $m = 1,\dots,r$ as a target:
   $$\forall i = 1,\dots,n_q: \quad CNOT^{b_{0,m}}\left(\Phi_{i_j}^{0,0}, |\bar{+}\rangle_{i_j}^{0,m}\right)$$
   (b) measures all systems indexed $\ell = 0,\ m = 1,\dots,r$ in the Z basis and broadcasts the result of the measurement.

X basis

for $\ell = 1,\dots,r$:

4. D prepares $|\bar{0}\rangle_{[1,n_q]}^{\ell,0} = \sum_{w\in W^\perp} |w\rangle$ using $\mathscr{C}$.
5. for $i = 1,\dots,n_q$:
   D sends $|\bar{0}\rangle_i^{\ell,0}$ to node i.
   Each node i encodes received systems using $\mathscr{C}$ into $|\bar{0}\rangle_{i_{[1,n_q]}}^{\ell,0}$ and sends j-th component $|\bar{0}\rangle_{i_j}^{\ell,0}$ to node j.

for $m = 1,\dots,r$:

6. D prepares $|\bar{0}\rangle_{[1,n_q]}^{\ell,m} = \sum_{w\in W^\perp} |w\rangle$ using $\mathscr{C}$.
7. for all $i = 1,\dots,n_q$:
   D sends $|\bar{0}\rangle_i^{\ell,m}$ to node i.
   Each node i encodes received systems using $\mathscr{C}$ into $|\bar{0}\rangle_{i_{[1,n_q]}}^{\ell,m}$ and sends j-th component $|\bar{0}\rangle_{i_j}^{\ell,m}$ to node j.
8. Nodes use shared public randomness source and get public random values $b_{\ell,m} \in_R \{0,1\}$. Each node j:
   (a) applies the CNOT gate to her shares depending on the value of $b_{\ell,m}$ ($CNOT^{b_{\ell,m}}$):
   $$\forall i = 1,\dots,n_q: \quad CNOT^{b_{\ell,m}}\left(|\bar{0}\rangle_{i_j}^{\ell,0}, |\bar{0}\rangle_{i_j}^{\ell,m}\right)$$
   (b) measures the m-th system in the Z basis and broadcasts the result of the measurement.
9. Nodes apply the Fourier transform $\mathscr{F}$ to all of their remaining shares, resulting in $\Phi^{\mathscr{F}}{}_{[1,n_q]_j}^{0,0}$ and $|\bar{0}^{\mathscr{F}}\rangle_{[1,n_q]_j}^{\ell,m}$ for each node j. Note that $|\bar{0}^{\mathscr{F}}\rangle = \sum_{w\in W} |w\rangle$.

10. Nodes use shared public randomness source and get public random values $b_{\ell,0} \in_R \{0,1\}$. Each node j:
    (a) applies the CNOT gate to her shares depending on the value of $b_{\ell,0}$ ($CNOT^{b_{\ell,0}}$):

$$\forall i = 1,\ldots,n_q: \quad CNOT^{b_{\ell,0}}\left(\Phi^{\mathscr{F}\,0,0}_{i_j}, |\bar{0}^{\mathscr{F}}\rangle^{\ell,0}_{i_j}\right)$$

    (b) measures ℓ-th system in the Z basis and broadcasts the result of the measurement.

11. (Decoding leaves Z basis) Broadcasted values in steps 3(b) and 8(b) yield words $\mathbf{v}_{\ell,m,i}$ from code V, corresponding to the second level of shares encoded by each node i. For each of the words, using classical decoding, the nodes:
    (a) obtain a decoded value $a_{\ell,m,i}$
    (b) publically check on which positions the errors have occurred, denote these positions by $B_{\ell,m,i}$. Nodes update sets $B_i = \cup_{\ell,m} B_{\ell,m,i}$ from the positions of errors which occurred in the systems encoded by node i. If $|B_i| > t$ then add i to a global set B.

12. (Decoding the root Z basis) The nodes arrange values $a_{\ell,m,i}$ into $\mathbf{a}_{\ell,m} = \{a_{\ell,m,1},\ldots,a_{\ell,m,n_q}\}$. Word $\mathbf{a}_{\ell,m}$ yields a classical codeword from the code V and the nodes decode it using classical decoder of code V. They add the positions on which an error occurred to the global set B.

13. (Decoding leaves X basis) Broadcasted values in step 10(b) yield words $\mathbf{w}_{\ell,0,i}$ from code W, corresponding to the second level of shares encoded by each node i. For each of the words, using classical decoding, the nodes:
    (a) obtain a decoded value $a_{\ell,0,i}$
    (b) publically check on which positions the errors have occurred, and update sets B_i and B as before. Sets B_i and B are cumulative throughout the protocol.

14. (Decoding the root X basis) Nodes create a codeword $\mathbf{a}_{\ell,0} = \{a_{\ell,0,1},\ldots,a_{\ell,0,n_q}\}$ and decode it using classical decoder of code W. They add the positions on which an error occurred to the global set B. If $|B| > t$ then reject the dealer and abort. Otherwise continue.

15. Nodes apply an inverse Fourier transform $\mathscr{F}^{-1}$ to their remaining system and obtain global sharing of D secret, i.e. each node j holds $\Phi^{0,0}_{[1,n_q]_j}$.

RECONSTRUCTION

1. Each quantum node $j = 1,\ldots,n_q$ sends their shares to the reconstructor R. Moreover, all of the n_c classical nodes send their classical shares to R.
2. R reconstructs the classical secret key s using a decoder of `VCSS`.
3. For each share $\Phi^{0,0}_{i_{[1,n]}}$ coming from encoding of node $i \notin B$, R runs a circuit for code $\mathscr{C}$ which identifies errors. R creates a set $\tilde{B}_i$ such that it contains B_i, $B_i \subseteq \tilde{B}_i$. If $|\tilde{B}_i| \leq t$ then errors are correctable, R corrects them and decodes the i-th share, obtaining $\Phi^{0,0}_i$. Otherwise, R adds i to the global set B.

4. For all $i \notin B$, R randomly chooses $n_q - 2t$ shares $\Phi_i^{0,0}$ and applies an erasure-recovery circuit to them. R obtains σ_R.
5. R decrypts σ_R using the classical key s and obtains $|\psi\rangle$.

4.4.2. SECURITY

As discussed in previous sections, in the task of verifiable secret sharing we want to ensure that the dealer is honest and that at the end of the protocol there will be a well-defined state to be reconstructed. In this section we prove the security of Protocol 1 against t non-adaptive active cheaters. First we state useful lemmas about the security of the VQSS protocol of [7], which we use as a subroutine. For a detailed discussion we refer the reader to [35]. We remark that we use an adapted version of VQSS in the setting where we run the verification phase sequentially, i.e. one ancilla at a time, whereas in [7] the verification is performed in a parallel setting, i.e. all ancillas together. In Section **??** we prove that this fact does not change security statements of the original VQSS.

Lemma 7 (soundness of VQSS)**.** *In the verifiable quantum secret sharing protocol [7], either the honest parties hold a consistently encoded secret or dealer is caught and the protocol aborts with probability at least* $1 - 2^{-\Omega(r)}$ *(see Equation* (4.34) *in Section* **??***).*

Lemma 8 (completeness of VQSS)**.** *In the verifiable quantum secret sharing protocol [7], if D is honest then she passes the verification phase. Moreover, if R is also honest she reconstructs D's secret with probability at least* $1 - 2^{-\Omega(r)}$*, where r is the security parameter (see Equation* (4.35) *in Section* **??***).*

Using the above lemmas we now show that our VHSS protocol, Protocol 1, is sound and complete.

Theorem 11 (soundness)**.** *In the verifiable hybrid secret sharing protocol, Protocol 1, either the honest parties hold a consistently encoded secret or dealer is caught and the protocol aborts with probability at least* $1 - 2^{-\Omega(r)}$.

Proof. The soundness of the hybrid protocol is a combination of soundness statements for the VQSS and VCSS protocols. Formally, we need to bound the probability that one of the protocols fails,

$$\Pr\left[\text{fail}_{\text{VQSS}} \vee \text{fail}_{\text{VCSS}}\right] \leq \Pr\left[\text{fail}_{\text{VQSS}}\right] + \Pr\left[\text{fail}_{\text{VCSS}}\right]. \tag{4.1}$$

Let us first consider $\Pr[\text{fail}_{\text{VCSS}}]$. Consider the protocol of [36] whose probability of failure scales exponentially with a security parameter r'. We choose r' such that it is equal to the security parameter of VQSS, $r' = r$, and therefore, $\Pr[\text{fail}_{\text{VCSS}}] \leq 2^{-\Omega(r)}$.

On the other hand, by Lemma 7, the VQSS protocol can fail with probability $\Pr[\text{fail}_{\text{VQSS}}] \leq 2^{-\Omega(r)}$. Therefore, we obtain

$$\Pr\left[\text{fail}_{\text{VQSS}} \vee \text{fail}_{\text{VCSS}}\right] \leq 2^{-\Omega(r)}. \tag{4.2}$$

□

Theorem 12 (completeness)**.** *In the verifiable hybrid secret sharing protocol, Protocol 1, if D is honest then she passes the verification phase. Moreover, if R is also honest she reconstructs D's secret with probability at least* $1-2^{-\Omega(r)}$*, where r is the security parameter.*

Proof. For the first part of the theorem, observe that an honest dealer always passes the verification phase. Indeed, if the dealer is honest, she does not introduce any errors, neither in the VQSS, nor in the VCSS protocol. Moreover, by the assumption that active cheaters t are always bounded by the number of tolerable errors, the VHSS protocol can always correct the arising errors and the verification phase always accepts an honest dealer.

For the second part of the theorem, as in the soundness statement, we calculate the probability that the VHSS protocol fails with an honest dealer,

$$\Pr\left[\text{fail}'_{\texttt{VQSS}} \vee \text{fail}'_{\texttt{VCSS}}\right] \leq \Pr\left[\text{fail}'_{\texttt{VQSS}}\right] + \Pr\left[\text{fail}'_{\texttt{VCSS}}\right]. \tag{4.3}$$

For the classical VCSS protocol, as before, we consider the protocol of [36]. By choosing the security parameter of the classical protocol such that $r' = r$, we obtain $\Pr[\text{fail}'_{\texttt{VCSS}}] \leq 2^{-\Omega(r)}$. For the VQSS protocol, if R is also honest, by Lemma 8 the probability that the verification phase fails to identify the set B of apparent malicious nodes, occurs with probability $2^{-\Omega(r)}$, see Section **??** for details. Therefore,

$$\Pr\left[\text{fail}'_{\texttt{VQSS}} \vee \text{fail}'_{\texttt{VCSS}}\right] \leq 2^{-\Omega(r)}. \tag{4.4}$$

□

The encryption of the secret with a classical key has significant consequences for the secrecy of the VHSS scheme. We expand on it in the theorem below. Note that in a VQSS [7] the secrecy property holds for any $p_q \leq 2t_q$ nodes not being able to learn any information about the dealer's secret. However, in our VHSS scheme we choose a classical scheme such that $p_c = p > 2t_q$, and therefore, we lift the secrecy of the VQSS scheme (for a detailed discussion see Sec. 4.4.3 below).

Theorem 13 (secrecy)**.** *In the verifiable hybrid secret sharing protocol, Protocol 1, when D is honest and there is at most t active cheaters in the verification phase, no group of at most* $p = p_c$ *nodes learns anything about D's secret state throughout the protocol, where* p_c *is the secrecy of the underlying classical scheme, except with probability exponentially small in the security parameter r.*

Proof. The state describing the dealer's encrypted quantum secret and the randomly chosen classical encryption key $s = ab$ is

$$\sigma_{QS} = \sum_{ab=\{0,1\}^2} \frac{1}{4} X^a Z^b \left|\psi\right\rangle\!\left\langle\psi\right|_Q Z^b X^a \otimes \left|ab\right\rangle\!\left\langle ab\right|_S \tag{4.5}$$

where Q is the quantum register of the dealer and S is the classical register of the encryption key. By Assumption 7 the classical VCSS scheme is secure and does not leak any information about the key $s = ab$ to any set of p_c nodes, even in the presence of a quantum adversary, except with probability exponentially small in the security parameter r.

Therefore, without the knowledge of the encryption key s, the quantum state shared by the dealer as seen by the rest of the nodes is maximally mixed,

$$\begin{aligned}\sigma_Q &= \mathrm{tr}_S(\sigma_{QS}) = \\ &= \sum_{ab=\{0,1\}^2} \frac{1}{4} X^a Z^b \left|\psi\right\rangle\!\left\langle\psi\right|_Q Z^b X^a = \frac{\mathbb{1}_Q}{2}.\end{aligned} \tag{4.6}$$

Before sending out the shares, the dealer applies an encoding $\mathscr{E}_Q$ to the quantum register Q, so that

$$\forall \left|\psi\right\rangle \quad \mathrm{tr}_S((\mathscr{E}_Q \otimes \mathbb{1}_S)(\sigma_{QS})) = \mathscr{E}_Q(\mathrm{tr}_S(\sigma_{QS})) \tag{4.7}$$

$$= \mathscr{E}_Q(\sigma_Q) =: \rho_{[1,n_q]}, \tag{4.8}$$

where $\rho_{[1,n_q]}$ is an n_q-qubit state sent by the dealer to n_q nodes. Importantly, since $\mathscr{E}_Q$ and σ_Q, Equation (4.6), are independent of $|\psi\rangle$, $\rho_{[1,n_q]}$ is also independent of $|\psi\rangle$. Subsequently, the honest nodes do their encoding $\mathscr{E}$, and the malicious nodes can perform any (CPTP) operation $\mathscr{A}$ that they desire. After this step, since $\mathscr{E}$ and $\mathscr{A}$ do not depend on $|\psi\rangle$, the state of the n_q nodes $\rho'_{[1,n_q]}$ is independent of $|\psi\rangle$. In the classical scheme any group of p_c or fewer nodes has no information about s. Hence, the partial state of any $p = p_c$ or fewer nodes in VHSS does not depend on $|\psi\rangle$ and no information about the dealer's secret can be obtained, except with probability exponentially small in r.

□

4.4.3. VERIFIABLE HYBRID SCHEMES

Our protocol for VHSS, Protocol 1, leads to a variety of schemes, depending on the parameters of the underlying VQSS and VCSS protocols. In this section we discuss the trade-offs between those parameters and specify what schemes can be achieved with our protocol.

VERIFIABLE SCHEMES WITH MAXIMUM SECRECY

In any VQSS scheme based on an error correcting code with distance d, any group of at most $d-1$ nodes cannot recover information about the secret. As mentioned before, this is due to the fact that a code of distance d can correct up to $d-1$ erasures, and therefore any $n-(d-1)$ nodes can recover the state perfectly. In particular, it implies that $d-1$ nodes do not have any information about the encoded state [18]. Quantum Singleton bound [50] allows that $n \leq 2d-1$ for codes encoding a single qubit. The construction of [7] saturates this inequality, and therefore allows for attaining $p = \lfloor \frac{n-1}{2} \rfloor$, which we refer to as maximum secrecy. However, this construction uses systems of local dimension $q > n$ and is based on quantum Reed-Solomon codes [51].

To remedy this problem, we use a VQSS scheme based on CSS codes with single-qubit shares, at the cost of reducing secrecy. However, in our VHSS scheme, we combine this with a classical scheme for which $p_c > 2t_q$. Specifically, the VCSS protocol of [36] tolerates up to $\lfloor \frac{n-1}{2} \rfloor$ cheaters. This allows us to maximally lift the secrecy of the quantum scheme to the one attainable by the VQSS of [7].

Lemma 9 (VHSS with maximum secrecy)**.** *Given a* $[[n,1,d]]_2$ *CSS error correcting code and a VCSS scheme tolerating up to* $\lfloor \frac{n-1}{2} \rfloor$ *classical active cheaters, Protocol 1 provides a way to construct a* $\{\lfloor \frac{n-1}{2} \rfloor, t, n\}$*-VHSS scheme with maximum secrecy* $p = \lfloor \frac{n-1}{2} \rfloor$*, tolerating* $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ *active cheaters, where all of the shares are used to recover the quantum secret state.*

Furthermore, we can explore other classical verifiable schemes in the context of lifting secrecy in VHSS. In [37] a classical VCSS scheme was presented, which has a strong secrecy property: any $p_c > t_c$ nodes cannot learn any information about the classical secret (for comparison, in the scheme of [36] $p_c = t_c$). However, this scheme is able to tolerate up to $t_c \leq \left\lfloor \frac{n_c-1}{4} \right\rfloor$ active classical cheaters. Additionally, there exists a trade-off between the number of nodes n, and the numbers of cheaters, i.e. $n_c \geq p_c + 3t_c + 1$ (for details see Section 3.2 of [37]). Consequently, this allows us to construct a VHSS scheme lifting the secrecy beyond $\frac{n}{2}$, but at the cost of tolerating less active cheaters t. Note that the classical scheme was proven to be information theoretically secure against a classical adversary, and by Assumption 7 we assume it remains information theoretically secure against quantum adversary. Moreover, the protocol was shown to be perfectly secure, i.e. with zero probability of error. Therefore, secrecy achieved in a VHSS which uses this protocol as a subroutine, is exact and does not depend on the security parameter r.

Lemma 10. *Given a* $[[n,1,d]]_2$ *CSS error correcting code and a VCSS scheme with* $n \geq p + 3t + 1$*, Protocol 1 provides a way to construct a* $\{p,t,n\}$*-VHSS scheme. In particular, to achieve* $p > \lfloor \frac{n-1}{2} \rfloor$ *the scheme tolerates* $t < \frac{1}{3}(n-p-1)$ *active cheaters. All of the shares are used to recover the quantum secret state.*

THRESHOLD VERIFIABLE SCHEMES

In the literature of secret sharing schemes, one often considers schemes which have a property called *threshold* [10, 11]. This property can be stated as the requirement that there exists $p > 0$, such that no subset of less than p shares reveals any information about the state of the dealer, while any subset of $p+1$ shares allows to perfectly reconstruct the state. Importantly, in such schemes, there are no actively cheating nodes in the protocol.

Since in Protocol 1 we allow for the existence of active cheaters, let us consider a definition of a threshold scheme when there are $t > 0$ active cheaters. We will call it a strong threshold scheme. In this case, in the reconstruction phase the reconstructor R receives shares from $p + 1 = n - t'$ of the nodes. Among those, up to t of them can be arbitrarily corrupted.

Definition 15 (strong threshold scheme)**.** A strong threshold (verifiable) secret sharing scheme is a scheme where:

1. Any set of shares held by $p = n - t' - 1$ nodes does not reveal any information about the secret state.
2. The reconstructor is able to perfectly reconstruct the secret state with the set of shares from any $n - t'$ nodes.

The above conditions hold in the presence of $t > 0$ active cheaters.

In the literature of classical verifiable secret sharing a similar definition of threshold is satisfied in the presence of cheaters. For example, the scheme of [52] considers a situation when honest shares are flagged. Therefore, the reconstructor knows which $n - t'$

honest shares to pick for the reconstruction. However, in our case, the reconstructor *does not* know which shares are honest and which are not. In such a situation, this definition cannot be satisfied, which we show in the following proposition.

Proposition 1. It is impossible to construct a strong threshold secret sharing scheme according to Definition 15.

Proof. From point 2 of Definition 15 we have that R must be able to reconstruct the secret state from any $n-t'$ shares, in particular, she must be able to do so when receiving $n-t'-t$ honest shares and t arbitrary ones. This implies that she is able to recover the state from the $n-t'-t$ honest shares alone. On the other hand, from point 1 of Definition 15 no $n-t'-1$ shares reveal any information, which implies that we must have $n-t'-t > n-t'-1$. The only way to satisfy this inequality is when $t=0$. □

Remark. Similarly to [52], it is possible to add a flagging system to Protocol 1 using techniques from [23, 41]. Indeed, there, one uses a quantum authentication scheme to flag whether the shares are honest or not. However, as mentioned before, this happens at a significant qubit cost. Since our objective is to reduce the number of qubits, we explore a alternative direction in the next section.

RAMP VERIFIABLE SCHEMES

In the previous section, we have seen that it is impossible to construct a strong threshold scheme which tolerates active cheaters according to Definition 15. In particular, this result also applies to verifiable schemes. Therefore, here we allow for a gap between the number of nodes p that obtain no information about the secret and the number of nodes $n-t'$ necessary to reconstruct the secret, and we introduce a definition of a ramp verifiable scheme.

Definition 16. A ramp verifiable secret sharing scheme is a scheme where any $n-t'$ nodes can reconstruct the secret, but any p nodes cannot gain any information about the secret state, for some $p < n-t'-1$. The scheme can verify the dealer in the presence of t active cheaters. We denote such a scheme with $\{p,t,t',n\}$-ramp.

Relating to discussion in Section 4.4.3, we see that the purely quantum VQSS scheme of [7] allows for constructing a ramp scheme with secrecy $p \leq \left\lfloor \frac{n-1}{2} \right\rfloor$. However, for qubit CSS codes this equality is not saturated. Therefore, as before we use a classical scheme [36] to increase the value of p (lift the secrecy) as compared to the purely quantum ramp scheme. We obtain the following result.

Lemma 11 (Ramp VHSS)**.** *Given a $[[n,1,d]]_2$ CSS error correcting code and a VCSS scheme tolerating up to $\left\lfloor \frac{n-1}{2} \right\rfloor$ classical active cheaters, Protocol 1 provides a way to construct a $\{p,t,t',n\}$-ramp VHSS scheme with $p = \left\lfloor \frac{n-1}{2} \right\rfloor$, where the quantum state can be recovered with shares from any $n-t'$ nodes in the presence of t active cheaters, and $t+t' \leq \left\lfloor \frac{d-1}{2} \right\rfloor$.*

By putting $t'=0$ we require reconstruction with all of the shares and recover the result of Lemma 9. Note that if we are interested in maximizing the number of cheaters and minimizing the number of the shares necessary for reconstruction, we can put $t = t' = \left\lfloor \frac{d-1}{4} \right\rfloor$.

4.5. OUTLOOK

We presented a protocol which achieves the task of sharing a quantum secret in a verifiable way, which reduces the number of qubits necessary to realize the protocol. In our scheme each node requires an n-qubit quantum memory and a workspace of at most $3n$ qubits in total. By combining classical encryption with a quantum scheme we showed that we can construct a variety of verifiable hybrid schemes attaining maximum secrecy. We proved that our protocol is secure in the presence of active non-adaptive adversary.

We remark that there is a dependence between the number of cheaters tolerated by a verifiable secret sharing protocol and quantum resources necessary to realize it. The number of cheaters can be increased to $2t$ by using approximate quantum error correction based on quantum authentication schemes [23, 41]. Indeed, in [8] the authors showed that by employing quantum authentication techniques, the VQSS scheme of [7] can tolerate up to $\frac{n}{2}$ malicious nodes. In this case, the power of the verification scheme increases up to the number of tolerable erasures of the code, and one can effectively tolerate twice as many malicious nodes. However, authentication schemes typically require another level of error correction, where the size of the code scales exponentially in the security parameter of the authentication. Therefore, such schemes increase the number of qubits required to realize the protocol.

4.6. TECHNICAL STATEMENTS

Here we state the soundness of the VQSS protocol. Since we use the VQSS in the sequential setting instead of the original parallel one, we restate security in the sequential setting. Our techniques are inspired by the approach suggested in [7, 35].

Proof of Lemma 7. To prove the soundness of the VQSS protocol, we bound the probability that the state held by the nodes after the verification phase is close to a codeword in $\mathscr{C} = V \cap \mathscr{F}W$ with at most t errors on the first level of encoding in the verification phase, or that the protocol aborts, and therefore, the dealer is caught. V denotes a space spanned by $\{|v\rangle : v \in V^C\}$, where V^C is a classical code space. Similarly, $\mathscr{F}W$ is spanned by $\{\mathscr{F}|w\rangle : w \in W^C\}$, where $\mathscr{F}$ is the Fourier transform and W^C is a classical code space such that the dual code $V^{C*} \subseteq W^C$.

Recall that in the protocol we encode the secret of the dealer into two levels of encoding. We will argue that performing verification on the second level of encoding is equivalent to verification on the first level of encoding. If a state is encoded once using $\mathscr{C}$, and has at most t errors, then the encoding defines a unique state. Therefore, it is enough to count the number of errors present in the first level of encoding and verify that there are at most t. However, the protocol requires two levels of encoding to make sure that no node has complete control over all shares. This implies that we cannot perform the verification directly at the first level. But since all the operations we use for verification are (essentially) transversal for code $\mathscr{C}$, we can argue about the verification as if it was performed on the first level.

In order to check for errors, it is enough to check for errors in the Z basis and errors in the X basis. Let V_t be the space of words that have at most t errors in the Z basis as compared to a codeword in V. In particular, if one measures a state $|v\rangle \in V_t$ in the Z basis, the outcome is a word in the space V_t^C, where V_t^C is the space of strings having at

most t compared to a string in the classical code V^C. Similarly, we can define $(\mathscr{F}W)_t$ as the space of words that have at most t errors in the X basis as compared to a codeword in W. This means that if one measures a state $|w\rangle \in (\mathscr{F}W)_t$ in the X basis, the outcome is a word in the space W_t^C, where W_t^C is the space of strings having at most t compared to a string in the classical code W^C.

Considering the above argument, now we proceed with proving soundness of verification of the state in the Z basis and as if we were considering only one level of encoding.

Without loss of generality, we can decompose the state of the nodes after the sharing phase in spaces V_t and $V_t^\perp$,

$$\rho_{sh} = \sum_i q_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|, \tag{4.9}$$

with $|\psi_i\rangle = a_i |\tilde{\psi}_i\rangle + b_i |\tilde{\psi}_i^\perp\rangle$, where $|\tilde{\psi}_i\rangle \in V_t$ and $|\tilde{\psi}_i^\perp\rangle \in V_t^\perp$. In words, the state after the sharing phase is a mixture of pure states which have components in V_t and $V_t^\perp$.

Moreover, let $\rho_{ver(Z)}$ be the state of all the nodes after the verification phase in the Z basis.

We will show that

"conditioned on not aborting, the state $\rho_{ver(Z)}$ is close to a codeword in the space V_t or the verification phase aborts with high probability".

By definition of the space V_t, $\rho_{ver(Z)}$ belongs to V_t, if by measuring it in the Z basis one obtains with certainty an outcome corresponding to a string $v \in V_t^C$. Therefore, we will quantify "the state $\rho_{ver(Z)}$ is close to a codeword in the space V_t" with a high probability of getting an outcome $v \in V_t^C$ when measuring $\rho_{ver(Z)}$. Alternatively, one can think of a situation in which first a measurement on the initial state is performed and then the verification takes place. To prove the security statement we will use a tool called "quantum-to-classical" reduction, which relates the statistics obtained in the two situations. That is, in order to compute the probability of aborting in the verification phase of the VQSS protocol or the probability that the resulting state is in $V \cap \mathscr{F}W$, we will analyze the situation in which the state is measured *before* the verification.

Probability of aborting. In order to evaluate probability of aborting, we will follow the solution suggested in [35] for the parallel execution of the VQSS and we will show how to use this result for the sequential setting. To do so, let us fix a round $(0,m)$, with $m > 0$. For this round we can use the "quantum-to-classical" reduction. It states that the two following situations are equivalent: *(i)* the honest nodes measure their shares of $\rho_{ver(Z)}$ in the standard basis at the end of the verification phase; *(ii)* the honest nodes measure their shares of ρ_{sh} and an m-th ancilla right after they have been distributed, i.e. before running the verification of round $(0,m)$. Formally,

$$\forall m \; \mathscr{M}_0 \mathscr{M}_m CNOT_{0,m}^{b_{0,m}} = \mathscr{M}_m CNOT_{0,m}^{b_{0,m}} \mathscr{M}_m \mathscr{M}_0 \tag{4.10}$$

where $\mathscr{M}_0$ and $\mathscr{M}_m$ denote measurements of the state of the nodes and m-th ancilla respectively. $CNOT_{0,m}^{b_{0,m}}$ denotes a CNOT gate performed with ρ_{sh} as a control and the m-th ancilla as target. Note that if the nodes perform measurements right after the shares

are distributed (situation *(ii)*) they only need to handle classical data from that moment on. Therefore, "quantum-to-classical" reduction means that the verification phase of the quantum VQSS protocol (Q-protocol) can be reduced to a corresponding verification in a classical protocol (C-protocol). That is to say, measurement outcomes in Q-protocol and C-protocol are exactly the same and the moment when the measurement is performed does not change the behavior of the protocol. Since the measurement is performed in the standard basis and the CNOT gate acts as a bit flip in the standard basis, the two operations commute.

Let us look now at the sequential execution of Q-protocol and C-protocol. Expanding the above dependence onto m sequential rounds, we obtain

$$\begin{aligned} &\mathscr{M}_0\mathscr{M}_r CNOT_{0,r}^{b_{0,r}} \ldots \mathscr{M}_1 CNOT_{0,1}^{b_{0,1}} = \\ &= \mathscr{M}_r CNOT_{0,r}^{b_{0,r}} \mathscr{M}_r \ldots \mathscr{M}_1 CNOT_{0,1}^{b_{0,1}} \mathscr{M}_1 \mathscr{M}_0 \end{aligned} \tag{4.11}$$

In particular, this means that the probability of aborting in the sequential Q-protocol can be reduced to considering the probability of aborting in the sequential C-protocol,

$$\Pr[\neg \text{abort}_Q] = \Pr[\neg \text{abort}_C]. \tag{4.12}$$

Consider the corresponding C-protocol for round ($\ell = 0, m$): the nodes have *classical* bit strings $v_{0,0}$ and $v_{0,m}$. They wish to verify whether $v_{0,0}$ is a string in the space V_t^C. To do so the (honest) nodes compute bit-wise $v_{0,m} + b_{0,m} v_{0,0}$ according to public random bit $b_{0,m}$. They broadcast the result and create the set of apparent cheaters B.

In the C-protocol, the string $v_{0,0}$ can either be a string in V_t^C or not. This depends on the shared state (4.9), and therefore happens with probabilities

$$\Pr[v_{0,0} \in V_t^C] = \sum_i q_i |a_i|^2 =: a, \tag{4.13}$$

$$\Pr[v_{0,0} \notin V_t^C] = \sum_i q_i |b_i|^2 =: b, \tag{4.14}$$

respectively. Indeed, the probability that any of the $|\psi_i\rangle$ from (4.9) yields a string from V_t^C (resp. not in V_t^C) is given by $|a_i|^2$ (resp. $|b_i|^2$). In the case when $v_{0,0}$ is a string in V_t^C, the verification always passes and we have that $\Pr[\neg \text{abort}_C | v_{0,0} \in V_t^C] = 1$. On the other hand, if $v_{0,0}$ is not a string in V_t^C, then for all bit strings $v_{0,m}$ there exists at most one bit $b_{0,m}$ such that $v_{0,m} + b_{0,m} v_{0,0}$ is a string in V_t^C. Since $b_{0,m}$ is chosen independently of $v_{0,m}$ and $v_{0,0}$, and uniformly at random, the probability that $v_{0,m} + b_{0,m} v_{0,0}$ a codeword is at most $\frac{1}{2}$. Since the above is true for any value of $v_{0,m}$, in particular it must be true even if $v_{0,m}$ depends on the previous rounds $1, \ldots, m-1$. Therefore, the overall probability p that the verification phase of the C-protocol does not abort given that $v_{0,0}$ is not a string in V_t^C, is at most

$$p = \Pr[\neg \text{abort}_C | v_{0,0} \notin V_t^C] \leq 2^{-r}. \tag{4.15}$$

The above consideration allows us to write that the probability of the C-protocol not aborting is

$$\begin{aligned} \Pr[\neg \text{abort}_C] = &\Pr[v_{0,0} \in V_t^C] \Pr[\neg \text{abort}_C | v_{0,0} \in V_t^C] \\ &+ \Pr[v_{0,0} \notin V_t^C] \Pr[\neg \text{abort}_C | v_{0,0} \notin V_t^C]. \end{aligned} \tag{4.16}$$

Since $\Pr[\neg\text{abort}_Q] = \Pr[\neg\text{abort}_C]$, Equation (4.12), in the Q-protocol we have

$$\Pr\left[\neg\text{abort}_Q\right] = a + pb. \tag{4.17}$$

Probability of measuring a string in V_t^C. Now our objective is to evaluate $\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right]$. By "quantum-to-classical" reduction argument (4.11), we know that the C-protocol should yield the same statistics as the Q-protocol,

$$\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] = \Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_C\right]. \tag{4.18}$$

From the considerations about the probability of aborting, using the rules of probability, we can compute

$$\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] = \frac{a}{a+pb}. \tag{4.19}$$

Now let us combine the statements about probability of aborting and probability of measuring a string in V_t^C. Using the "quantum-to-classical" reduction, we can formally reformulate the initial statement "conditioned on not aborting, the state $\rho_{ver(Z)}$ is close to a codeword in the space V_t, or the verification phase aborts with high probability" as

$$\begin{cases} \Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] > 1-\delta \\ \text{or} \\ \Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] \leq 1-\delta \\ \qquad \text{and } \Pr\left[\text{abort}_Q\right] \geq 1 - \frac{2^{-r}}{\delta} \end{cases} \tag{4.20}$$

where δ is a threshold for probability of measuring a string from V_t^C. Indeed, using equations (4.17) and (4.19) we can express $\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right]$ as a function of $\Pr[\neg\text{abort}_Q]$,

$$\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] = \frac{\Pr[\neg\text{abort}_Q] - p}{\Pr[\neg\text{abort}_Q](1-p)} \tag{4.21}$$

Now, either $\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] > 1-\delta$ and the first condition is satisfied, or $\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] \leq 1-\delta$ and using (4.21) we get

$$\Pr\left[\neg\text{abort}_Q\right] \leq \frac{p}{\delta} \leq \frac{2^{-r}}{\delta}, \tag{4.22}$$

and therefore $\Pr\left[\text{abort}_Q\right] \geq 1 - \frac{2^{-r}}{\delta}$.

In analogy to the above reasoning, one can construct an argument for a check in the X basis. Therefore, we can write

$$\begin{cases} \Pr\left[w_{0,0} \in W_t^C | \neg\text{abort}_Q\right] > 1-\delta' \\ \text{or} \\ \Pr\left[w_{0,0} \in W_t^C | \neg\text{abort}_Q\right] \leq 1-\delta' \\ \qquad \text{and } \Pr\left[\text{abort}_Q\right] \geq 1 - \frac{2^{-r}}{\delta'} \end{cases} \tag{4.23}$$

where δ' is a threshold for probability of measuring a string from W_t^C.

Furthermore, in the protocol we verify that each of the $|\bar{0}\rangle$ ancilla states is sufficiently close to space V_t before running the verification in the X basis. Let V_t^{0C} be a subspace of the code V_t^C whose codewords are entries in the logical $|\bar{0}\rangle$, i.e. $0 + (W^{C*})_t$, where the dual code $(W^{C*})_t \subseteq V_t^C$. Then V_t^0 is a subspace of V_t, such that V_t^0 is spanned by $\{|v\rangle : v \in V_t^{0C}\}$. Formally, we verify that conditioned on not aborting, the actual state of the ancilla is close to a codeword in V_t^0, or the verification phase aborts with high probability,

$$\begin{cases} \Pr\left[v \in V_t^{0C} | \neg \text{abort}_Q\right] > 1 - \delta'' \\ \text{or} \\ \Pr\left[v \in V_t^{0C} | \neg \text{abort}_Q\right] \leq 1 - \delta'' \\ \qquad \text{and } \Pr\left[\text{abort}_Q\right] \geq 1 - \frac{2^{-r}}{\delta''} \end{cases} \tag{4.24}$$

where δ'' is a threshold for probability of measuring a string from V_t^{0C}. Since there are r of ancilla checks, the probability that measuring all of the $|\bar{0}\rangle$ states yield a codeword from space V_t^{0C} can be written as

$$\Pr\left[\bigwedge_{\ell=1}^{r} v_{\ell,0} \in V_t^{0C} \middle| \neg \text{abort}_Q\right] \geq 1 - r\delta''. \tag{4.25}$$

The purpose of having $|\bar{0}\rangle \in V_t^0$ is that using these ancillas for verification in the X basis will not introduce bit flip errors in the Z basis. In other words, any state in V_t remains in V_t after its verification in the X basis, as long as we use ancillas $|\bar{0}\rangle \in V_t^0$.

We will now make a statement about the whole verification phase. Let the state of the nodes after the verification in the Z basis have the form

$$\rho_{ver(Z)|b_Z \neq 0} = \alpha \rho_{V_t} + \beta \rho_{V_t^\perp} \tag{4.26}$$

where ρ_{V_t} is a mixture of pure states in V_t and $\rho_{V_t^\perp}$ is a mixture of pure states in $V_t^\perp$. Here we condition the state on the fact that the public random bits b_Z used in the verification in the standard basis (i.e. $b_{0,m}$ for $m = 1, \ldots, r$) are all different than 0, i.e. that at least one CNOT gate is performed. In this case, measuring the state of the nodes after the CNOT, projects it either on V_t or $V_t^\perp$. It happens with probabilities α and β, respectively.

Similarly, after the consecutive verification in the X basis, the state of the nodes will be

$$\begin{aligned} &\rho_{ver(Z,X)|b_Z, b_X \neq 0, |\bar{0}\rangle \in V_t^0} = \\ &= \alpha\alpha' \rho_{V_t \cap \mathcal{F}W_t} + \alpha\beta' \rho_{V_t^\perp \cap \mathcal{F}W_t} \\ &\quad + \beta\left(\alpha'' \rho_{V_t \cap \mathcal{F}W_t^\perp} + \beta'' \rho_{V_t^\perp \cap \mathcal{F}W_t^\perp}\right), \end{aligned} \tag{4.27}$$

where we additionally condition the state on the fact that bits b_X used for verification in the X basis are all different than zero (i.e. at least one CNOT was performed in the X

basis). Moreover, we condition it on the fact that $|\bar{0}\rangle$ ancillas used for verification in the X basis are in V_t^0. Assuming the first lines of Equations (4.20) and (4.23), we get that

$$\alpha\alpha' + \alpha\beta' > 1-\delta \tag{4.28}$$
$$\alpha\alpha' + \beta\alpha'' > 1-\delta' \tag{4.29}$$

The first line implies that $\beta(\alpha'' + \beta'') \leq \delta$ and therefore, $\beta \leq \delta$. Using this in the second line we get that $\alpha\alpha' \geq 1-\delta-\delta'$. Now, $\alpha\alpha'$ is exactly the probability that measuring $\rho_{ver(Z,X)|b_Z,b_X\neq 0,|\bar{0}\rangle\in V_t^0}$ in the Z basis yields a string in V_t^C *and* measuring it in the X basis yields a string in W_t^C. Therefore, we get,

$$\begin{aligned}\Pr\left[v_{0,0}\in V_t^C \wedge w_{0,0}\in W_t^C | \neg\text{abort}, b_Z, b_X\neq 0, |\bar{0}\rangle\in V_t^0\right] \\ \geq 1-\delta-\delta'.\end{aligned} \tag{4.30}$$

Now we will lower-bound the probability $\Pr\left[v_{0,0}\in V_t^C \wedge w_{0,0}\in W_t^C|\neg\text{abort}\right]$ i.e. remove the conditioning on $b_Z, b_X \neq 0, |\bar{0}\rangle \in V_t^0$ from the above probability expression. Let us evaluate,

$$\begin{aligned}&\Pr\left[v_{0,0}\in V_t^C \wedge w_{0,0}\in W_t^C|\neg\text{abort}\right] = \\ &= \Pr\left[b_Z, b_X\neq 0 \wedge |\bar{0}\rangle\in V_t^0|\neg\text{abort}\right]\Pr\left[v_{0,0}\in V_t^C \wedge w_{0,0}\in W_t^C|\neg\text{abort}, b_Z, b_X\neq 0, |\bar{0}\rangle\in V_t^0\right] + \\ &+ \underbrace{\Pr\left[\neg(b_Z, b_X\neq 0)\vee|\bar{0}\rangle\notin V_t^0|\neg\text{abort}\right]}_{\leq r2^{-r}+\Pr[|\bar{0}\rangle\notin V_t^0|\neg\text{abort}]\leq r2^{-r}+r\delta''}\underbrace{\Pr\left[v_{0,0}\in V_t^C \wedge w_{0,0}\in W_t^C|\neg\text{abort}, \neg(b_Z, b_X\neq 0), |\bar{0}\rangle\notin V_t^0\right]}_{\leq 1},\end{aligned} \tag{4.31}$$

where we assumed the first line of Equation (4.24) to bound $\Pr\left[|\bar{0}\rangle\notin V_t^0|\neg\text{abort}\right]$. To sum up, the conjunction of

$$\begin{aligned}&\Pr\left[v_{0,0}\in V_t^C|\neg\text{abort}_Q\right] > 1-\delta \\ &\Pr\left[w_{0,0}\in W_t^C|\neg\text{abort}_Q\right] > 1-\delta' \\ &\Pr\left[\bigwedge_{\ell=1}^{r} v_{\ell,0}\in V_t^{0C}\middle|\neg\text{abort}_Q\right] \geq 1-r\delta''\end{aligned} \tag{4.32}$$

implies that

$$\begin{aligned}\Pr\left[v_{0,0}\in V_t^C \wedge w_{0,0}\in W_t^C|\neg\text{abort}\right] \geq \\ \geq (1-\delta-\delta') + r(2^{-r}+\delta'')(\delta+\delta').\end{aligned} \tag{4.33}$$

Therefore, either Equation (4.33) is satisfied or at least one of the equations in (4.32) not satisfied. In the latter case, Equations (4.20), (4.23) and (4.24) imply that

$$\Pr[\text{abort}] \geq 1-\max\left\{\frac{2^{-r}}{\delta}, \frac{2^{-r}}{\delta'}, \frac{2^{-r}}{\delta''}\right\} \tag{4.34}$$

□

Proof of Lemma 8. If the dealer is honest, the size of set B must be at most t – there is at most t malicious nodes and only real malicious nodes are accused of cheating. Therefore, the verification phase will always lead to accepting an honest dealer.

If R is also honest then we must calculate the probability that the verification phase fails to identify the set B of apparent malicious nodes. In this case, the reconstruction phase could take inconsistent shares to reconstruct the original state of the dealer. We can use the "quantum-to-classical" reduction argument again (see [35] and the argument above) and argue about the probability of error for the classical protocol. An error in the classical case can occur when any of the checks for Z or X basis, or checks of $|\bar{0}\rangle$, lead to consistent strings on V_t^C, $\mathscr{F}W_t^C$ or V_t^{C0}. Similarly to the argument above, the probability of that occurring is

$$\epsilon_c = (2+r)2^{-r} \tag{4.35}$$

4

Let us now look at the reconstruction phase of the quantum protocol to bound the fidelity of the output state. When the reconstructor is honest, she first applies a decoding operator to each branch i corresponding to node $i \notin B$. The operator corrects errors without knowledge of the positions which carry errors (i.e. it corrects arbitrary errors). Therefore, whenever in qubits corresponding to branch $i \notin B$ there is no more than t errors, the decoding will identify the errors and correct them. In the case when there are more than t errors in a branch i, the procedure will leave that branch untouched and the reconstructor will update the set B with position i. Secondly, the honest reconstructor applies an erasure-recovery circuit to randomly chosen $n-2t$ positions from $i \notin B$. In the case when all of the errors are correctly identified in B, the erasure-recovery corrects for $n-2t$ erasure errors, i.e. missing qubits of the dealer and malicious nodes, and outputs the original state of the dealer. Since the verification phase can fail to identify the set B with probability ϵ_c, we have:

$$\rho_{rec} = (1-\epsilon_c)\left|\psi\right\rangle\!\left\langle\psi\right| + \epsilon_c \tilde{\rho}_R, \tag{4.36}$$

where $\tilde{\rho}_R$ is an arbitrary state that depends on the action of the malicious nodes. Let us define the fidelity of the reconstructed state as $F = \mathrm{Tr}\left[\rho_{rec}\left|\psi\right\rangle\!\left\langle\psi\right|_R\right]$. Using linearity properties of the trace together with the fact that quantum states have non-zero trace, we have that

$$\begin{aligned} F &= \mathrm{Tr}\left[\left((1-\epsilon_c)\left|\psi\right\rangle\!\left\langle\psi\right| + \epsilon_c\tilde{\rho}\right)\ \left|\psi\right\rangle\!\left\langle\psi\right|\right] \\ &= (1-\epsilon_c)\,\mathrm{Tr}\left[\left|\psi\right\rangle\!\left\langle\psi\right|\left|\psi\right\rangle\!\left\langle\psi\right|\right] + \underbrace{\epsilon_c\,\mathrm{Tr}\left[\tilde{\rho}\ \left|\psi\right\rangle\!\left\langle\psi\right|\right]}_{\geq 0} \\ &\geq 1-\epsilon_c. \end{aligned} \tag{4.37}$$

□

REFERENCES

[1] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, *Verifiable secret sharing and achieving simultaneity in the presence of faults,* in *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, SFCS '85 (IEEE Computer Society, Washington, DC, USA, 1985) pp. 383–395.

[2] P. Feldman, *A practical scheme for non-interactive verifiable secret sharing,* in *28th Annual Symposium on Foundations of Computer Science (sfcs 1987)* (1987) pp. 427–438.

[3] W. Du and M. J. Atallah, *Secure multi-party computation problems and their applications: A review and open problems,* in *Proceedings of the 2001 Workshop on New Security Paradigms*, NSPW '01 (ACM, New York, NY, USA, 2001) pp. 13–22.

[4] P. Feldman and S. Micali, *An optimal probabilistic protocol for synchronous byzantine agreement,* SIAM J. Comput. **26**, 873 (1997).

[5] P. Y. A. Ryan, S. Schneider, and V. Teague, *End-to-end verifiability in voting systems, from theory to practice,* IEEE Security Privacy **13**, 59 (2015).

[6] X. Défago, A. Schiper, and P. Urbán, *Total order broadcast and multicast algorithms: Taxonomy and survey,* ACM Comput. Surv. **36**, 372 (2004).

[7] C. Crépeau, D. Gottesman, and A. Smith, *Secure multi-party quantum computation,* in *Proceedings of the Thirty-fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (ACM, New York, NY, USA, 2002) pp. 643–652.

[8] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, *Secure multiparty quantum computation with (only) a strict honest majority,* in *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)* (2006) pp. 249–260.

[9] M. Ben-Or and A. Hassidim, *Fast quantum byzantine agreement,* in *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05 (ACM, New York, NY, USA, 2005) pp. 481–485.

[10] A. Shamir, *How to share a secret,* Commun. ACM **22**, 612 (1979).

[11] G. R. Blakley, *Safeguarding cryptographic keys,* in *Managing Requirements Knowledge, International Workshop on* (IEEE Computer Society, Los Alamitos, CA, USA, 1979) p. 313.

[12] H. Krawczyk, *Secret sharing made short,* in *Advances in Cryptology — CRYPTO' 93*, edited by D. R. Stinson (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994) pp. 136–146.

[13] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing,* Phys. Rev. A **59**, 1829 (1999).

[14] A. Karlsson, M. Koashi, and N. Imoto, *Quantum entanglement for secret sharing and secret splitting,* Phys. Rev. A **59**, 162 (1999).

[15] K. Chen and H. Lo, *Multi-partite quantum cryptographic protocols with noisy GHZ states,* Quantum Information & Computation **7**, 689 (2007).

[16] L. Xiao, G. Lu Long, F.-G. Deng, and J.-W. Pan, *Efficient multiparty quantum-secret-sharing schemes,* Phys. Rev. A **69**, 052307 (2004).

[17] R. Cleve, D. Gottesman, and H.-K. Lo, *How to share a quantum secret,* Phys. Rev. Lett. **83**, 648 (1999).

[18] D. Gottesman, *Theory of quantum secret sharing,* Phys. Rev. A **61**, 042311 (2000).

[19] D. Markham and B. C. Sanders, *Graph states for quantum secret sharing,* Phys. Rev. A **78**, 042309 (2008).

[20] A. Marin and D. Markham, *Equivalence between sharing quantum and classical secrets and error correction,* Phys. Rev. A **88**, 042332 (2013).

[21] J. Javelle, M. Mhalla, and S. Perdrix, *New protocols and lower bounds for quantum secret sharing with graph states,* in *Theory of Quantum Computation, Communication, and Cryptography*, edited by K. Iwama, Y. Kawano, and M. Murao (Springer Berlin Heidelberg, Berlin, Heidelberg, 2013) pp. 1–12.

[22] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, *Experimental demonstration of graph-state quantum secret sharing,* Nature Communications **5**, 5480 (2014).

[23] C. Crépeau, D. Gottesman, and A. Smith, *Approximate quantum error-correcting codes and secret sharing schemes,* in *Advances in Cryptology – EUROCRYPT 2005*, edited by R. Cramer (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 285–301.

[24] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned,* Nature **299**, 802 (1982).

[25] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, *Quantum secret sharing schemes and reversibility of quantum operations,* Phys. Rev. A **72**, 032318 (2005).

[26] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, *Improving quantum secret-sharing schemes,* Phys. Rev. A **64**, 042311 (2001).

[27] V. Gheorghiu, *Generalized semiquantum secret-sharing schemes,* Phys. Rev. A **85**, 052309 (2012).

[28] B. Fortescue and G. Gour, *Reducing the quantum communication cost of quantum secret sharing,* IEEE Transactions on Information Theory **58**, 6659 (2012).

[29] S. K. Singh and R. Srikanth, *Generalized quantum secret sharing,* Phys. Rev. A **71**, 012328 (2005).

[30] S. Bravyi, G. Smith, and J. A. Smolin, *Trading classical and quantum computational resources,* Physical Review X **6**, 021043 (2016).

[31] M. Steudtner and S. Wehner, *Fermion-to-qubit mappings with varying resource requirements for quantum simulation,* New Journal of Physics **20**, 063010 (2018).

[32] N. Moll, A. Fuhrer, P. Staar, and I. Tavernelli, *Optimizing qubit resources for quantum chemistry simulations in second quantization on a quantum computer,* Journal of Physics A: Mathematical and Theoretical **49**, 295301 (2016).

[33] S. Bravyi, J. M. Gambetta, A. Mezzacapo, and K. Temme, *Tapering off qubits to simulate fermionic hamiltonians,* arXiv preprint arXiv:1701.08213 (2017).

[34] T. Peng, A. Harrow, M. Ozols, and X. Wu, *Simulating large quantum circuits on a small quantum computer,* arXiv preprint arXiv:1904.00102 (2019).

[35] A. Smith, *Multi-party quantum computation,* (2001), arXiv:quant-ph/0111030 .

[36] T. Rabin and M. Ben-Or, *Verifiable secret sharing and multiparty protocols with honest majority,* in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89 (ACM, New York, NY, USA, 1989) pp. 73–85.

[37] D. R. Stinson and R. Wei, *Unconditionally secure proactive secret sharing scheme with combinatorial structures,* in *Selected Areas in Cryptography*, edited by H. Heys and C. Adams (Springer Berlin Heidelberg, Berlin, Heidelberg, 2000) pp. 200–214.

[38] M. Mosca, A. Tapp, and R. Wolf, *Private quantum channels and the cost of randomizing quantum information,* (2000), arXiv:quant-ph/0003101 .

[39] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, *Multicast security: a taxonomy and some efficient constructions,* in *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, Vol. 2 (1999) pp. 708–716 vol.2.

[40] R. Canetti, *Universally composable signature, certification, and authentication,* in *Proceedings. 17th IEEE Computer Security Foundations Workshop, 2004.* (2004) pp. 219–233.

[41] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, *Authentication of quantum messages,* in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* (2002) pp. 449–458.

[42] A. J. Landahl, J. T. Anderson, and P. R. Rice, *Fault-tolerant quantum computing with color codes,* (2011), arXiv:1108.5738 .

[43] S. B. Bravyi and A. Y. Kitaev, *Quantum codes on a lattice with boundary,* (1998), arXiv:quant-ph/9811052 .

[44] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist,* Phys. Rev. A **54**, 1098 (1996).

[45] A. Steane, *Multiple-particle interference and quantum error correction,* Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **452**, 2551 (1996).

[46] D. Unruh, *Universally composable quantum multi-party computation,* in *Advances in Cryptology – EUROCRYPT 2010*, edited by H. Gilbert (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010) pp. 486–505.

[47] M. M. Prabhakaran and A. Sahai, *Secure multi-party computation*, Vol. 10 (IOS press, 2013).

[48] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai, *Universally composable two-party and multi-party secure computation,* in *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (Association for Computing Machinery, New York, NY, USA, 2002) p. 494–503.

[49] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, USA, 2011).

[50] E. Knill, R. Laflamme, and L. Viola, *Theory of quantum error correction for general noise,* Phys. Rev. Lett. **84**, 2525 (2000).

[51] D. Aharonov and M. Ben-Or, *Fault-tolerant quantum computation with constant error,* in *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97 (ACM, New York, NY, USA, 1997) pp. 176–188.

[52] B. Schoenmakers, *A simple publicly verifiable secret sharing scheme and its application to electronic voting,* in *Advances in Cryptology — CRYPTO' 99*, edited by M. Wiener (Springer Berlin Heidelberg, Berlin, Heidelberg, 1999) pp. 148–164.

5

SECURE MULTIPARTY QUANTUM COMPUTATION

We consider the task of secure multiparty distributed quantum computation on a quantum network. We propose a protocol based on quantum error correction which reduces the number of necessary qubits. That is, each of the n nodes in our protocol requires an operational workspace of $n^2 + 4n$ qubits, as opposed to previously shown $\Omega\big((n^3 + n^2 s^2)\log n\big)$ qubits, where s is a security parameter. Additionally, we reduce the communication complexity by a factor of $\mathcal{O}(n^3 \log(n))$ qubits per node, as compared to existing protocols. To achieve universal computation, we develop a distributed procedure for verifying magic states, which allows us to apply distributed gate teleportation and which may be of independent interest. We showcase our protocol on a small example for a 7-node network.

This chapter has been published, with minor changes, in V. Lipinska, J. Ribeiro, and S. Wehner, *Secure multiparty quantum computation with few qubits*, Phys. Rev. A 102, 022405 (2020).

5.1. INTRODUCTION

Secure multiparty computation is a task which allows n nodes of a network to jointly compute a function on their inputs [1]. The inputs are private, meaning that they are only known to the nodes who supplied them. What is more, the only information that can be inferred about the private inputs is whatever can be inferred from the outputs of the computation and the computation itself. Multiparty computation allows for distributed evaluation of any function, and hence it is a powerful cryptographic primitive with many practical (e.g. clearing a commodity derivative market) and theoretical (e.g. zero knowledge proofs) applications [2].

In the domain of quantum computation the problem of multiparty quantum computation (MPQC) on quantum data was first introduced by [3]. It can be defined as follows: each node $i = 1,\dots,n$ gets one, possibly unknown, input quantum state ρ_i. The nodes jointly perform an n-input arbitrary quantum circuit $\mathfrak{R}$ on their inputs $\rho_1,\dots,\rho_n$. The output of the circuit is divided into n parts and each node i gets i-th part of the output state, see Figure 5.1. In MPQC there can be nodes who do not follow the protocol (cheaters). We then require that an MPQC protocol satisfies the following informal requirements:

- (Correctness) If there are no cheaters, then the protocol implements the intended circuit $\mathfrak{R}$ on the inputs of the nodes.
- (Soundness) Cheaters cannot affect the outcome of the computation of the other nodes, beyond their ability to choose their own inputs.
- (Privacy) Cheaters do not learn anything about private inputs and outputs of the other nodes.

Throughout this paper we will consider that an input ρ_i of each node is a single-qubit state.

The approach taken by the original work of [3] is based on a subroutine called verifiable quantum secret sharing and is a generalization of a classical multiparty computation [**?**]. The security achieved by the protocol is information theoretical, meaning that the cheaters are not constrained by computational assumptions. However, the number of cheaters has to be strictly smaller than $\frac{n}{6}$. This bound was later lifted to $\frac{n}{2}$ by [4], who used authentication schemes and approximate error correction. However this solution requires significantly more qubits to be realized. At the same time, there exist parallel approaches tolerating a cheating majority and whose security relies on computational assumptions, for example [5] for the case of $n = 2$ or its recent generalization to $n > 2$ [6]. Note that a protocol tolerating more than $\frac{n}{2}$ cheaters is not possible without additional computational assumptions, since that would imply the existence of unconditionally secure bit commitment [7, 8].

In this work we are interested in the former approach to MPQC, namely the one based on verifiable quantum secret sharing of [3]. Our objective is to perform MPQC on a quantum network with n nodes using as few qubits as possible. The approach we take is based on [3] and extensively relies on techniques from fault-tolerant quantum error correction. It can be intuitively understood as follows. Nodes use a chosen quantum error correcting code and create a global logical state $\bar{\Psi}$ by encoding each of the single-qubit input states. Each node holds a part of this logical state, we call such a part a *share*. They verify the encoding of each state using verifiable secret sharing protocol and

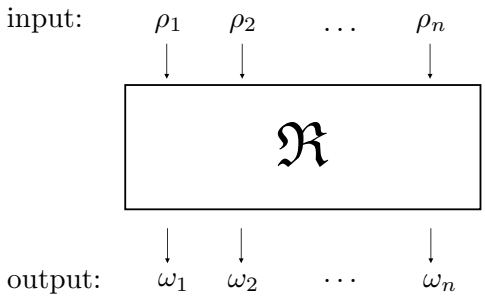


Figure 5.1: Each of the nodes $1,\ldots,n$ provides a single-qubit input $\rho_1,\ldots,\rho_n$. The goal of the multiparty quantum computation (MPQC) protocol is to implement circuit $\mathfrak{R}$ such that each node gets an output $\omega_1,\ldots,\omega_n$ without gaining any knowledge of the other inputs or outputs beyond their ability to choose their own inputs. Note that the inputs (and outputs) can be entangled.

Table 5.1: Summary of qubit savings presented in this paper, s denotes the security parameter of the protocol, #ancillas denotes the number of ancillas in circuit $\mathfrak{R}$, $\#T$ denotes the number of T gates, and #Toff is the number of Toffoli gates. The size of the workspace in our protocol does not depend on the security parameter, because of the sequential execution of the verification phase, see Section 5.3.2. Note that here we do not list the work of [6], since their protocol does not use techniques based on error correction and achieves computational security guarantees.

	Our protocol	Crepeau et al. [3]
size of the input in qubits per node	1	$\Omega(\log n)$
size of an individual share during the computation in qubits per node	1	$\Omega(\log n)$
# qubits in workspace per node	n^2+4n	$\Omega\big((n^3+n^2s^2)\log n\big)$
# qubits sent per node	$\mathcal{O}\big((n+\#\text{ancillas}+\#T)ns^2\big)$	$\mathcal{O}\big((n^2+\#\text{ancillas}+\#\text{Toff})n^3s^2\log(n)\big)$

perform local operations to evaluate a logical version of the circuit $\mathfrak{R}$, and then locally reconstruct their outputs.

To be able to apply any circuit $\mathfrak{R}$ this way, we need two properties. First, $\mathfrak{R}$ needs to be composed of gates which form a universal set, i.e. any circuit can be decomposed into gates from that set. Second, if the nodes apply only local operations Λ from the universal set, it should yield a meaningful logical operation $\bar{\Lambda}$ for the global state $\bar{\Psi}$. This property is called *transversality*. However, for any error correcting code, it is impossible to perform universal quantum computation using only transversal gates [9]. For this reason, it is common to extend a transversal set of gates (for example Clifford gates) with a non-transversal gate (for example T gate or the Toffoli gate). Note that there exist methods to realize single non-transversal gates in a distributed way, for example by using ancilla states [10] or locally modifying the error correcting code [11].

In particular, [3] considers quantum polynomial codes and a universal set of gates with the Toffoli gate [11]. This solution is very expensive in qubits. Firstly, the polynomial codes require local shares whose dimension scales with the number of nodes, and therefore require $\Omega(\log n)$ qubits per share. Moreover, the nodes need to perform a distributed encoding of the shares in order to apply the Toffoli gate. This means that each input state must be encoded three times using the polynomial code. Performing the three-level en-

coding serves one more purpose, namely, it localizes all of the errors in the encoding to the positions of the cheaters. As a result, the cheaters cannot force the protocol to abort, since any error they introduce will always be corrected by the underlying polynomial code. All in all, each node needs an operational workspace of $\Omega\big((n^3 + n^2 s^2)\log n\big)$ qubits, where s is the security parameter of the protocol, see Table 5.1. We remark that in schemes based on exact error correcting codes, the number of cheaters t is intrinsically constrained by the distance d of the underlying code as $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, which in principle can reach $\frac{n}{4}$ [12, 13]. However, the technique for applying the Toffoli gate in [3] puts a constraint on the number of cheaters to $\frac{n}{6}$.

Since near-term quantum networks will be able to support only a small number of qubits, it would be preferable to implement an MPQC protocol with as few qubits as possible. So far, reducing quantum resources has received a lot of attention in the domain of non-distributed quantum computation and simulation, see for example [14–18]. Recently, in [19] we considered a problem of reducing quantum resources for a distributed protocol, namely verifiable secret sharing of a quantum state. Here we address a similar issue of whether distributed multiparty quantum computation can be performed on a quantum network with less quantum resources. We answer this question positively by proposing a scheme for universal distributed computation which uses fewer qubits as compared to the existing approach of [3] outlined above.

This paper is organized as follows. In Section 5.2 we summarize our contributions, where in 5.2.1 we discuss the implications of our protocol on resource reduction and in 5.2.2 we give an explicit example of the protocol on a 7-node network. In Section 5.3 we zoom in on the technical aspects of our work. There we present the protocol in detail and provide formal security statements. We leave out technical proofs for Appendix 5.5.

5.2. RESULTS

We propose a protocol for secure multi-party quantum computation where each node holds single-qubit shares. Our approach is based on quantum error correcting codes, similar to the idea of [3, 4, 20]. The key to our results is using error correcting codes which encode a single qubit into n single qubits. Since our interest lies in reducing the quantum resources necessary to realize the protocol, we abandon the original idea of three-level encoding at the cost of allowing the protocol to abort if the initial encoding of the shares is incorrect. Thanks to this, we are able to execute the protocol with less qubits in the workspace per node and lower communication complexity, see Table 5.1. Moreover, we develop a procedure for a distributed verification of any logical state which is stabilized by a Clifford gate. This allows us to perform distributed gate teleportation and implement a universal set of gates without creating three levels of encoding. What is more, we follow the approach outlined in [19] which allows for a sequential execution of the verification of the inputs. This solution reduces the operational workspace to n^2+4n qubits per node. We elaborate on these techniques in the next section, Section 5.2.1. We show that our protocol is secure in the presence of active non-adaptive cheaters (see Adversary model), where the number of cheaters is constrained by the distance d of the underlying error correcting code, i.e. $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$. Finally, we showcase our protocol on a small example for 7 nodes using Steane's 7-qubit code [21].

Outline 1 (Multiparty quantum computation)**.**
Input: single-qubit state ρ_i from each node, CSS code $\hat{\mathscr{C}}$ with transversal Cliffords, circuit $\mathfrak{R}$.

1. *Sharing and verification*
   Each node $i = 1,\ldots,n$ encodes her input ρ_i using code $\hat{\mathscr{C}}$ into an n-qubit logical state, and sends one qubit (i.e. one single-qubit share) of the logical state to every other node, while keeping one for herself. The nodes jointly verify the encoding done by node i using verifiable quantum secret sharing protocol (see Protocol 1).

2. *Computation*

   - For every Clifford gate in circuit $\mathfrak{R}$:
     The nodes apply transversal Clifford gates locally to qubits specified by the circuit $\mathfrak{R}$.

   - For every T gate in circuit $\mathfrak{R}$ applied to qubit i:
     Node i prepares the magic state $|m\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle)$. The nodes verify it using Verification of Clifford-Stabilized States protocol, see Protocol 3. If the verification is successful, the nodes perform Distributed Gate Teleportation, see Protocol 2.

   Every $|0\rangle$ ancilla state required for circuit $\mathfrak{R}$, which is prepared by node i, is jointly verified by the nodes using verifiable quantum secret sharing, Protocol 1.

   If the verification of any step fails the nodes substitute their shares for $|0\rangle$ and abort the protocol at the end of the computation.

3. *Reconstruction*
   Each node i collects all shares of her part of the output. She corrects errors using code $\hat{\mathscr{C}}$ and reconstructs her output.

Network model. We consider a quantum network with n nodes. Each node can locally process $\mathscr{O}(n^2)$ qubits, and can perfectly process and store classical information. Each pair of nodes is connected via private and authenticated classical [22] and quantum [23] channels. Additionally, we assume that the nodes have access to an authenticated classical broadcast channel [24] and a public source of randomness. Note that a source of randomness can be created, for example, by running a classical multiparty computation protocol [25].

Adversary model. We say that t out of n nodes are *active* cheaters during the protocol. This means that they can act maliciously throughout the entire execution of the multiparty computation and perform arbitrary joint quantum operations on their shares, possibly with quantum side information. Therefore, the security of our protocol does

not rely on computational assumptions. We assume that the active cheaters are *non-adaptive*, meaning that they are determined prior to the beginning of the protocol and stay fixed throughout its execution. On the other hand, the nodes which follow the protocol exactly are *honest*. A protocol *tolerates* the presence of t active cheaters if they cannot influence the output of the protocol beyond choosing their own inputs.

5.2.1. TECHNIQUES

Thanks to using single-qubit error correcting codes, distributed verification of magic states, the possibility to abort the protocol and sequential verification of the inputs, our MPQC protocol lowers the number of qubits that each node needs to control and send. Here we discuss in detail all the reductions made by our protocol. Then, we give an explicit example of a protocol based on the 7-qubit Steane's code.

- **Single-qubit CSS codes.** We consider a class of Calderbank-Shor-Steane (CSS) error correcting codes [21, 26], which encode a single logical qubit into n physical qubits, and for which applying Clifford gates is transversal, see Section 5.3.1 for details. In particular, this means that each input state and each encoded ancilla is encoded and distributed using single-qubit shares. For comparison, the protocol of [3] uses a class of polynomial codes, called Reed-Solomon codes [11], where the size of individual share grows with the number of nodes n in the network as $\Omega(\log n)$ qubits.

- **MPQC with abort.** We introduce an "abort" event in the MPQC protocol. That is, the protocol aborts if there are more than t errors introduced by the cheaters, accumulated over all inputs. This condition is necessary, since applying a transversal gate between different logical inputs can still propagate errors between them. As a result, we are able to perform the MPQC protocol on the two-level encoding created by the verifiable quantum secret sharing (VQSS) subroutine, see Section 5.3.2. This allows us to achieve a lower communication complexity – in our protocol each node sends $\mathcal{O}\big((n+\#\text{ancillas}+\#T)ns^2\big)$ qubits, as opposed to $\mathcal{O}\big((n^2+\#\text{ancillas}+\#\text{Toff})n^3s^2\log(n)\big)$ qubits in [3], where s denotes the security parameter of the protocol, #ancillas denotes the number of ancillas in circuit $\mathfrak{R}$, $\#T$ denotes the number of T gates, and #Toff is the number of Toffoli gates. Note that in our protocol we can avoid the abort event by creating the third level encoding, following the idea of [3]. This approach confines the errors of all inputs only to the positions of t cheaters, see Section 5.4 for discussion. However, this solution significantly increases quantum communication complexity. Since our objective is to reduce the number of qubits, we do not consider this approach here.

- **Verification of Clifford-stabilized states.** We develop a distributed method for verifying states stabilized by the Clifford gates, which in particular can be applied to verify magic states. This solution allows us to perform distributed gate teleportation and apply the T gate in a distributed way. Recall that for our MPQC protocol we choose CSS codes with transversal Clifford gates. This, together with distributed gate teleportation and transversal measurements, provides a way to apply a universal set of gates in a distributed way. Thanks to using magic state

ancillas, we can perform the computation on a two-level encoding created during the verification phase (see Protocol 4). This means that each node controls n^2 single-qubit shares of all inputs. In contrast, in the approach of [3] the nodes need to apply a non-linear Toffoli gate to achieve universality of computation. This, in turn, required a workspace of $\Omega\big((n^3+n^2s^2)\log n\big)$ qubits per node.

- **Sequential verification.** We use the verifiable quantum secret sharing (VQSS) protocol of [3] to verify that the encoding was carried out correctly and that at the end of the computation there will be a state to reconstruct. The verification procedure requires ancillary states. However, following the idea developed in [19], we perform the verification in a sequential way. That is, to verify each input we use the ancillas one by one instead of all at once as in [3]. In particular, the nodes use at most $2n$ single-qubit ancillas at a time to verify the input states (or ancillas in $\mathfrak{R}$) and at most $4n$ single-qubit ancillas to apply the T gate.

All in all, this amounts to an operational workspace of at most n^2+4n single qubit shares for our protocol. Out of those, n^2 shares correspond to the input states on which the distributed computation is performed. For comparison, the protocol of [3] requires simultaneous control over $\Omega\big((n^3+n^2s^2)\log n\big)$ qubits per node, where s is the security parameter of the protocol. Moreover, due to introducing the possibility of aborting the protocol, our MPQC scheme lowers the communication complexity. That is, our protocol reduces the number of qubits that each nodes has to send by a factor of $\mathcal{O}(n^3\log(n))$ compared to the protocol of [3].

Finally, when the number of cheaters t is restricted by the distance d of the CSS code, i.e. when $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, we prove that our protocol satisfies the usual security requirements (soundness, completeness and privacy, see above). Our statements follow from the fact that any error correcting code has the ability to correct at most $\left\lfloor \frac{d-1}{2} \right\rfloor$ arbitrary errors and therefore, any errors introduced by the cheaters can be corrected by the honest nodes. What is more, the inputs and outputs of honest nodes will be also private, since if they recover the outputs exactly, then the cheaters get no information about inputs or outputs [27]. Our statements hold with probability exponentially close to 1 in the security parameter s.

5.2.2. EXAMPLE FOR 7 NODES

Let us consider a network of $n = 7$ nodes and assume that the nodes want to perform a CNOT between inputs ρ_1 and ρ_2 of nodes "1" and "2" of the network. For the execution of this protocol we will need a workspace of 28 qubits per node. For the sake of the example, we will also assume that the inputs are pure single-qubit states, $\rho_1 = |\psi_1\rangle\langle\psi_1|$ and $\rho_2 = |\psi_2\rangle\langle\psi_2|$, and that the protocol does not abort. The 7-qubit Steane's code [21] is the smallest example of a qubit CSS code with transversal Cliffords. This code has distance $d = 3$ meaning that it can correct $\left\lfloor \frac{d-1}{2} \right\rfloor = 1$ arbitrary error. This also means that in an MPQC protocol built on the 7-qubit code, we can tolerate $t = 1$ cheater.

Sharing and verification. Node "1" encodes her single-qubit pure input $|\psi_1\rangle$ into 7 physical qubits using the Steane's code encoding map $\mathcal{E}$. She sends one qubit to each of the remaining 6 nodes, while keeping one qubit to herself. Each node again encodes the

received qubit using the Steane's code and shares 6 qubits of that encoding with other nodes. At this point the input state $|\psi_1\rangle$ has been encoded twice, i.e.

$$\bar{\bar{\Psi}}_1 = \mathscr{E}^{\otimes 7} \circ \mathscr{E}(|\psi_1\rangle\langle\psi_1|). \tag{5.1}$$

Each node holds 7 qubits in total.

The nodes run the verification procedure according to [19], verifying that the encoding of each node i was done correctly. The encoding of each input state can be verified one at a time. In one round of verification of a single input, each node uses at most 14 local ancilla qubits. The ancillas shares are encoded twice with the 7 qubit code and distributed in the same way as the input states. The nodes randomly perform the CNOT gate between $\bar{\bar{\Psi}}_1$ and an ancilla, to identify errors possibly introduced by cheating nodes. These ancillas are then measured and the outcome of the measurement allows the nodes to jointly conclude whether verification of the encoding was correct, i.e. whether the distributed input states have at most $t = 1$ error on the same position. If so, then the errors are correctable by the 7 qubit code, and the nodes hold a valid logical state of the code. This procedure is repeated $s^2 + 2s$ times in total, where s is the security parameter.

The same sharing and verification procedure is carried out for node "2" and her single-qubit pure input $|\psi_2\rangle$: it is first shared, as the logical state

$$\bar{\bar{\Psi}}_2 = \mathscr{E}^{\otimes 7} \circ \mathscr{E}(|\psi_2\rangle\langle\psi_2|) \tag{5.2}$$

and then verified. As before, the verification requires at most 14 local ancilla qubits at a time. After the second verification each node holds 14 verified data qubits corresponding to the logical inputs $\bar{\bar{\Psi}}_1 \otimes \bar{\bar{\Psi}}_2$. Note that the input states are never measured.

Computation. Each node applies the CNOT gate locally to shares coming from node "1" and "2". The CNOT gate is a Clifford gate. Therefore, since the inputs are verified to be logical states of the 7 qubit code, applying the CNOT locally is well-defined and yields a logical operation between logical inputs $\bar{\bar{\Psi}}_1 \otimes \bar{\bar{\Psi}}_2$. Let us define the output of the computation $\bar{\bar{\omega}}$,

$$\bar{\bar{\omega}} = \bar{\bar{CNOT}}\left(\bar{\bar{\Psi}}_1 \otimes \bar{\bar{\Psi}}_2\right). \tag{5.3}$$

Reconstruction. Nodes "1" and "2" get all of the shares corresponding to her own outputs, i.e.

$$\bar{\bar{\omega}}_1 = \mathrm{tr}_2(\bar{\bar{\omega}}), \quad \bar{\bar{\omega}}_2 = \mathrm{tr}_1(\bar{\bar{\omega}}). \tag{5.4}$$

They separately run local error correcting circuit of the 7 qubit code on $\bar{\bar{\omega}}_1$ and $\bar{\bar{\omega}}_2$, respectively. They identify errors, see Reconstruction of Protocol 4 for details. This is necessary, since the cheater might have introduced errors during or after the computation, and right before the reconstruction. Each of the nodes "1" and "2" corrects errors and reconstructs her output ω_1 and ω_2, respectively. The outputs are single qubit states, and are such that

$$\omega_1 = \mathrm{tr}_2(CNOT(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|)), \tag{5.5}$$

$$\omega_2 = \mathrm{tr}_1(CNOT(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|)). \tag{5.6}$$

We remark that to tolerate a larger numbers of cheaters t one can use CSS error correcting codes $\hat{\mathscr{C}}$ with a higher distance for which implementing Clifford gates is transversal. For example, using the so called color codes [28], one can construct MPQC with the total number of nodes expressed in the number of cheaters t as $n = 2t^2 + 4t + 1$, $n = 3t^2 + 3t + 1$ and $n = 6t^2 + 1$.

5.3. METHODS

In this section we discuss our MPQC protocol in detail. We lay down the framework by first discussing properties of CSS codes which will be useful for the distributed computation in Section 5.3.1. Then we introduce a few important subroutines, namely Verifiable Secret Sharing (Section 5.3.2), Distributed Gate Teleportation (Section 5.3.2) and Verification of Clifford-Stabilized States (Section 5.3.2). Finally, in Section 5.3.3 we discuss our Multiparty Quantum Computation protocol and state its security in Section 5.3.4.

5.3.1. CSS CODES

In our considerations we will focus on a class of error correcting codes called Calderbank-Shor-Steane (CSS) codes [21, 26]. A CSS code $\mathscr{C}$ is defined through two binary classical linear codes, V and W , satisfying $V^* \subseteq W$, where V^* is the dual code of V. Then, $\mathscr{C} := V \cap \mathscr{F} W$ is a set of states of n qubits which yield a codeword in V when measured in the standard basis, and a codeword in W when measured in the Fourier basis. A code encoding one logical qubit into n physical qubits is commonly denoted with double square brackets $[[n, 1, d]]$. Here d is the distance of the code, which relates to the maximum number of arbitrary errors t which the code can correct as $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$.

In distributed computation each node can only apply local operations. Therefore, we want that logical operations $\bar{\Lambda}$ are implemented by applying local operations Λ on the individual qubits held by the nodes and encoded with $\mathscr{C}$, i.e. $\bar{\Lambda} = \Lambda^{\otimes n}$. This property is called transversality. For our construction of the MPQC protocol we choose specific CSS codes $\hat{\mathscr{C}}$ with transversal operations, which satisfy:

1. $\hat{\mathscr{C}}$ uses the same classical code to correct X and Z errors, i.e. $V = W$.
2. The weight of the stabilizer generators of $\hat{\mathscr{C}}$ is a multiple of 4, and the logical Pauli operators X and Z have weight 1 mod 4, or 3 mod 4.

Property 1 guarantees that the Hadamard gate H can be applied transversally, while property 2 guarantees that the phase gate $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ can be applied transversally. Additionally, note that the CNOT gate is transversal for any CSS code. Since H, P and CNOT generate the Clifford set, one can apply any Clifford gate on the code $\hat{\mathscr{C}}$ transversally [29]. Finally, any CSS code has a property that measurements can be performed qubitwise, but the measurement outcome of every qubit must be communicated classically to obtain the result of the logical measurement.

5.3.2. SUBROUTINES

Here we list and describe the subroutines we will later use as building blocks in our MPQC protocol. We start with reviewing an existing construction of verifiable quantum

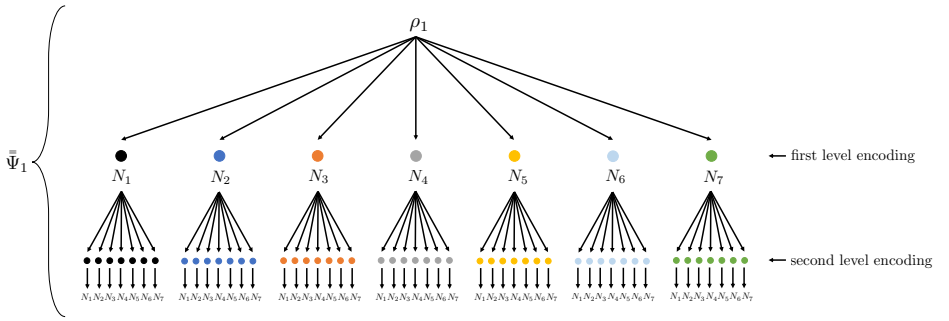


Figure 5.2: Two-level encoding of the input qubit state ρ_1 of node "1". The double-encoded distributed state is denoted by $\bar{\bar{\Psi}}_1$. Each dot represents a single-qubit share.

secret sharing used for verifying inputs in MPQC. Next, we discuss two of our contributions – distributed gate teleportation and verification of states stabilized by Clifford gates. These last two subroutines will be essential for implementing universal circuits in MPQC.

5

VERIFIABLE QUANTUM SECRET SHARING

One of the first ingredients of our MPQC protocol is verifiable quantum secret sharing (VQSS) first introduced in [3], see Protocol 1. Here we use a modified version of the scheme, which we introduced in [19] to reduce the qubit workspace required for each node. A VQSS scheme is a scheme which shares a quantum state among n nodes in a verifiable way using quantum shares. The scheme we use is based on a CSS code $\mathscr{C}$ with distance d, and tolerates at most $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ non-adaptive active cheaters. We remark that the scheme works for any CSS code $\mathscr{C}$.

Let us describe the task in detail. In VQSS the dealer D encodes her input state ρ using the code $\mathscr{C}$. The encoding produces an n-qubit entangled state. D shares this state among the nodes by sending one qubit to each node. Each node then encodes the received one-qubit share again with the same error correcting code into n qubits, and sends one qubit to each of the n nodes. This way each node holds n single-qubit shares. We denote a double-encoded logical global state of the nodes with a double bar, $\bar{\bar{\Psi}}$. Throughout the rest of this chapter we will use index $i = 1,\ldots,n$ to denote the encoding performed by node i, and $\ell = 1,\ldots,n$ to denote the share held by node ℓ. The share held by node ℓ and coming from encoding performed by node i will be denoted as $\bar{\bar{\Psi}}_{i_\ell}$.

The nodes run a verification procedure to verify that $\bar{\bar{\Psi}}$ is a valid codeword of the code $\mathscr{C}$. The verification is a generalization of Steane's error correction method to the distributed setting [30]. More specifically, the nodes publicly check that there are at most $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ errors at the first level of encoding, i.e. the encoding done by the dealer. To do so, they use ancilla qubits encoded twice with the same code $\mathscr{C}$. These ancillas are measured during the verification. Since $\mathscr{C}$ is a CSS code, the measurement outcomes yield a codeword from a classical code V (resp. W) when measured in the standard (resp. Fourier) basis. Using an error correcting procedure for the classical linear codes

allows the nodes to identify shares of the first-level encoding which carry errors. The positions of these shares are collected in a public set B of *apparent* cheaters (indeed, there is no way to tell apart the errors introduced by the dealer and errors introduced by the cheaters on the first-level encoding). If there are at most t first-level errors (i.e. $|B| \leq t$), the dealer passes the verification. Moreover, since the protocol assumes the existence of at most t cheaters, there can be at most t errors in each second-level encoding. Therefore, if the dealer passes the verification, at the end of the protocol there will always be a state to reconstruct, since errors at both first and second level encoding can be corrected by the code $\mathscr{C}$. Following the idea introduced in [19], this verification procedure can be performed by encoding and measuring one ancilla qubit at a time. There are s^2+2s iterations of the verification procedure, where s is the security parameter. Additionally, similarly as in [19], we use CSS codes which encode a single qubit into n single qubits. The sequential VQSS protocol requires a $3n$-qubit workspace per node to verify one single-qubit input state, see [19] for details. Each node needs to send $\mathscr{O}(n^2 s^2)$ qubits.

Protocol 1 (Verifiable Quantum Secret Sharing (VQSS) [3, 19] - outline)**.**
Input: Single-qubit state ρ of dealer D to share, CSS error correcting code $\mathscr{C}$.

1. **Sharing**
   The dealer D encodes her input ρ into a logical state using code $\mathscr{C}$ and sends each qubit of the logical state to every other node, while keeping one for herself. Each node encodes the share received from D again using $\mathscr{C}$ and shares among the nodes keeping one qubit for herself. Therefore, the nodes create a two-level encoding of ρ. At this point each node holds n single-qubit shares coming from every other node.

2. **Verification**
   Nodes verify whether D is honest, i.e. that the shares held by the nodes are consistent with a codeword of $\mathscr{C}$ and at the end of the protocol a state will be reconstructed. The nodes construct a public set B which records positions of nodes with inconsistent shares on the first level of encoding.
   Each node uses at most additional $2n$ ancilla qubits for one iteration of the verification procedure. There are s^2+2s iterations of verification, where s is the security parameter. If $|B| \leq t$ the dealer passes the verification phase.

Verification of logical 0 (VQSS(0)). In the following sections we will make use of a handy property of the VQSS protocol of [3]. Namely, the protocol can verify that the state shared by the nodes is exactly the logical $|\bar{0}\rangle$ of code $\mathscr{C}$, see [3, 19, 20]. The verification phase is almost the same as in the VQSS protocol of [3], except now the nodes check whether the classical measurement outcomes interpolate to 0 after decoding them twice with a classical decoder, see [3, 20] for details. We will refer to this verification procedure as VQSS(0).

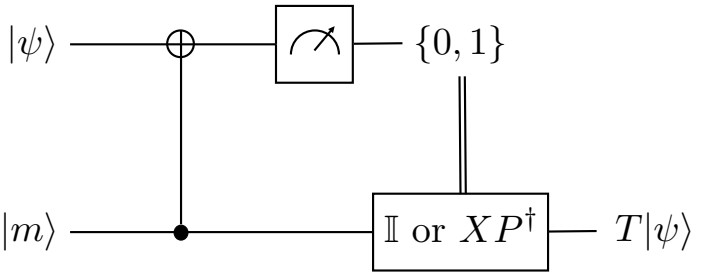


Figure 5.3: Gate teleportation of the T gate. The circuit applies the T gate to an arbitrary single-qubit state ρ. Each state may be logical and each operation may be applied transversally.

DISTRIBUTED GATE TELEPORTATION

To perform universal computation, we need a universal set of gates. However, Clifford gates by themselves are not a universal set. An example of a set that *is* universal, is the set generated by the Clifford gates extended with the $T = \sqrt{P}$ gate [31], denoted Cliff+T[1]. On the other hand, for any error correcting code, it is impossible to perform universal quantum computation using only transversal gates [9]. In particular, for the class of CSS codes under consideration, $\hat{\mathscr{C}}$, the Clifford gates can be applied transversally (see Sec. 5.3.1), but the T gate cannot.

To remedy this problem in the domain of quantum (non-distributed) computing, one can use a technique called gate teleportation [10]. In particular, for the T gate, the idea is to use a specially created ancilla state, measure, and apply a correction depending on the measurement outcome, see Figure 5.3. Importantly, this correction is done with $XP^\dagger$ and since $XP^\dagger$ is a Clifford gate, it can be applied transversally. The cost of this procedure is to create the special ancilla state, which is commonly referred to as a magic state. In the case of the T gate it is $|m\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$.

We generalize this procedure to a distributed setting, see Protocol 2. Our protocol takes two states as an input: logical $\bar{\bar{\Psi}}$ and logical $|\bar{m}\rangle$, both encoded twice (two-level encoding) with code $\hat{\mathscr{C}}$. We assume at this point that both states are verified with respect to the same dealer D. The verification of $\bar{\bar{\Psi}}$ can be performed with VQSS. However, verifying that $|\bar{m}\rangle$ is *exactly* the magic state is non-trivial and we introduce it in the next section.

To apply a logical T gate to $\bar{\bar{\Psi}}$ the nodes first perform a logical transversal CNOT operation on their shares, taking shares of $|\bar{m}\rangle$ as a control and shares of $\bar{\bar{\Psi}}$ as a target. Then each node $i = 1,\ldots,n$ measures the target qubit in the standard basis and announces the measurement outcome. Nodes publicly check whether the measurement collapsed the target state onto a classical string corresponding to a logical $|\bar{\bar{0}}\rangle$ or a logical $|\bar{\bar{1}}\rangle$. To do so, they check whether the resulting string of measurement outcomes $\mathbf{v}_i$ interpolates to 0 or to 1 using the classical decoder twice. At the same time the nodes update the set of errors B. If the interpolated value is 0 then no correction is necessary. If the interpolated value is 1 then the nodes apply the correction $XP^\dagger$ transversally.

[1] One can efficiently approximate any gate G within distance ϵ using polylog$(1/\epsilon)$ gates from set Cliff+T [32].

Protocol 2 (Distributed Gate Teleportation (GTele))**.**
Input: $\bar{\bar{\Psi}}$, $|\bar{\bar{m}}\rangle$ distributed by D to the nodes and verified by the nodes using VQSS (Protocol 1), set of apparent cheaters B from verification of $\bar{\bar{\Psi}}$ and $|\bar{\bar{m}}\rangle$.
Output: Logical T gate applied to the input logical state, $\bar{\bar{T}}(\bar{\bar{\Psi}})$.

1. Each node ℓ, for a share coming from node i:
   (a) applies CNOT with $|\bar{\bar{m}}\rangle_{i_\ell}$ as control qubit and $\bar{\bar{\Psi}}_{i_\ell}$ as target qubit,
   (b) measures the target qubit in the Z basis and broadcasts the result using the secure broadcast channel, see Network model.
2. Broadcasted values yield words $\mathbf{v}_i$. Nodes publicly check on which positions the errors occurred using the classical decoder and update set B with the positions of errors. They decode the classical value a:
   - If $a = 0$, the nodes do not apply any correction.
   - If $a = 1$, the nodes apply $XP^\dagger$ to their shares.

5

VERIFICATION OF CLIFFORD-STABILIZED STATES

One last ingredient we need to perform distributed computation is to verify that the logical magic state $|\bar{\bar{m}}\rangle$ is indeed the logical magic state. This is necessary since we want to be sure that when we apply the T gate in a distributed way, the result will be the T gate on the shares of honest nodes.

Here we present a protocol, Protocol 3, to verify the magic state in a distributed way. In fact, our protocol works for any qubit state $|g\rangle$ stabilized by a single-qubit Clifford gate G. Our idea is inspired by so called stabilizer measurement in quantum error correction, see Figure 5.4. Consider a single-qubit gate $XP^\dagger$ with a $+1$ eigenstate $|m\rangle$. Then it holds that the state $|+\rangle|m\rangle$ is stabilized by controlled $XP^\dagger$ gate, $C\text{-}XP^\dagger$, where $|+\rangle$ is used as a control and $|m\rangle$ is used as a target. That is

$$C\text{-}XP^\dagger(|+\rangle|m\rangle) = |+\rangle|m\rangle\,. \tag{5.7}$$

This gives us an insight into how the verification of $|m\rangle$ should work: if the target state was the magic state then after performing $C\text{-}XP^\dagger$ we will always measure the control in $|+\rangle$ (or equivalently, first apply H and measure 0). Additionally, if the target was not in the magic state and we measure the control in $|+\rangle$, we will project the target onto $|m\rangle$. For this to work, one needs to make sure that the control qubit was in $|+\rangle$ before applying the controlled gate.

We adapt this procedure to run on the logical level in a distributed way as follows. Using VQSS(0), the nodes first verify a logical $|\bar{\bar{0}}\rangle$ encoded and shared by D. They also share $|\bar{\bar{m}}\rangle$ and verify that it is a valid codeword of $\hat{\mathscr{C}}$ using the VQSS, Protocol 1. This step

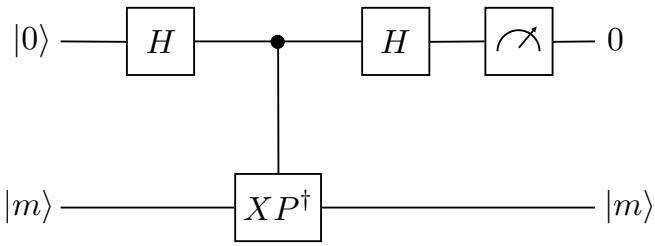


Figure 5.4: Verification of the magic state using stabilizer measurement. The circuit verifies that the target input is the magic state using the fact that the state $|+\rangle|m\rangle$ is stabilized by the controlled $C\text{-}XP^\dagger$ gate.

is necessary since we want the transversal operations which the nodes will perform in next steps to be well defined. Each of the nodes now applies the Hadamard gate to her share of $|\bar{\bar{0}}\rangle$ to turn it into a logical $|\bar{\bar{+}}\rangle$, and after that performs $C\text{-}XP^\dagger$ between her shares of $|\bar{\bar{+}}\rangle$ and $|\bar{m}\rangle$. Then the nodes apply the Hadamard gate to the control qubits one more time and measure in the standard basis. They announce their measurement results and use the classical decoder to get the value a, just like in VQSS(0) and GTele. Note that the protocol works as long as the gate $C\text{-}XP^\dagger$ can be applied transversally with respect to the code used to encode $|\bar{\bar{0}}\rangle$ and $|\bar{m}\rangle$.

Protocol 3 requires an operational workspace of $4n$ qubits per node: first the verification of $|\bar{m}\rangle$ requires a $3n$-qubit workspace per node. After this verification step, each node needs to store n qubits of $|\bar{m}\rangle$ and uses an extra $3n$-qubit workspace to verify $|\bar{\bar{0}}\rangle$. This amounts to a $4n$-qubit workspace per node. The communication complexity is the same as in the sequential VQSS protocol, that is $\mathcal{O}(n^2 s^2)$ qubits per node, where s is the security parameter.

Protocol 3 (Verification of Clifford-Stabilized States (VMagic))**.**
Input: $|0\rangle$ and $|g\rangle$ prepared by D, single-qubit Clifford gate G stabilizing $|g\rangle$, error correcting code $\hat{\mathscr{C}}$, set of apparent cheaters B. Output: verified logical states $|\bar{\bar{0}}\rangle$ and $|\bar{\bar{g}}\rangle$

1. The nodes run VQSS(0) with $|0\rangle$ as an input and VQSS with $|g\rangle$ as an input with dealer D. They update the set B with apparent cheaters B_0 revealed in verifying $|0\rangle$ and apparent cheaters B_g revealed in verifying $|g\rangle$.
2. Each node ℓ, for all shares coming from node i:
   (a) applies H to $|\bar{\bar{0}}\rangle_{i_\ell}$,
   (b) applies $C\text{-}G$ with $|\bar{\bar{0}}\rangle_{i_\ell}$ as the control qubit and $|\bar{\bar{g}}\rangle_{i_\ell}$ as the target qubit,
   (c) applies H to control qubit,
   (d) measures the control qubit in the Z basis and broadcasts the result using the secure broadcast channel, see Network model.

3. Broadcasted values yield words $\mathbf{v}_i$. Nodes publicly check on which positions the errors occurred using the classical decoder and update set B with the positions of errors. They decode the classical value a:
   - If $a = 0$, continue.
   - If $a = 1$, set $B = [n]$ (this will cause the MPQC protocol to abort after the computation phase).

5.3.3. MULTIPARTY QUANTUM COMPUTATION

We are now ready to perform a distributed computation using the ingredients from the previous sections. Recall, the goal of the protocol is to perform a circuit $\mathfrak{R}$ in a distributed way on n single-qubit private inputs $\rho_1, \ldots, \rho_n$, each coming from one node $1, \ldots, n$. Note that the inputs can possibly be entangled. In universal MPQC we compute an arbitrary circuit $\mathfrak{R}$. We choose Clifford gates supplemented with a T gate to be our universal set of gates.

Sharing and verification. During this phase the nodes jointly verify whether dealer D_i is honest, i.e. whether there are less than $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ errors in the first-level encoding performed by D_i. They publicly record the positions on which the errors occurred in the set of apparent cheaters B_i corresponding to dealer D_i. After all of the dealers are verified, they publicly construct a global set of apparent cheaters B, see step 2 of Protocol 4. If $|B| \leq t$ the protocol continues. Note that $|B| \leq t$ implies that each of the honest nodes holds shares with at most t errors on the same positions of the first level of encoding. Otherwise, when $|B| > t$, the honest nodes know they will abort the protocol after the computation and replace their shares with $|0\rangle$. This step is necessary to complete the security proof.

In this phase each node requires a workspace of $n^2 + 2n$ qubits to verify all of the inputs in a sequential way, and sends $(n+1)ns^2$ qubits, where s is the security parameter. The size of the workspace for our MPQC protocol does not depend on s since the verification phase of VQSS is performed in a sequential way.

Computation. In the computation phase, the goal is to compute the circuit $\mathfrak{R}$ on the twice-encoded (see Figure 5.2) and verified inputs. Note that the set of B of apparent cheaters created during the verification is public and cumulative throughout the protocol. That means that it accumulates errors from executions of VMagic, VQSS(0), GTele in the computation phase. If at any point $|B| > t$ during these protocols, the honest nodes proceed in the same way as in the verification phase – they replace their shares with $|0\rangle$. At the end of the computation phase the nodes look at the set B. If $|B| > t$ the protocol aborts. Otherwise, the nodes proceed to the reconstruction phase.

The inputs require a workspace of n^2 qubits per node. For applying the T gate, each node needs a workspace of additional $4n$ qubits, see Protocol 3. Additionally, the verification of every ancilla in $\mathfrak{R}$ requires a workspace of $3n$ qubits per node. This means that each node requires a workspace of at most n^2+4n qubits in total. In this phase, each node sends $\mathcal{O}\big((\#\text{ancillas}+\#T)ns^2\big)$ qubits.

At this point the nodes hold a global state $\bar{\bar{\omega}}$. Let $\bar{\bar{\omega}}_k = \mathrm{tr}_{[n]\setminus i}(\bar{\bar{\omega}})$ be the outcome of each node i.

Reconstruction. After the computation phase the cheating nodes can still introduce errors to the shares they hold before sending them back to corresponding dealers. Therefore, each of the dealers, after receiving her original shares back, runs an error correcting circuit for the code $\hat{\mathscr{C}}$ and identifies further errors. If there is no more than t errors, she reconstructs her output state ω_i. In this phase, the nodes just exchange the existing qubits, therefore the operational workspace does not increase from n^2+4n. Each node sends n^2 qubits.

Altogether, each node requires an operational workspace of n^2+4n qubits, and sends $\mathcal{O}\big((n+\#\text{ancillas}+\#T)ns^2\big)$ qubits throughout the execution of the MPQC protocol, Protocol 4.

Protocol 4 (Multiparty quantum computation (MPQC))**.**
Input: private input ρ_i for every node i, circuit $\mathfrak{R}$, error correcting code $\hat{\mathscr{C}}$.

Sharing and Verification

1. Each node $i = 1,\ldots,n$ runs sequential verifiable quantum secret sharing (VQSS, Protocol 1) with single-qubit input ρ_i and code $\hat{\mathscr{C}}$, acting as dealer D_i. This way nodes create logical $\bar{\bar{\Psi}}_i$ encoded twice with $\hat{\mathscr{C}}$, see Figure 5.2.

2. The nodes publicly create sets $B_{i,\ell}$ containing all second-level errors from all n executions of sequential VQSS (see [3, 19] for details). If for each node ℓ, if $|B_{i,\ell}| > t$ then they add node ℓ to a set of apparent cheaters B_i for dealer D_i. After all n executions of VQSS, they create a global set of apparent cheaters $B = \bigcup_i B_i$. If $|B| > t$ the nodes know they will abort after the computation. They replace all the shares they hold with $|0\rangle$.

Computation

3. For every Clifford gate C of the circuit $\mathfrak{R}$ the nodes apply C transversally to their local qubits. For every T gate in $\mathfrak{R}$ applied to the input of D_i:
   (a) D_i creates $|0\rangle$ and $|m\rangle$. The nodes run Verification of Clifford-Stabilized States (VMagic, Protocol 3). The nodes update the set B with apparent cheaters from execution of VMagic. If $|B| > t$ the nodes replace all the shares they hold with $|0\rangle$.

(b) The nodes apply Distributed Gate Teleportation (GTele, Protocol 2) to their shares of $\bar{\bar{\Psi}}_i$ and verified $|\bar{\bar{m}}\rangle$. The nodes update the set B with apparent cheaters from execution of GTele. If $|B| > t$ the nodes replace all the shares they hold with $|0\rangle$ and do not apply a correction in GTele (treating the measurement outcome as 0).

4. For every $|0\rangle$ ancilla necessary to perform the circuit $\mathfrak{R}$, a node $i \notin B$ chosen at random using the public source of randomness, runs VQSS(0) acting as a dealer. They update B with the set of apparent cheaters from the execution of VQSS(0). The nodes use the verified $|\bar{0}\rangle$ to perform $\mathfrak{R}$. If $|B| > t$ the nodes replace all the shares they hold with $|0\rangle$.

5. If $|B| > t$ the protocol aborts. Otherwise continue.

Let the logical global outcome of the computation be $\bar{\bar{\omega}}$, with $\bar{\bar{\omega}}_i = \mathrm{tr}_{[n]\setminus i}(\bar{\bar{\omega}})$ corresponding to the outcome of each node i.

Reconstruction

6. Each node sends all of the shares of $\bar{\bar{\omega}}_i$ to D_i.

7. Each D_i:
   (a) For each share coming from node $j \notin B$, D_i runs an error correcting circuit for the code $\hat{\mathscr{C}}$. She creates a set of errors $\tilde{B}_{i,j}$ such that it contains $B_{i,j}$, i.e. $B_{i,j} \subseteq \tilde{B}_{i,j}$. If $|\tilde{B}_{i,i}| \leq t$ then errors are correctable, D_i corrects them and decodes the i-th share obtaining $\bar{\omega}_i$. Otherwise, D_i adds j to the global set B.
   (b) For all $j \notin B$, D_i randomly chooses $n-2t$ shares of $\bar{\omega}_i$ and applies an erasure-recovery circuit to them. She obtains ω_i.

5.3.4. SECURITY STATEMENTS

In this section we prove the security of our MPQC protocol. To do so, we first state the security framework and definition following the work of [33–36]. We employ the simulator-based security definition, see Definition 17 below. It implies that the three properties – correctness, soundness and privacy defined at the beginning of this chapter – are automatically satisfied. Our security definition uses two models of the protocol – "real" and "ideal". The real model corresponds to the execution of the actual MPQC protocol. In the ideal model the nodes interact with an oracle that perfectly realizes the MPQC task and is incorruptible. The general idea is that the protocol is secure if one cannot distinguish a real execution of MPQC from the ideal one.

In the ideal model the honest nodes can only interact with the oracle. What is more, they do so in a so called "dummy" way, i.e. they simply forward their input to the oracle,

and output whatever they receive from the oracle. The cheating nodes can collude and perform any joint operation on their inputs before sending it to the oracle. Similarly, they can perform any joint operation on whatever they receive from the oracle before they output their state. Recall that we do not make any assumption on the computational power of the cheaters. For the purpose of the proof we will say that the cheaters can be corrupted by an adversary $\mathscr{A}$ which can corrupt at most t nodes, but otherwise is arbitrarily powerful. Moreover, by $\mathscr{A}_{\text{real}}$ we will denote the adversary in the "real" protocol and by $\mathscr{A}_{\text{ideal}}$ the adversary in the "ideal" protocol.

Definition 17 (ϵ-security)**.** We say that a MPQC protocol Π is ϵ-secure if for any input state ρ, and any real adversary $\mathscr{A}_{\text{real}}$, there exists an ideal adversary $\mathscr{A}_{\text{ideal}}$, such that the output state $\omega_{\text{real}} := \Pi_{\text{real}}(\rho)$ of the real protocol is ϵ-close to the output state $\omega_{\text{ideal}} := \Pi_{\text{ideal}}(\rho)$ of the ideal protocol, that is

$$\frac{1}{2} \parallel \omega_{\text{real}} - \omega_{\text{ideal}} \parallel_1 \leq \epsilon. \tag{5.8}$$

To prove the security of the MPQC protocol, Protocol 4 we first restate the soundness of the VQSS protocol [3, 19, 20].

Lemma 12 (Soundness of VQSS)**.** *In the verifiable quantum secret sharing protocol, Protocol 1, either the honest parties hold a consistently encoded secret or the dealer is caught with probability at least* $1 - 2^{-\Omega(s)}$.

Theorem 14. *The multiparty Quantum Computation protocol, Protocol 4, is* $\kappa 2^{-\Omega(s)}$*-secure, where* $\kappa = n + \#T$ *gates* $+ \#$ *ancillas in* $\Re$.

Idea of the proof. Our proof is inspired by the approach taken in [3, 20], on which we expand and explicitly show that the outputs of the real and ideal protocol are ϵ-close, see Section 5.5. We construct an ideal protocol using a common simulation technique, where $\mathscr{A}_{\text{ideal}}$ locally simulates the MPQC protocol, Protocol 4, with honest nodes interacting with the cheaters. This means that for any real adversary $\mathscr{A}_{\text{real}}$ we construct an ideal adversary $\mathscr{A}_{\text{ideal}}$ by saying that it internally simulates the execution of real protocol with the real adversary $\mathscr{A}_{\text{real}}$. Then we formally write the execution of the real protocol. We show that the outputs of both protocols are equal in the case when the encoding in the sharing phase of Protocol 4 is done correctly. We also prove that the ϵ error in the security comes from the fact that the verification of inputs and any ancillas needed for MPQC can fail with probability defined by Lemma 12. □

We remark that our security definition follows the paradigm of sequential composability, formalized by the real-vs-ideal security definition, Definition 17. The extendibility of our security definition to the more general framework of universal composability [35, 36] is left as an open problem.

5.4. DISCUSSION

In our protocol we allow an abort when there are too many errors introduced by the cheaters, see Protocol 4. However, this condition can be removed following the approach outlined in [3, 20] (there called Top-Level Sharing), at the cost of more rounds of quantum communication. Given our objective is to save resources, we did not pursue this

path in this work. However, we can introduce a step before computation, in which the nodes perform a distributed encoding (creating the third level of encoding) of the verified inputs. It works as follows. The nodes run the VQSS verification procedure for every input state ρ_i, but do not create a global set of cheaters. Instead, they create a set B_i recording first-level errors on input state ρ_i. To perform the distributed encoding of input ρ_i the nodes use ancilla states prepared and encoded by the corresponding dealer D_i. The nodes also verify the ancillas using VQSS and add the errors that occurred on the first level of encoding of ancillas to B_i. If $|B_i| \leq t$, the nodes perform the distributed encoding with the verified ancillas. The encoding can be done transversally, since for any stabilizer error correcting code the encoding procedure is a Clifford operation [37].

If a dealer is caught cheating, $|B_i| > t$, the protocol does not abort. Instead, a node which has not been caught cheating yet prepares an encoding of $|0\rangle$ and the nodes proceed to verify it in the same way as before. Note that there will be at most t failed tries in preparing a valid encoding of $|0\rangle$ since there are at most t cheaters. Otherwise, upon a successful verification of the encoded $|0\rangle$, the nodes proceed to the distributed encoding. This step replaces the invalid input from the cheater with a valid encoding of $|0\rangle$. The same "try until you succeed" procedure can be adapted to verify magic states and $|0\rangle$ ancillas needed to perform the circuit $\mathfrak{R}$. The nodes simply try until the verification of an ancilla has at most t errors.

Performing the distributed encoding of the inputs creates a three-level encoding before the computation phase. The shares initially dealt by dealer D_i are then sent back to D_i, who reconstructs them and corrects the errors using the reconstruction step from VQSS (as in reconstruction of MPQC, Protocol 4). As a result, each node holds a single qubit corresponding to a correctly encoded input state ρ_i, with at most t errors confined to the cheaters' positions. The protocol proceeds with the distributed computation, but now the circuit is performed on a single level of encoding. Since the errors are only on the shares held by the cheaters, the errors will not propagate to the honest shares during the computation. Therefore, after the computation it will be possible to reconstruct outputs for the honest nodes.

Finally, we remark that the distributed encoding can be performed in a sequential way, similar to the execution of VQSS we present in Protocol 1. In fact, this does not increase the qubit workspace per node, each node will not exceed the workspace of n^2+4n. However, this approach has significantly higher quantum communication complexity. Specifically, in this version of the protocol, each node needs to send $\mathcal{O}(n^5 s^2)$ qubits.

5.5. TECHNICAL STATEMENTS

Here we provide the security proof of our protocol based on the simulator definition, see Definition 17. We first construct the ideal protocol step by step and model each operation performed in this protocol by general maps, and finally express the output of this protocol ω_{ideal} in terms of these maps. Then, we analyze the real protocol and similarly express its output ω_{real} in terms of the maps modeling the real protocol. Finally, we compare the two outputs, ω_{ideal} and ω_{real}, and show they are exponentially close in the security parameter s.

To prove security of the MPQC protocol, Theorem 14, we first state the following useful lemma. Intuitively, it says that sharing and verifying the input, performing the dis-

tributed circuit and decoding is equivalent to applying the circuit to the inputs directly. Note that we consider the decoding to be "hypothetical" – after the computation phase in MPQC the nodes send all of the shares coming from input of node i to node i, and node i reconstructs it.

Lemma 13. *Let B be a set of apparent cheaters at the end of the computation phase, such that $|B| \leq t$, and A be a set of cheaters. Let $\mathscr{D}$ denote the decoding procedure for code $\hat{\mathscr{C}}$ and $\hat{\mathscr{D}}$ denote the erasure recovery circuit for code $\hat{\mathscr{C}}$. If the state $\bar{\bar{\rho}}$ encoded twice with the code $\hat{\mathscr{C}}$ is decodable, i.e.*

$$\rho = \bigotimes_{i\in[n]} \left(\hat{\mathscr{D}}_{\overline{B\cup A}} \circ \bigotimes_{\ell \in \overline{B\cup A}} \mathscr{D}_\ell \right) (\bar{\bar{\rho}}), \tag{5.9}$$

then applying a logical gate $\bar{\bar{G}}$ ($G \in \text{Cliff} + T$) on $\bar{\bar{\rho}}$ is also decodable, i.e.

$$G(\rho) = \bigotimes_{i\in[n]} \left(\hat{\mathscr{D}}_{\overline{B\cup A}} \circ \bigotimes_{\ell \in \overline{B\cup A}} \mathscr{D}_\ell \right) \left(\bar{\bar{G}}(\bar{\bar{\rho}}) \right), \tag{5.10}$$

where $\bar{\bar{G}}$ is gate G applied transversally on the CSS code $\hat{\mathscr{C}}$ if $G \in$ Cliff, or it is the implementation of the T gate described in Protocol 2 if $G = T$. The same property holds when replacing G by the projective measurement in the Z basis denoted P, and where $\bar{\bar{P}}$ corresponds to measuring each qubit of the double-encoded state in the Z basis followed by broadcasting the outcome classically.

Proof. The lemma follows from the fact that to realize a logical gate $\bar{\bar{G}}$ it is sufficient to apply G honestly on shares in $\overline{B\cup A}$. Indeed, applying a Clifford gate transversally on shares in $\overline{B\cup A}$ realizes a logical Clifford gate [29]. For a CSS code $\hat{\mathscr{C}}$ measuring each qubit in the Z basis and broadcasting the measurement result realizes the logical transversal measurement. Additionally, we implement the T gate by composing an ancilla state, Z measurement and a Clifford operation. Therefore, the transversal properties of Cliffords and Z measurement can be transferred to this implementation of the T gate. □

Property 1. Let $\mathfrak{R}$ be a circuit implementing a completely positive trace preserving (CPTP) map. Lemma 13 holds when replacing G by any circuit $\mathfrak{R}$,

$$\mathfrak{R}(\rho) = \bigotimes_{i\in[n]} \left(\hat{\mathscr{D}}_{\overline{B\cup \bar{H}}} \circ \bigotimes_{\ell \in \overline{B\cup \bar{H}}} \mathscr{D}_\ell \right) \left(\bar{\bar{\mathfrak{R}}}(\bar{\bar{\rho}}) \right). \tag{5.11}$$

This follows from the fact that any circuit $\mathfrak{R}$ can be represented as $\mathfrak{R} = P \circ \mathscr{U}$, where $\mathscr{U}$ can be decomposed into gates from the set Cliff+T and P is a measurement.

Now we prove the security of our MPQC protocol, Theorem 14.

Proof of Theorem 14. This proof is inspired by the approach taken in [3, 20]. In the following we construct a proof aiming to show that the outputs of the real and ideal protocol are ϵ-close. We first construct an ideal protocol using a simulator approach and

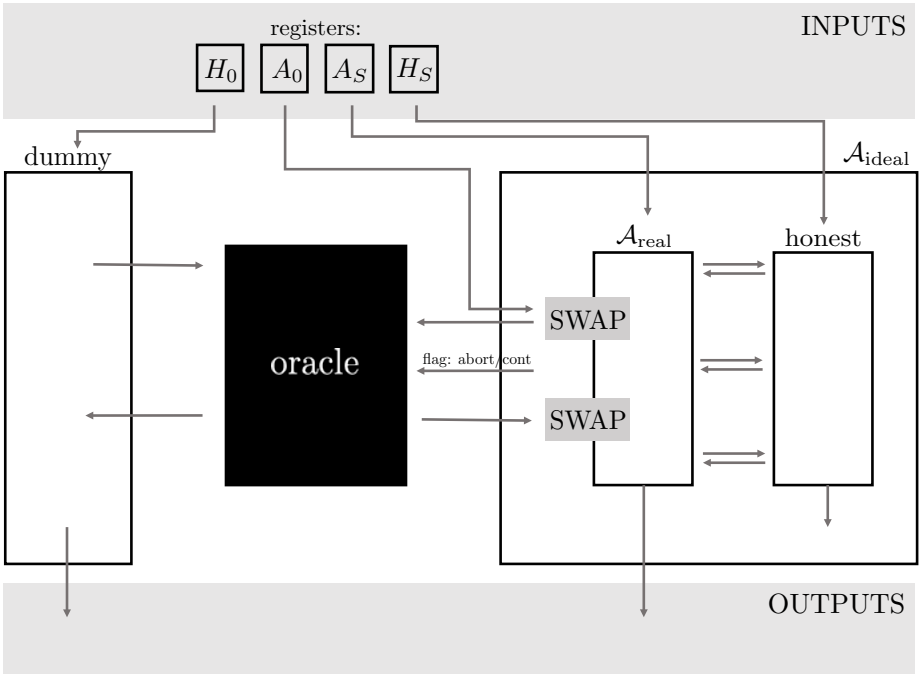


Figure 5.5: Schematic of our simulator-based security proof of the MPQC protocol, Protocol 4.

formally state every step of the simulation. Then we formally write the execution of the real protocol.

Box 1. Registers used in the security proof.

Ideal protocol:
H_S – registers of "dummy" inputs of the honest nodes in the simulation
A_S – registers of the cheaters' inputs
H_0 – registers of the simulated honest nodes
A_0 – registers of the simulated cheaters.

Real protocol:
H_R – registers of honest nodes
A_R – registers of cheaters.

Ideal protocol. $\mathcal{A}_{\text{ideal}}$ will locally simulate the MPQC protocol, Protocol 4, with honest nodes interacting with the cheaters. The cheaters are controlled by $\mathcal{A}_{\text{real}}$ and $\mathcal{A}_{\text{real}}$ is simulated within $\mathcal{A}_{\text{ideal}}$, see Figure 5.5. In the ideal model $\mathcal{A}_{\text{ideal}}$ and the honest nodes

interact with an oracle that perfectly realizes the MPQC task and is incorruptible. The oracle requires two types of inputs: first the input registers H_S, A_0 on which the computation of the circuit will occur, second a flag input that indicates whether the oracle should abort or continue. If the flag input is "abort" the oracle outputs $|\perp\rangle\langle\perp|$. If the the flag input is "continue" the oracle outputs the evaluation of circuit $\mathfrak{R}$ on the inputs $H_S A_0$. At any moment of this simulated execution, the ideal adversary has access to all the simulated registers, in particular, the set B of apparent cheaters. Let the input to the simulation be

$$\rho_{H_S A_S} \otimes |0\rangle\langle 0|_{H_0 A_0}, \tag{5.12}$$

where $\rho_{H_S A_S}$ denotes the input state of all nodes, such that $\mathrm{tr}_{[n]\setminus i}\left(\rho_{H_S A_S}\right) = \rho_i$.

1. $\mathscr{A}_{\text{ideal}}$ locally simulates sharing and verification with simulated honest nodes using $|0\rangle$ as their input. The input registers $H_0 A_S$ given to $\mathscr{A}_{\text{ideal}}$ is forwarded to the simulated $\mathscr{A}_{\text{real}}$, i.e.

$$\sigma^{(1)}_{H_0 A_0 H_S A_S} = \mathscr{SV}_{H_0 A_S}\left(\rho_{H_S A_S} \otimes |0\rangle\langle 0|_{H_0 A_0}\right), \tag{5.13}$$

where $\mathscr{SV}_{H_0 A_S}$ denotes the sharing and verification (see Protocol 4) performed on registers H_0 and A_S. We assume that the identity operation is applied on all the registers that are not in the map $\mathscr{SV}$, i.e. $\mathbb{1}_{H_S A_0}$.

2. Before $\mathscr{A}_{\text{ideal}}$ proceeds with the simulation of the computation phase, for each input of the cheaters $\mathscr{A}_{\text{ideal}}$, creates an encoding of $|0\rangle$ in register A_0. Then $\mathscr{A}_{\text{ideal}}$ performs a swap gate between A_0 and cheaters' input A_S.

- In the case when the set $|B| \leq t$, there are sufficiently few errors on both levels of encoding. Then $\mathscr{A}_{\text{ideal}}$ can apply an erasure-recovery circuit twice (for the double encoding), denoted $\tilde{\mathscr{D}}_{A_0}$, to the input of nodes not in B and pass it to the oracle. Applying decoding $\tilde{\mathscr{D}}_{A_0}$ is necessary, since the oracle accepts only single-qubit inputs.
- Otherwise, when $|B| > t$, $\mathscr{A}_{\text{ideal}}$ simply passes previously prepared $|0\rangle$ states as inputs of the cheaters to the oracle and the simulated honest nodes H_S replace their shares with $|0\rangle$. The simulated cheaters apply an arbitrary map $\mathscr{M}_{A_S}$ to their shares.

We therefore describe this step as

$$\sigma^{(2)}_{H_0 A_0 H_S A_S} = \begin{cases} \tilde{\mathscr{D}}_{A_0} \circ \mathrm{Swap}_{A_0 A_S} \circ \mathscr{E}_{A_0}(\sigma^{(1)}_{H_0 A_0 H_S A_S}) & \text{if } |B| \leq t \\ \mathscr{M}_{A_S} \otimes \mathrm{tr}_{H_0}[\sigma^{(1)}_{H_0 A_0 H_S A_S}] \otimes |0\rangle\langle 0|_{H_0} & \text{if } |B| > t. \end{cases} \tag{5.14}$$

3. $\mathscr{A}_{\text{ideal}}$ proceeds with the simulation of the computation phase on registers H_0 and A_S. At the same time, the oracle computes the ideal circuit $\mathfrak{R}^{\text{ideal}}_{H_S A_0}$ on the simulated honest shares H_S and register A_0 of the cheaters. The state after this step is therefore,

$$\sigma^{(3)}_{H_0 A_0 H_S A_S} = \begin{cases} (\mathfrak{R}^{\text{ideal}}_{H_S A_0} \otimes \bar{\tilde{\mathfrak{R}}}_{H_0 A_S})(\sigma^{(2)}_{H_0 A_0 H_S A_S}) & \text{if } |B| \leq t \\ (\mathfrak{R}^{\text{ideal}}_{H_S A_0} \otimes \bar{\tilde{\mathfrak{R}}}_{H_0 A_S})(\sigma^{(2)}_{H_0 A_0 H_S A_S}) & \text{if } |B| > t. \end{cases} \tag{5.15}$$

4. If $|B| > t$, $\mathscr{A}_{\text{ideal}}$ sends the flag "abort" to the oracle, and "continue" otherwise.

- If the oracle receives "abort" it outputs a flag $|\perp\rangle\langle\perp|$ to all nodes.
- Otherwise, it outputs the computation of the ideal circuit on the inputs.

5. The nodes in H_S output whatever they received from the oracle. Upon receiving the oracle's output, $\mathscr{A}_{\text{ideal}}$ does the following:

- if "abort" was sent in the previous step, then it must be that $|B| > t$. The simulated protocol aborts. Therefore, $\mathscr{A}_{\text{ideal}}$ outputs the output of the $\mathscr{A}_{\text{real}}$. Note that the simulated cheaters could have applied an arbitrary map $\mathscr{M}'_{A_S}$ on their register.
- if "continue" sent in the previous step, then $\mathscr{A}_{\text{ideal}}$ applies double encoding $\mathscr{E}_{A_0}$ to all shares of the cheating nodes A_0. Then $\mathscr{A}_{\text{ideal}}$ applies the swap gate between the simulated registers of cheaters A_S and A_0, and proceeds to the next step.

$$\begin{cases} \text{Swap}_{A_0A_S} \circ \mathscr{E}_{A_0} \circ (\mathfrak{R}^{\text{ideal}}_{H_SA_0} \otimes \bar{\bar{\mathfrak{R}}}_{H_0A_S})(\sigma^{(2)}_{H_0A_0H_SA_S}) \otimes |\text{cont}\rangle\langle\text{cont}| & \text{if } |B| \leq t \\ |\perp\rangle\langle\perp|_{H_SA_0} \otimes \text{tr}_{H_SA_0}\left[\mathscr{M}'_{A_S}(\sigma^{(3)}_{H_0A_0H_SA_S})\right] \otimes |\text{abort}\rangle\langle\text{abort}| & \text{if } |B| > t. \end{cases} \tag{5.16}$$

Let us denote by $\sigma^{(5)}_{H_0A_0H_SA_S}$ the following and use the explicit form of $\sigma^{(2)}_{H_0A_0H_SA_S}$ for $|B| \leq t$, Equation (5.15),

$$\sigma^{(5)}_{H_0A_0H_SA_S} = \text{Swap}_{A_0A_S} \circ \mathscr{E}_{A_0} \circ (\mathfrak{R}^{\text{ideal}}_{H_SA_0} \otimes \bar{\bar{\mathfrak{R}}}_{H_0A_S}) \circ \tilde{\mathscr{D}}_{A_0} \circ \text{Swap}_{A_0A_S} \circ \mathscr{E}_{A_0}(\sigma^{(1)}_{H_0A_0H_SA_S}). \tag{5.17}$$

We will now simplify the above expression. For this we first state the following useful property.

Property 2. For any operation $\mathscr{O}_{ABCD}$ on registers $ABCD$, the following identity holds,

$$\text{Swap}_{BC} \circ \mathscr{O}_{ABCD} \circ \text{Swap}_{BC} = \mathscr{O}_{ACBD}. \tag{5.18}$$

Using this property for $\sigma^{(5)}_{H_0A_0H_SA_S}$ we get that

$$\text{Swap}_{A_0A_S} \circ \mathscr{E}_{A_0} \circ (\mathfrak{R}^{\text{ideal}}_{H_SA_0} \otimes \bar{\bar{\mathfrak{R}}}_{H_0A_S}) \circ \tilde{\mathscr{D}}_{A_0} \circ \text{Swap}_{A_0A_S} \circ \mathscr{E}_{A_0} = \mathscr{E}_{A_S} \circ \mathfrak{R}^{\text{ideal}}_{H_SA_S} \circ \tilde{\mathscr{D}}_{A_S} \otimes \bar{\bar{\mathfrak{R}}}_{H_0A_0} \circ \mathscr{E}_{A_0}. \tag{5.19}$$

This means that that the composition of the swaps with the ideal circuit performed by the oracle is equivalent to applying the ideal circuit to registers H_SA_S by the oracle. Therefore, we can simplify $\sigma^{(5)}_{H_0A_0H_SA_S}$ to

$$\sigma^{(5)}_{H_0A_0H_SA_S} = (\mathscr{E}_{A_S} \circ \mathfrak{R}^{\text{ideal}}_{H_SA_S} \circ \tilde{\mathscr{D}}_{A_S}) \otimes (\bar{\bar{\mathfrak{R}}}_{H_0A_0} \circ \mathscr{E}_{A_0})(\sigma^{(1)}_{H_0A_0H_SA_S}).\,, \tag{5.20}$$

and using Equation (5.13) we obtain,

$$\sigma^{(5)}_{H_0A_0H_SA_S} = (\mathscr{E}_{A_S} \circ \mathfrak{R}^{\text{ideal}}_{H_SA_S} \circ \tilde{\mathscr{D}}_{A_S}) \otimes (\bar{\bar{\mathfrak{R}}}_{H_0A_0} \circ \mathscr{E}_{A_0} \circ \mathscr{TV}_{H_0A_S})\left(\rho_{H_SA_S} \otimes |0\rangle\langle 0|_{H_0A_0}\right) \tag{5.21}$$

$$= \left(\mathscr{E}_{A_S} \circ \mathfrak{R}^{\text{ideal}}_{H_SA_S} \circ \tilde{\mathscr{D}}_{A_S} \circ \mathscr{TV}_{A_S}\left(\rho_{H_SA_S}\right)\right) \otimes \left(\bar{\bar{\mathfrak{R}}}_{H_0A_0} \circ \mathscr{E}_{A_0} \circ \mathscr{TV}_{H_0}\left(|0\rangle\langle 0|_{H_0A_0}\right)\right). \tag{5.22}$$

6. If the protocol did not abort, $\mathscr{A}_{\text{ideal}}$ proceeds to the reconstruction phase, in which the simulated honest nodes H_0 first use the decoding procedure for code $\hat{\mathscr{C}}$ and then apply an erasure recovery circuit, as in the reconstruction phase of Protocol 4. We denote this procedure by $\tilde{\mathscr{D}}_{H_0}$. On the other hand, the simulated cheaters A_S apply an arbitrary map $\mathscr{W}_{A_S}$. $\mathscr{A}_{\text{ideal}}$ outputs whatever is the output of the simulated $\mathscr{A}_{\text{real}}$. Therefore, the output of the ideal protocol is

$$\omega_{\text{ideal}} = \text{tr}_{H_0 A_0}\left[\tilde{\mathscr{D}}_{H_0} \otimes \mathscr{W}_{A_S}(\sigma^{(5)}_{H_0 A_0 H_S A_S})\right]. \tag{5.23}$$

Using Equation (5.22) and the fact that the sharing and verification followed double decoding, $\tilde{\mathscr{D}}_{A_S} \circ \mathscr{SV}_{A_S}$, is equivalent to $\mathbb{1}_{A_S}$, we obtain,

$$\omega_{\text{ideal}} = \mathscr{W}_{A_S} \circ \mathscr{E}_{A_S} \circ \mathfrak{R}^{\text{ideal}}_{H_S A_S}\left(\rho_{H_S A_S}\right). \tag{5.24}$$

Similarly, to later compare with the real protocol, we write the identity map on H_S as $\mathbb{1}_{A_S} = \tilde{\mathscr{D}}_{H_S} \circ \mathscr{E}_{H_S}$, and get

$$\omega_{\text{ideal}} = (\tilde{\mathscr{D}}_{H_S} \otimes \mathscr{W}_{A_S}) \circ \mathscr{E}_{H_S A_S} \circ \mathfrak{R}^{\text{ideal}}_{H_S A_S}\left(\rho_{H_S A_S}\right). \tag{5.25}$$

Real protocol. In the real protocol whenever the honest nodes observe $|B| > t$ they replace all of their shares with $|0\rangle$. This is necessary because in the ideal protocol the oracle receives "abort" at the end of the computation phase. Therefore, in the real protocol we also abort at the end of the computation phase. However, it could happen that in the case when $|B| > t$ continuing the computation leaks some information about the honest nodes' inputs. To avoid this situation, we make the honest nodes substitute their shares with $|0\rangle$.

1. The protocol starts with the sharing and verification phase, which we describe by the map $\mathscr{SV}$ acting on inputs of all the nodes $\rho_{H_R A_R}$. The state after this step is

$$\mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right). \tag{5.26}$$

2. The protocol continues;

- In the case when $|B| \leq t$, the nodes apply the distributed circuit $\bar{\bar{\mathfrak{R}}}_{H_R A_R}$.
- In the case when $|B| > t$, the honest nodes replace their shares with $|0\rangle$ and the cheaters apply an arbitrary map $\mathscr{M}_{A_R}$.

At the end of the computation phase the state is therefore,

$$\sigma^{(2)}_{H_R A_R} = \begin{cases} \bar{\bar{\mathfrak{R}}}_{H_R A_R} \circ \mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right) & \text{if } |B| \leq t, \\ \mathscr{M}_{A_R}(\text{tr}_{H_R}[\mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right)]) \otimes |0\rangle\langle 0|_{H_R} & \text{if } |B| > t. \end{cases} \tag{5.27}$$

3. The nodes check the size of set B.

- If $|B| \leq t$ then the protocol continues to the reconstruction phase, where the honest nodes apply first a decoding operator for code $\hat{\mathscr{C}}$ and then an interpolation circuit, denoted $\mathscr{D}_{H_R}$. At the same time, the cheaters can apply an arbitrary map on their registers, which we denote $\mathscr{W}_{A_R}$.
- In the case when $|B| > t$, the nodes output the abort flag $|\perp\rangle\langle\perp|$ and the cheaters output their part of $\sigma^{(2)}_{H_R A_R}$, possibly with an arbitrary map $\mathscr{M}'_{A_R}$. The protocol aborts.

We can describe this step as,

$$\begin{cases} (\mathscr{D}_{H_R} \otimes \mathscr{W}_{A_R}) \circ \bar{\tilde{\mathfrak{R}}}_{H_R A_R} \circ \mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right) \otimes |\text{cont}\rangle\langle\text{cont}| & \text{if } |B| \leq t, \\ |\perp\rangle\langle\perp|_{H_R} \otimes \mathscr{M}'_{A_R}(\text{tr}_{H_R}[\sigma^{(2)}_{H_R A_R}]) \otimes |\text{abort}\rangle\langle\text{abort}| & \text{if } |B| > t. \end{cases} \tag{5.28}$$

We introduce the identity map as encoding followed by double encoding on both registers, i.e. $\mathbb{1}_{H_R A_R} = \tilde{\mathscr{D}}_{H_R A_R} \circ \mathscr{E}_{H_R A_R}$. Then, plugging this $\mathbb{1}_{H_R A_R}$ between $\bar{\tilde{\mathfrak{R}}}_{H_R A_R}$ and $(\mathscr{D}_{H_R} \otimes \mathscr{W}_{A_R})$, the first case can be rewritten as,

$$\omega_{\text{real}} = (\mathscr{D}_{H_R} \otimes \mathscr{W}_{A_R}) \circ \mathscr{E}_{H_R A_R} \circ \tilde{\mathscr{D}}_{H_R A_R} \circ \bar{\tilde{\mathfrak{R}}}_{H_R A_R} \circ \mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right), \tag{5.29}$$

which defines the output of the real protocol when it does not abort.

Now we aim to simplify ω_{real} to compare it to the output of the ideal protocol. Our goal is to show that sharing and verifying the input, performing the distributed circuit and decoding is equivalent to applying the circuit to the inputs directly,

$$\tilde{\mathscr{D}}_{H_R A_R} \circ \bar{\tilde{\mathfrak{R}}}_{H_R A_R} \circ \mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right) = \mathfrak{R}_{H_R A_R}(\rho_{H_R A_R}). \tag{5.30}$$

Indeed, this follows from Lemma 13 and Property 1. By security of the VQSS [3, 19, 20], if the protocol does not abort, there exists a unique double-encoded state after the verification phase, i.e. $\mathscr{SV}_{H_R A_R}\left(\rho_{H_R A_R}\right)$. By definition the decoding $\tilde{\mathscr{D}}_{H_R A_R}$ is exactly the one performed in Lemma 13. Therefore, we have that

$$\begin{aligned} \omega_{\text{real}} &= (\mathscr{D}_{H_R} \otimes \mathscr{W}_{A_R}) \circ \mathscr{E}_{H_R A_R} \circ \tilde{\mathscr{D}}_{H_R A_R} \circ \bar{\tilde{\mathfrak{R}}}_{H_R A_R} \circ \mathscr{E}_{H_R A_R}\left(\rho_{H_R A_R}\right) && (5.31) \\ &= (\mathscr{D}_{H_R} \otimes \mathscr{W}_{A_R}) \circ \mathscr{E}_{H_R A_R} \circ \mathfrak{R}_{H_R A_R}\left(\rho_{H_R A_R}\right). && (5.32) \end{aligned}$$

This, together with Equation (5.25), gives us that the outputs of the ideal and real protocol are equal for $|B| \leq t$,

$$\omega_{\text{ideal}} = \omega_{\text{real}}. \tag{5.33}$$

Similarly, when $|B| > t$, one can compare (5.15) with (5.16) and obtain that the states are the same for the real and ideal protocol. What we described so far, considers that the encoding in the sharing phase was performed correctly in the real protocol. However, this does not have to be the case. Every verification performed during the MPQC has a probability of error inherited from the VQSS. Recall that from Lemma 12 the probability of unsuccessful verification in VQSS is lower-bounded by $2^{-\Omega(s)}$. In MPQC we verify:

- each of the n inputs,
- each $|\bar{\bar{0}}\rangle$ and $|\bar{\bar{m}}\rangle$ necessary to perform the T gate,
- each $|\bar{\bar{0}}\rangle$ necessary for the circuit $\mathfrak{R}$

Let $\kappa = n + \#T$ gates +#ancillas for $\mathfrak{R}$. Then the total probability of error in MPQC is $\kappa 2^{-\Omega(s)}$.

□

REFERENCES

[1] A. C. Yao, *Protocols for secure computations,* in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82 (IEEE Computer Society, USA, 1982) p. 160–164.

[2] R. Cramer, I. B. Damgrd, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*, 1st ed. (Cambridge University Press, USA, 2015).

[3] C. Crépeau, D. Gottesman, and A. Smith, *Secure multi-party quantum computation,* in *Proceedings of the Thirty-fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (ACM, New York, NY, USA, 2002) pp. 643–652.

[4] C. Crépeau, D. Gottesman, and A. Smith, *Approximate quantum error-correcting codes and secret sharing schemes,* in *Advances in Cryptology – EUROCRYPT 2005*, edited by R. Cramer (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 285–301.

[5] F. Dupuis, J. B. Nielsen, and L. Salvail, *Actively secure two-party evaluation of any quantum operation,* in *Proceedings of the 32nd Annual Cryptology Conference on Advances in Cryptology — CRYPTO 2012 - Volume 7417* (Springer-Verlag, Berlin, Heidelberg, 2012) p. 794–811.

[6] Y. Dulek, A. B. Grilo, S. Jeffery, C. Majenz, and C. Schaffner, *Secure multi-party quantum computation with a dishonest majority,* (2019), arXiv:quant-ph/1909.13770 .

[7] D. Mayers, *Unconditionally secure quantum bit commitment is impossible,* Physical review letters **78**, 3414 (1997).

[8] H.-K. Lo and H. F. Chau, *Why quantum bit commitment and ideal quantum coin tossing are impossible,* Physica D: Nonlinear Phenomena **120**, 177 (1998).

[9] B. Eastin and E. Knill, *Restrictions on transversal encoded quantum gate sets,* Phys. Rev. Lett. **102**, 110502 (2009).

[10] D. Gottesman and I. L. Chuang, *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations,* Nature **402**, 390 (1999).

[11] D. Aharonov and M. Ben-Or, *Fault-tolerant quantum computation with constant error,* in *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97 (ACM, New York, NY, USA, 1997) pp. 176–188.

[12] E. M. Rains, *Nonbinary quantum codes,* (1997).

[13] M. Grassl, T. Beth, and M. Rotteler, *On optimal quantum codes,* International Journal of Quantum Information **02**, 55 (2004).

[14] S. Bravyi, G. Smith, and J. A. Smolin, *Trading classical and quantum computational resources,* Physical Review X **6**, 021043 (2016).

[15] M. Steudtner and S. Wehner, *Fermion-to-qubit mappings with varying resource requirements for quantum simulation,* New Journal of Physics **20**, 063010 (2018).

[16] N. Moll, A. Fuhrer, P. Staar, and I. Tavernelli, *Optimizing qubit resources for quantum chemistry simulations in second quantization on a quantum computer,* Journal of Physics A: Mathematical and Theoretical **49**, 295301 (2016).

[17] S. Bravyi, J. M. Gambetta, A. Mezzacapo, and K. Temme, *Tapering off qubits to simulate fermionic hamiltonians,* arXiv preprint arXiv:1701.08213 (2017).

[18] T. Peng, A. Harrow, M. Ozols, and X. Wu, *Simulating large quantum circuits on a small quantum computer,* arXiv preprint arXiv:1904.00102 (2019).

[19] V. Lipinska, G. Murta, J. Ribeiro, and S. Wehner, *Verifiable hybrid secret sharing with few qubits,* (2019), arXiv:1911.09470 .

[20] A. Smith, *Multi-party quantum computation,* (2001), arXiv:quant-ph/0111030 .

[21] A. Steane, *Multiple-particle interference and quantum error correction,* Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **452**, 2551 (1996).

[22] R. Canetti, *Universally composable signature, certification, and authentication,* in *Proceedings. 17th IEEE Computer Security Foundations Workshop, 2004.* (2004) pp. 219–233.

[23] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, *Authentication of quantum messages,* in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* (2002) pp. 449–458.

[24] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, *Multicast security: a taxonomy and some efficient constructions,* in *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, Vol. 2 (1999) pp. 708–716 vol.2.

[25] T. Rabin and M. Ben-Or, *Verifiable secret sharing and multiparty protocols with honest majority,* in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89 (ACM, New York, NY, USA, 1989) pp. 73–85.

[26] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist,* Phys. Rev. A **54**, 1098 (1996).

[27] D. Gottesman, *Theory of quantum secret sharing,* Phys. Rev. A **61**, 042311 (2000).

[28] A. J. Landahl, J. T. Anderson, and P. R. Rice, *Fault-tolerant quantum computing with color codes,* (2011), arXiv:1108.5738 .

[29] D. Gottesman, *Theory of fault-tolerant quantum computation,* Phys. Rev. A **57**, 127 (1998).

[30] A. M. Steane, *Active stabilisation, quantum computation, and quantum state sythesis,* Phys. Rev. Lett , 9608026 (1997).

[31] G. Nebe, E. M. Rains, and N. J. A. Sloane, *The invariants of the clifford groups,* Designs, Codes and Cryptography **24**, 99 (2001).

[32] A. Y. Kitaev, *Quantum computations: algorithms and error correction,* Russian Mathematical Surveys **52**, 1191 (1997).

[33] D. Beaver, *Foundations of secure interactive computing,* in *Advances in Cryptology — CRYPTO '91*, edited by J. Feigenbaum (Springer Berlin Heidelberg, Berlin, Heidelberg, 1992) pp. 377–391.

[34] S. Micali and P. Rogaway, *Secure computation,* in *Advances in Cryptology — CRYPTO '91*, edited by J. Feigenbaum (Springer Berlin Heidelberg, Berlin, Heidelberg, 1992) pp. 392–404.

[35] R. Canetti, *Universally composable security: A new paradigm for cryptographic protocols,* (2001) pp. 136 – 145.

[36] D. Unruh, *Universally composable quantum multi-party computation,* in *Advances in Cryptology – EUROCRYPT 2010*, edited by H. Gilbert (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010) pp. 486–505.

[37] D. Gottesman, *An introduction to quantum error correction and fault-tolerant quantum computation,* (2009), arXiv:quant-ph/0904.2557 .

6

CERTIFICATION OF A QUANTUM NETWORK FUNCTIONALITY

We consider testing the ability of quantum network nodes to execute multi-round quantum protocols. Specifically, we examine protocols in which the nodes are capable of performing quantum gates, storing qubits and exchanging said qubits over the network a certain number of times. We propose a simple ping-pong test, which provides a certificate for the capability of the nodes to run certain multi-round protocols. We first show that in the noise-free regime the only way the nodes can pass the test is if they do indeed possess the desired capabilities. We then proceed to consider the case where operations are noisy, and provide an initial analysis showing how our test can be used to estimate parameters that allow us to draw conclusions about the actual performance of such protocols on the tested nodes. Finally, we investigate the tightness of this analysis using example cases in a numerical simulation.

This chapter has been published, with minor changes, in V. Lipinska, T. Phuc Le, J. Ribeiro and S. Wehner *Certification of a functionality in a quantum network stage*, Quantum Sci. Technol. 5 035008 (2020).

6.1. INTRODUCTION

Quantum communication allows us to solve tasks that are impossible to achieve using classical communication alone. The most well known example of such a task is quantum key distribution (QKD) [1, 2], but many more application protocols are already known (see e.g. [3]). Such application protocols run on the end nodes of a quantum network. These may range from simple photonic devices capable of preparing and measuring qubits, to sophisticated quantum processors. Recently, stages of development for a quantum internet were identified [3], where each stage is distinguished by a specific functionality that is offered to a user wishing to execute quantum network applications. Higher stages bring an increase of functionality – and thus a richer set of possible application protocols – at the expense of increased experimental difficulty.

Given such stages of development, one can ask whether there exists an efficient test to certify that a network offers the capabilities of a specific stage, and with what quality parameters. Here, we will examine this question with a focus on a specific set of protocols in the stage called a *quantum memory network* [3]:

> *"For any two end nodes A and B the network allows the execution entanglement generation and the following additional tasks in any order: (i) preparation of a single-qubit ancilla state $|\psi\rangle$ by end node A or B, (ii) measurements of any subset of the qubits at node A or B, (iii) application of an arbitrary unitary gate G at node A or B. (iv) storage of the qubits for a minimum time $k\cdot(\ell_z+\tau)$, where τ is defined as the time that is required to generate one Einstein–Podolsky–Rosen (EPR) pair and send a classical message from node A to B maximized over all pairs of nodes, ℓ_z is the time that it takes for the execution of a depth z quantum circuit at the end node."*

Note that to realize useful application protocols, the storage time τ needs to be understood as the communication time in the network. In particular, the nodes that are far apart must exhibit longer storage capabilities to achieve this stage of development. Moreover, the stage is only attained if *any* two nodes in the network can realize the functionality, even those that are farthest apart. Therefore, time τ can be thought of as the maximum time which takes any two nodes to communicate.

To certify that a quantum network achieves a functionality defined by this stage of development, we will consider a set of protocols which pass a qubit state $|\psi\rangle$ a number k of times between the nodes A and B, apply the gates and measure at the end. We will choose the testing nodes A and B to be farthest apart in the network.

Many existing tests are known that can be used to estimate whether the operations above can each be performed individually with high accuracy. Examples include quantum state [4] and process tomography [5], gate set tomography [6, 7], randomized benchmarking [8–10] or capacity estimation to verify the quality of qubit transmission [11]. The concept of self-testing even allows such estimates to be made with only partial trust in the devices (so called device-independent setting) [12, 13]. Having estimated the quality of each individual operation with metrics such as the diamond distance, it is straight-

forward to derive an overall estimate on how well protocols in this stage may be executed [3]. Yet, running many individual tests is rather inefficient, and one may wonder whether there might exist an integrated test that instills confidence that we are capable of performing protocols up to a certain number of rounds using the quantum memory network.

Another approach to testing quantum devices comes from the literature of (interactive) proof systems where a verifier interacts with one or more provers, who are trying to convince the verifier that a certain assertion is true, or indeed that they possess certain capabilities. A well known example of such work is the question whether a classical polynomially bounded verifier can convince herself that (two non-communicating) provers holding a quantum computer do indeed have full quantum computing capabilities [14]. Restricting to only a single prover, there exists also a verification protocol under complexity theoretic assumptions [15]. This line of research is not concerned with the quality of specific operations, but rather aims to obtain a certificate of the provers' general abilities to solve certain tasks. Such tests are appealing as they measure general aptitude – for example in the domain of quantum computation the ability to execute quantum algorithms – but do not typically make specific statements such as the actual number of physical qubits involved. Consequently, such tests usually require large amount of resources to be executed.

6.2. RESULTS

Here we take a first step towards finding effective tests to certify that a network has reached the quantum memory stage of development (see Definition 18). We propose a test which can be interpreted from two different angles. First, we interpret it as a prover-verifier type protocol inspired by interactive proof literature, to certify that the network has certain capabilities. Second, we interpret it as a tomography-type protocol where we estimate certain properties of operations.

- **Ping-pong test.** We formulate our test in a bipartite scenario where nodes A and B exchange quantum registers according to a defined set of rules. We call our test the ping-pong game as it is executed by passing qubits back and forth between two nodes. Additionally, the nodes apply gates specified by a gate set G. An important parameter of our test is the number of times k that the nodes pass (ping-pong) the state around.

- **Prover-verifier view.** Our protocol can be viewed as a simple game that the provers (the nodes) play against the verifier with the objective of convincing the verifier that they are capable of executing any protocol in the quantum memory stage, which has a specific form. In particular, we show that the provers win the k-round ping-pong game with probability one if and only if they are capable of executing perfectly any protocol of the following form: for any possible starting state $|\psi\rangle$, each node is capable of executing one possible gate $G \in \mathsf{G}$, before sending the resulting state to the other node. The nodes continue in this form for k rounds, before measuring at the end. Moreover, in the case when the winning probability is strictly less than one, we certify that the nodes sent information about the state at least a certain number $m < k$ of times.

- **Estimation view.** In the estimation view we take on a different perspective with the objective to estimate the quality of the operations performed by the nodes, as opposed to certifying their capabilities. We use the statistics of the ping-pong test to assess a measure of the overall quality of the network. We then compare this to the quality one would expect from combining the estimates of the individual devices used in the network. What is more, we estimate the performance of k-round protocols based on our ping-pong test. In order to evaluate the accuracy of our analytical results, we compare our analytical estimate with numerical estimates for a specific example of a k-round protocol influenced by noise.

This chapter is organized as follows. In Section 6.3 we define the k-round protocols and introduce our test. Then, inspired by the interactive proof literature, in Section 6.4 we view our test in the prover-verifier setting. In Section 6.5 we view our test in the context of estimation.

6.3. PING-PONG TEST

6.3.1. ASSUMPTIONS

IID. Protocol 1 (see Section 6.3.3) implements n executions of a ping-pong procedure, each of them containing at most k rounds. In Section 6.4 (prover-verifier view) we assume that the execution of each of these ping-pong procedures is independent of the others and identical. In particular, this means that the provers' strategy will be the same in every execution of the ping-pong procedure, i.e. their strategy is independent and identically distributed (IID) across executions. However, within one execution, the provers' strategy can involve arbitrary correlation across rounds. Furthermore, in Section 6.5 (estimation view), we assume that every round of the ping-pong procedure is independent of the others, although does not have to be identical.

EPR pairs. The main objective in the quantum memory network stage is using quantum memory in the presence of local gates. Therefore, for simplicity, we assume that any pair of nodes can generate a perfect EPR pair between them. This assumption is strictly speaking not necessary, but merely serves as an aid in understanding our test. In Section 6.5.5 we show how to remove this assumption and how the noise associated with an EPR pair can be absorbed into the noise of the quantum memory.

State preparation and measurement. For the same reasons as above, we also assume that any node can perfectly prepare a local qubit state and perfectly measure at the end of a protocol. In Section 6.5.5 we also discuss how to relax this assumption.

Hilbert space dimension. For the sake of clarity, throughout the rest of the chapter we will assume that protocols run on a single qubit. We remark that the results we present generalize for any number Q of qubits (for details see Section 6.7.7).

Device stability. In the estimation view Section 6.5 (in particular in Theorem 20) we assume that after the devices were tested with the ping-pong test, their behavior does not change. That is, the devices used during the test and in a k-round protocol are identical. Note that this can be understood as a consequence of the above IID assumption for the estimation view.

6.3.2. k-ROUND PROTOCOLS

We start with formally describing k-round protocols. A bipartite k-round protocol between any two nodes A and B consists of the following consecutive operations:

1. Local preparation PREP of a perfect qubit state $|\psi\rangle$ by node A.
2. Sending deterministically the local qubit from node A to node B and vice versa, using a quantum channel $\mathscr{E}_{A\to B}$. Note that the time t_{send} it takes to send a qubit (or a classical bit) from node A to B is upper-bounded by the distance between them and the transmission speed for the qubit carrier. For example, for optical qubits the transmission speed can be understood as the speed of photons in a fiber [3].
3. Storing the local qubit by nodes A or B, denoted by M_A and M_B respectively. Storage of the qubit takes time t_M.
4. Applying an arbitrary local operation by a node on the local qubit. We describe this operation by a gate $G_A \in \mathsf{G}$ and $G_B \in \mathsf{G}$, where G is an arbitrary set of gates, for example the single-qubit Clifford gates. Executing a circuit of depth z takes time ℓ_z.
5. Perfect local measurement of the local qubit at the end of the protocol. The measurements are specified by operators Π_A and Π_B for nodes A and B respectively.

Steps 2. – 4. are performed in rounds $j = 1, ..., k$ a total number of k times. We call k the depth of the protocol. Each round takes time $\Delta t = t_{\text{send}} + t_M + \ell_z$, so that $t_{j+1} - t_j = \Delta t$, for all j. Without loss of generality we assume here that the protocols always start at node A. Note that the parity of j indicates at which node the single qubit is located, i.e., for odd j the qubit is held (sent) by A and for even j – by B. Therefore, we denote the local operations performed by A or B at a j-th round by simply putting M_j, G_j. In particular, in this notation $\mathscr{E}_j$ means that a qubit is sent by A and received by B for odd j ($\mathscr{E}_j \equiv \mathscr{E}_{A_j\to B_j}$), and vice-versa for even j.

Definition 18 (k-round protocols)**.** We define a k-round protocol as a map of the form $\Pi \circ \mathscr{P}^k \circ \text{PREP}$, where:

- PREP is a preparation of a local qubit $|\psi\rangle$ (Step 1).
- $\mathscr{P}^k$ is a map describing k rounds of local operations – memories M_j and gates G_j, as well as sending a qubit between A and B (Steps 2 – 4),

$$\mathscr{P}^k = \bigcirc_{j=1}^{k} G_j \circ M_j \circ \mathscr{E}_j. \tag{6.1}$$

- Π is a local measurement of all the local qubits (Step 5). Note that depending on the parity of k the measurement is performed either on A's or B's side.

6.3.3. TEST

In this section we describe our ping-pong test. The test is a simple instance of a k-round protocol as in Definition 18. As we will see in next sections, passing the test will allow us to draw conclusion about the whole class of k-round protocols.

Since our test will be later on viewed from two different angles, we introduce a node V which will interact with the nodes A and B. In the prover-verifier view, Section 6.4, the node V will act as a verifier. Whereas, in the estimation view, Section 6.5, the nodes A and B can take up the role of V. We choose the testing nodes A and B to be farthest apart in the network. For those nodes it is the hardest to fulfill the test, since they must account for the longest communication delays.

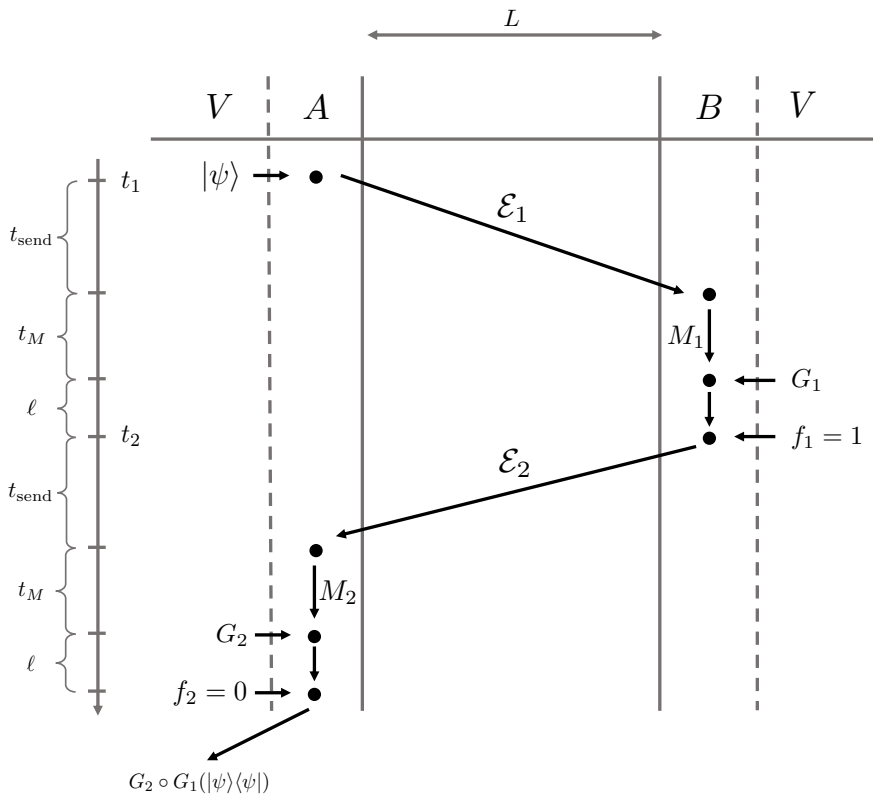


Figure 6.1: A schematic illustrating a single execution of depth $\kappa = 2$ of the ping-pong test, Test 1.

GENERAL PING-PONG TEST

The ping-pong test of depth κ for a sequence of chosen gates $\vec{g}_\kappa = G_1, \ldots, G_\kappa$ can be associated with the following operator

$$\mathscr{S}_\kappa = \bigcirc_{j=1}^{\kappa} G_j \circ M_j \circ \mathscr{E}_j. \tag{6.2}$$

In a single execution of Test 1, the test can succeed with a certain probability. For all executions i, we define such probability, conditioned on a specific input state $|\psi\rangle$, a fixed

Test 1 General ping-pong test (k,G,$\mathscr{X}$)

Fix maximum depth k, gate set G and set of states $\mathscr{X}$. Fix a total number of executions n.

for $i = 1,\ldots,n$ **do**
  V chooses depth κ uniformly at random and constructs a challenge string $\vec{f}_\kappa = 1\ldots110$ of length κ
  V samples independently κ gates from the set G and creates a sequence $\vec{g}_\kappa = G_1\ldots G_\kappa$
  V samples a state $|\psi\rangle \in \mathscr{X}$ and distributes it to A ▷ $t_1 = 0$
  for $j = 1,...,\kappa$ **do**
    if j odd **then**
      A sends $|\psi\rangle$ to B using $\mathscr{E}_j$ ▷ t_j
      B stores the received state in memory M_j ▷ $t_j + t_{\text{send}}$
      V gives a classical description of G_j to B ▷ $t_j + t_{\text{send}} + t_M$
      B applies G_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0,1\}$ to B according to the string $\vec{f}_\kappa$ ▷ $t_j + t_{\text{send}} + t_M + \ell$
      if $f_j = 1$ **then**
        $j = j + 1$
        continue
      else
        B outputs his state
        V measures $\{\Pi_\kappa^{\checkmark} = \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{\times} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' accept, '1' reject)
        break
    else if j even **then**
      B sends $|\psi\rangle$ to A using $\mathscr{E}_j$ ▷ t_j
      A stores the received state in memory M_j ▷ $t_j + t_{\text{send}}$
      V gives a classical description of G_j to A ▷ $t_j + t_{\text{send}} + t_M$
      A applies G_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0,1\}$ to A according to the string $\vec{f}_\kappa$ ▷ $t_j + t_{\text{send}} + t_M + \ell$
      if $f_j = 1$ **then**
        $j = j + 1$
        continue
      else
        A outputs her state
        V measures $\{\Pi_\kappa^{\checkmark} = \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{\times} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' accept, '1' reject)
        break

depth κ and a fixed sequence of gates $\vec{g}_\kappa$ as

$$p_{\checkmark|\psi,\vec{g}_\kappa,\kappa} = \mathrm{Tr}\left[\mathscr{S}_\kappa(|\psi\rangle\langle\psi|)\cdot\Pi_\kappa^{\checkmark}\right] \tag{6.3}$$

and similarly the probability of failure, $p_{\times|\psi,\vec{g}_\kappa,\kappa} = \mathrm{Tr}\left[\mathscr{S}_\kappa(|\psi\rangle\langle\psi|)\cdot\Pi_\kappa^{\times}\right]$. Note that $p_{\checkmark|\psi,\vec{g}_\kappa,\kappa}$ does not depend on the execution i, since we assume that executions are IID. Here $\{\Pi_\kappa^{\checkmark},\Pi_\kappa^{\times}\}$ denotes the measurement performed by V at the end of each execution i. We fix the figure of merit to be the average probability $P_{\checkmark}$ that the nodes succeed ($v_i = 1$) in the test.

Definition 19 (average probability of success for Test 1)**.** The probability of success in the general ping-pong test, Test 2, averaged over depths κ, strings of gates $\vec{g}_\kappa$ of length κ, and states $|\psi\rangle \in \mathscr{X}$ is defined as

$$\begin{aligned} P_{\checkmark} &= \frac{1}{n}\sum_i \frac{1}{k}\sum_\kappa \frac{1}{|\mathscr{X}|}\sum_\psi \frac{1}{|\mathsf{G}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{g}_\kappa,\kappa} \\ &= \frac{1}{k}\sum_\kappa \frac{1}{|\mathscr{X}|}\sum_\psi \frac{1}{|\mathsf{G}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{g}_\kappa,\kappa}, \end{aligned} \tag{6.4}$$

where the last equality holds due to the IID assumption. Here k is the maximum depth of the test, $\mathscr{X}$ is the chosen set of states and G is the chosen set of gates.

In our test, the task of the nodes is to send ("ping-pong") an unknown state an unknown number of times and at every ping-pong *round* apply a quantum operation given by V, see Figure 6.1. Additionally, at every round V gives the nodes a challenge denoted by f – either to output the quantum state or continue the ping-pong. At the end of each *execution* of the test, $i = 1,\ldots,n$, the nodes output a state. V measures this output and produces a single classical bit v^i: 1 means "accept" and 0 means "reject", see Test 1. As stated before, we assume that the nodes' operations are independent and identical across executions i of the test. This implies that v^i are independent and identically distributed (IID) random variables. We define a winning rate in such a game as the ratio of wins to the total number of executions:

$$R = \frac{1}{n}\sum_{i=1}^{n} v^i. \tag{6.5}$$

TELEPORTATION-BASED PING-PONG TEST

In the case when $\mathscr{X}$ is the set of all single-qubit states, the average probability of success gives us an estimate on the average fidelity of the test, see Section 6.5. This would require sampling from $\mathscr{X}$ according to the Haar measure in the test. However, the same can be achieved more efficiently, by using sampling from the finite set of the six Pauli states X. The reason for this is that X has a property of a 2-design, meaning that discrete uniform averaging over states (polynomials of degree 2) in X, reproduces the Haar average over the full state space. A similar observation holds for Haar sampling from a set of gates G in the case when G is a full unitary group. Then, it is enough to consider sampling from the Clifford group of single-qubit gates Cliff to reproduce the average probability of success.

Note that this allows us to estimate the average fidelity of the test, even in the case when one is not able to implement the full unitary group. Lastly, we remark that any set of states and unitary gates with 2-design properties can be used in place of the Pauli states and Clifford gates. For more details on 2-design properties of the above sets see Section 6.7.4.

Therefore, we consider a more efficient version of the ping-pong test, Test 2. Motivated by the above and the fact that for a quantum network quantum channels between the nodes are realized by quantum teleportation, we choose:

1. the set of states is the set of six Pauli eigenstates, $|\psi\rangle \in \mathsf{X}$ with a uniform probability distribution $\frac{1}{|\mathsf{X}|} = \frac{1}{6}$;
2. the set of gates is the Clifford set for a single qubit, $C_j \in \mathsf{Cliff}$ with a uniform probability distribution $\frac{1}{|\mathsf{Cliff}|}$;
3. sending a qubit from node A to B is done with perfect deterministic teleportation.

We describe the teleportation-based ping-pong test with a triple $(k, \mathsf{Cliff}, \mathsf{X})$. Note that in this case the quantum channel at round j, $\mathscr{E}_j$, is equivalent to applying a quantum memory $M_j^{\mathscr{T}}$ to a half of the EPR pair by one of the provers. We can put $\tau = t_M + t_{\text{send}}$, which is the time required to generate one maximally entangled state and send over a classical message from node A to B. Hence, a teleportation-based ping-pong test of depth κ for a sequence of chosen Clifford gates $\vec{c}_\kappa = C_1, \ldots, C_\kappa$ can be associated with the following operator

$$\mathscr{T}_\kappa = \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathscr{T}}. \tag{6.6}$$

For detailed mathematical description of the test, we refer the reader to Section 6.7.2.

By using Definition 19 with the set of Pauli states X and the set of Clifford gates Cliff, the average probability of success for the teleportation-based ping-pong, Test 2, is

$$P_{\checkmark} = \frac{1}{k} \sum_{\kappa} \frac{1}{|\mathsf{X}|} \sum_{\psi} \frac{1}{|\mathsf{Cliff}|^\kappa} \sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}. \tag{6.7}$$

Note that in Test 2 the sampling of depths, gates and states is done uniformly at random. Using the definition of the expected value and the IID assumption ($\forall i, j\ \mathbb{E}[v_i] = \mathbb{E}[v_j]$), we can write that the winning rate has the expected value
$\mathbb{E}[R] = \frac{1}{k}\sum_\kappa \frac{1}{|\mathsf{X}|}\sum_\psi \frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \cdot 1 + p_{\text{✗}|\psi,\vec{c}_\kappa,\kappa} \cdot 0$.

Lemma 14. *The expected value of the winning rate R in Test 2, Eq. (6.5), is equal to the average probability of success $P_{\checkmark}$,*

$$\mathbb{E}[R] = P_{\checkmark}. \tag{6.8}$$

Corollary 1 (finite statistics)**.** The probability that the winning rate R differs from the average probability of success $P_{\checkmark}$ by more than ϵ is exponentially small in ϵ,

$$\Pr\left[|R - P_{\checkmark}| \leq \epsilon\right] \geq 1 - 2e^{-2n\epsilon^2}. \tag{6.9}$$

Furthermore, let us set $\delta = 2e^{-2n\epsilon^2}$. If one fixes confidence δ and accuracy ϵ, then the minimum number of rounds n necessary to attain these parameters is given by $n \geq \frac{\ln(2\delta^{-1})}{2\epsilon^2}$.

Test 2 Teleportation-based ping-pong test (k, Cliff, X)

Fix maximum depth k, fix the gate set to Clifford set Cliff and the set of states to the set of six Pauli states X. Fix the total number of executions n.

for $i = 1, \ldots, n$ **do**
  V chooses depth κ and constructs a challenge string $\vec{f}_\kappa = 1 \ldots 110$ of length κ
  V samples independently and uniformly at random κ gates from the set Cliff and creates a sequence $\vec{c}_\kappa = C_1 \ldots C_\kappa$
  V samples independently and uniformly at random a state $|\psi\rangle \in$ X and distributes it to A ▷ $t_1 = 0$
  for $j = 1, ..., \kappa$ **do**
    if j odd **then**
      A sends $|\psi\rangle$ to B using deterministic teleportation ▷ t_j
      B stores half of his teleportation EPR pair in memory $M_j^{\mathcal{T}}$ for time τ
      V gives a classical description of C_j to B ▷ $t_j + \tau$
      B applies C_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0, 1\}$ to B according to the string $\vec{f}_\kappa$ ▷ $t_j + \tau + \ell$
      if $f_j = 1$ **then**
        Set $B = A$ and $A = B$
        continue
      else
        B outputs his state
        V measures $\{\Pi_\kappa^{\checkmark} = \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{\times} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' reject, '1' accept)
        break
    else if j even **then**
      B sends $|\psi\rangle$ to A using deterministic teleportation ▷ t_j
      A stores half of her teleportation EPR pair in memory $M_j^{\mathcal{T}}$ for time τ
      V gives a classical description of C_j to A ▷ $t_j + \tau$
      A applies C_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0, 1\}$ to A according to the string $\vec{f}_\kappa$ ▷ $t_j + \tau + \ell$
      if $f_j = 1$ **then**
        continue
      else
        A outputs her state
        V measures $\{\Pi_\kappa^{\checkmark} = \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{\times} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' reject, '1' accept)
        break

6.4. PROVER-VERIFIER VIEW

In this section we interpret our test, Test 2 in the prover-verifier view. Specifically, we view our test as an interactive game played between a verifier V (trusted third party), and two provers (the nodes A and B) [16]. An interactive game is a situation where provers exchange a fixed-sized quantum register with the verifier n times. The verifier is honest and wants to verify a certain statement, operating according to a defined set of rules. However, potentially dishonest provers optimize towards a strategy that causes a verifier to output 1 (accept). We further assume assume a standard scenario, where the provers agree on their strategy prior to the beginning of the test and they do not communicate to readjust it during the execution, see Definition 21. In contrast to the interactive proof literature, in our framework we consider finitely many test executions and therefore, we can also make non-asymptotic statistical statements.

In this view, performing Test 2 allows us to certify that the provers have capabilities to perform k-round protocols. Indeed, if the provers follow the test then they can convince the verifier that they do so and achieve a high average probability of success. On the other hand, if the provers do not follow the test they cannot achieve a high probability of success and the verifier detects this behavior with high probability. Formally, we require that the test satisfies:

- *completeness* – if the provers are able to execute protocols that are certified by the test then they succeed in a game against the verifier, i.e. achieve a winning rate above a certain winning threshold t, $R > t$, see Eq. (6.5);
- *soundness* – if the provers are not able to execute protocols certified by the test, then they can only achieve a winning rate $R \leq t$.

6.4.1. SENDING CHANNEL

Let us now introduce a framework that formalizes what we mean by a round of a quantum communication. Whereas numerous schemes to describe local operations exist [4–10] it is not clear how to certify a round of quantum communication. To achieve this, we will assume that the provers are not honest, and might therefore employ an arbitrary strategy leading to a high probability of success. In particular, they might even try to not use a communication channel at all in some rounds of the protocol. As a consequence, we have to specify what we mean by a round of communication.

For sending classical bits one typically considers the following scenario: A chooses a random bit $b_{A_0} \in_R \{0,1\}$ at time t_0 and wishes to send it to B. We then say that the nodes used a classical channel $\mathscr{E}_{cl} : A \to B$ if the probability at time t_1 that B's bit is the same as A's, is equal to 1, $\Pr[b_{B_1} = b_{A_0}] = 1$. In analogy, we could say that quantum communication through a quantum channel $\mathscr{E} : A_0 \to B_1$ occurred if at time t_0 a quantum state $|\psi\rangle_{A_0}$ was input on node A and at time t_1 it appeared on node B with probability 1, $\Pr[\rho_{B_1} = |\psi\rangle\langle\psi|_{A_0}] = 1$.

Note that in the classical case, we can prove that the channel was used to send information about the bit only for one round, by giving a uniformly random bit to A and ask B to guess it. Indeed if B guesses it with probability higher than $1/2$ then some information must have traveled from A to B. Given a single bit as an input, one cannot generalize that to many rounds with a "ping-pong" type of protocol like Test 2. This is due to the

fact that before A sends information to B in the first round, she can keep a copy of the bit. However, this issue can be avoided in a quantum setting due to the no-cloning theorem [17]. Indeed, if A gets a random unknown state and B is able to output the exact same state (with probability 1), then not only did all the (quantum) information about the state traveled from A to B, but also A could not have kept any information about the state to herself (see Theorem 16).

While the above definition provides a good intuition of what is going on, it becomes impractical when states do not have a unit probability of being transmitted through a channel (which in relation to our test means $t < 1$). In such a scenario, classically, we can say that the nodes used a classical channel $\mathscr{E}_{cl} : A_0 \to B_1$ if the probability of correctly identifying A's input bit on B's side increased in time, $\Pr[\text{out}_{B_1} = b_{A_0}] > \Pr[\text{out}_{B_0} = b_{A_0}]$. This implies that some information about the bit must have been transferred from A to B, see Figure 6.2. Our definition of quantum communication is, therefore, a generalization of the above to the quantum case. We say that quantum communication $\mathscr{E} : A_0 \to B_1$ occurred if the probability of correctly outputting A's input quantum state on B's side increased in time, see Definition 20.

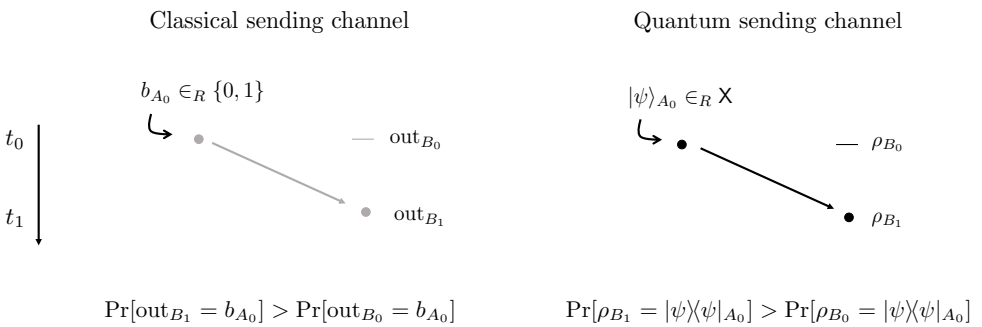


Figure 6.2: Informal representation of a sending channel in a classical and quantum case.

In words, we say that a sending channel was used by the nodes if the fidelity averaged over all states, and optimized over all operations Γ that the nodes can locally do, increased from instant t_0 to t_1. Note that the above definition implies that any communication, quantum or classical, which increases fidelity of the state is considered a sending channel. As an example consider the following strategy. Node A receives an unknown state from the verifier, measures it in the standard basis and sends the measurement outcome to B. Without loss of generality, let this measurement outcome be 0. Before receiving A's measurement outcome, B has average probability $\frac{1}{2}$ of correctly passing verifier's test. However, after receiving A's measurement outcome, B can locally prepare $|0\rangle$ state which increases the average probability of correctly identifying verifier's state to $\frac{2}{3}$. Therefore, there exists a purely classical strategy which satisfies our definition. As a consequence, we say that whenever the nodes do not use a sending channel $\mathscr{E}$, no communication (quantum or classical) occurred between them.

Definition 20 (sending channel)**.** A channel $\mathscr{E}_{A_0 \to B_1}$ is a sending channel if there exists a

CPTP map $\Omega_{A_0\to A_0B_0}$ such that $\forall\,|\psi\rangle_{A_0}$ it creates a state $\rho^{\psi}_{A_0B_0}=\Omega(|\psi\rangle\langle\psi|_{A_0})$ and

$$\sup_{\Gamma_{B_0B_1}}\int \mathrm{d}\psi\ \mathrm{Tr}\left[\Gamma_{B_0B_1}\left(\rho^{\psi}_{B_0B_1}\right)\cdot|\psi\rangle\langle\psi|_{A_0}\right] > \sup_{\Gamma_{B_0}}\int \mathrm{d}\psi\ \mathrm{Tr}\left[\Gamma_{B_0}\left(\rho^{\psi}_{A_0B_0}\right)\cdot|\psi\rangle\langle\psi|_{A_0}\right], \quad (6.10)$$

where $\rho^{\psi}_{B_0B_1}=\mathscr{E}_{A_0\to B_1}(\rho^{\psi}_{A_0B_0})$, Γ is a CPTP map which traces out additional registers of A and B and outputs a qubit state. In particular, if

$$\sup_{\Gamma_{B_0B_1}}\int \mathrm{d}\psi\ \mathrm{Tr}\left[\Gamma_{B_0B_1}\left(\rho^{\psi}_{B_0B_1}\right)\cdot|\psi\rangle\langle\psi|_{A_0}\right]=1 \quad\text{and}\quad \sup_{\Gamma_{B_0}}\int \mathrm{d}\psi\ \mathrm{Tr}\left[\Gamma_{B_0}\left(\rho^{\psi}_{A_0B_0}\right)\cdot|\psi\rangle\langle\psi|_{A_0}\right]=\frac{1}{2} \quad (6.11)$$

then we talk about an *exact sending* channel.

Definition 21 (m-cheating)**.** Provers A and B are m-cheating if their cheating strategy uses a sending channel $\mathscr{E}$ between them at most m times. We assume that the provers choose a strategy – in which round they use a sending channel and in which they do not – prior to the beginning of the test.

6.4.2. EXACT COMPLETENESS AND SOUNDNESS

To investigate the power of Test 2 in verifying capabilities of the network, we first consider an instructive case when $P_{\checkmark}=1$. If the nodes are able to perfectly execute the test then they succeed with a unit probability, trivially satisfying the completeness, see Theorem 15. On the other hand, if we demand that the nodes always succeed in the game, we can ask the question whether the nodes have the ability to perfectly execute protocols that have the form of Test 2, i.e., whether the test is sound. We answer this question positively in Theorem 16 below.

Theorem 15 (exact completeness)**.** *If the provers are honest and they are able to perfectly execute Test 2 then they succeed $P_{\checkmark}=1$.*

Theorem 16 (exact soundness)**.** *If the provers win the test with $P_{\checkmark}=1$ then they must be able to perfectly execute Test 2 and they use an exact sending channel $\mathscr{E}$ between them k times.*

Idea of the proof. To prove the theorem, we argue that $P_{\checkmark}=1$ implies that the probability of winning $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ for all states, all Clifford gates and all depths should be 1 (in particular, this implies that the provers are able to apply the required Clifford gates on the input state). Therefore, the average fidelity at every depth κ should be 1. That is, if at step $\kappa-1$ A has fidelity 1 it means that the state on A is pure, and by a purifying argument, B's average fidelity at step $\kappa-1$ must be 1/2. At step κ B has fidelity 1, which means that whatever channel A and B have used between step $\kappa-1$ and κ, it must be an exact sending channel (see Definition 20). For more details see Section 6.7.5. □

Note that in practice we are only able to observe the winning rate R and, due to the finite statistics of our test, we cannot certify $P_{\checkmark}=1$.

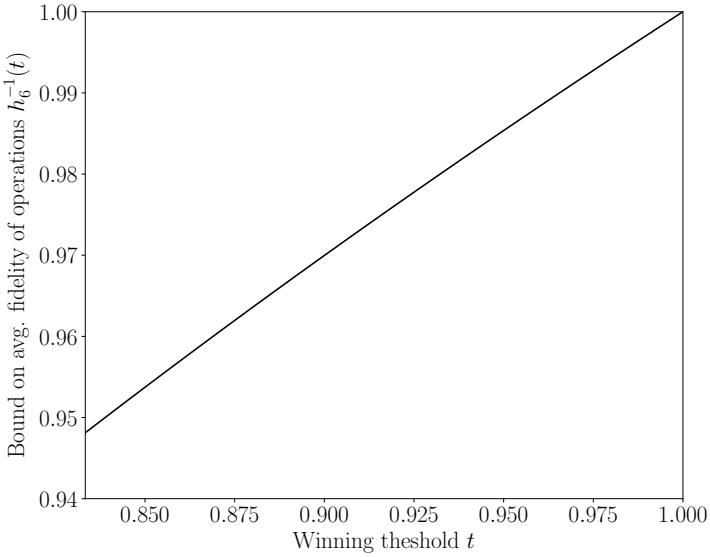


Figure 6.3: The average fidelity of individual operations $\bar{\mu}$ as a function of the winning threshold t (see Theorem 17 completeness). The plot shows the inverse of the function h_k, i.e. $h_k^{-1}(t)$ for $k = 6$ and relevant values of t.

6.4.3. COMPLETENESS AND SOUNDNESS

Therefore, let us explore the implications of Test 2, given that the winning rate $R > t$ is observed. If the provers are honest and their devices are sufficiently good, their winning rate should be larger than threshold t with high probability. More specifically, let memories and gates at every round j be described in terms of the average fidelity. Assume that the quality of memory and gates is the same at every round j, i.e. for all j, the average fidelity $\bar{\mu} = \int \mathrm{d}\psi \, \mathrm{Tr}\Big[C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot C_j(|\psi\rangle\langle\psi|)\Big]$. Below we show that for honest provers, a certain fidelity of operations implies a bound on the winning rate. In order to satisfy both completeness and soundness we choose the winning threshold $t > \frac{5}{6}$, since the Test 2 does not lead to any conclusion in the case when $t \leq \frac{5}{6}$, see Theorem 18. Let $h_k(\bar{\mu}) = \frac{\bar{\mu}(\bar{\mu}^k - 1)}{k(\bar{\mu} - 1)}$.

Theorem 17 (completeness)**.** *If provers are honest and their individual operations satisfy $\bar{\mu} \geq h_k^{-1}(t) + \epsilon$, then the winning rate R in Test 2 is bounded by $R \geq t$ with probability at least $1 - e^{-n\epsilon^2}$, where $t \in (\frac{5}{6}, 1]$ is a winning threshold and ϵ is given by Eq.* (6.9)*.*

Idea of the proof. Using 2-design properties of the set of states X and the set of gates Cliff, we show that in the regime where fidelity $\bar{\mu}$ is the same for every round j, we can express the average probability of success as a sum of powers of $\bar{\mu}$. That is, $P_{\checkmark} = \frac{1}{k}\sum_{\kappa=1}^{k} \bar{\mu}^{\kappa} = \frac{\bar{\mu}(\bar{\mu}^k - 1)}{k(\bar{\mu} - 1)} = h_k(\bar{\mu})$, see Section 6.7.5 for details. Since we want the winning rate R to be higher than the threshold t, we invert the function h_k to obtain a bound on the fidelity

of the devices $\bar{\mu}$. We plot the inverse $h_k^{-1}(t)$ in Figure 6.3 for $t \in (\frac{5}{6}, 1]$. □

Moreover, we can ask whether the converse of the above statement is true, i.e. whether a certain winning rate $R > t$ implies something about Test 2. When the provers are honest, we can reverse the completeness statement obtaining a bound on the quality of their devices. If the provers are dishonest (m-cheating) then they do not have to exactly follow the test. However, in this case we will show that the winning rate R allows us to certify that the provers used a sending channel (Definition 20) a certain number of times.

Theorem 18 (soundness)**.** *If the provers are m-cheating then the winning rate in Test 2 is bounded by $R \leq \frac{1}{k}\left(m + \frac{5}{6}(k-m)\right) + \epsilon$, with probability exponentially close to 1, i.e. at least $1 - e^{-n\epsilon^2}$, where $\epsilon \in (0,1)$.*

Idea of the proof. In the case when the provers are m-cheating they can agree on a cheating strategy which uses a quantum channel $\mathscr{E}$ between them at most m times, see Definition 21. To prove soundness in this case we look at the average probability of winning for A and B at time steps $\kappa - 1$ and κ. In Section 6.7.5 we argue that whenever the provers use the channel $\mathscr{E}$, this probability is bounded by 1. On the other hand, whenever they do not use the channel and no communication occurred, we argue that the average probability of winning at both time steps is bounded by $\frac{5}{6}$ which is the bound provided by the approximate cloning theorem [18]. Since the nodes use the channel $\mathscr{E}$ at least m times, their overall average probability of winning $P_{\checkmark}$ is bounded by $\frac{1}{k}\left(m + \frac{5}{6}(k-m)\right)$. □

The above theorem implies that in the situation when we do not trust the nodes, the higher m we would like to certify, the higher the winning threshold should be. Indeed, for $P_{\checkmark} \geq t$ we obtain $m \geq k(6t-5)$. If we now set $t = 1-\eta$, for some small η, then $m \geq k - 6k\eta$. For $m \sim k$, one should set at least $\eta = \mathcal{O}(k^{-1})$.

Remark. Note that in Theorem 16 we are able to fully certify the action of the provers, even if they are not trusted. In particular, we know that they have perfectly sent the state to each other k times. On the other hand, Theorem 18 only certifies the use of some quantum or classical channel regardless of its quality. In particular, in the limit where $P_{\checkmark} = 1$, Theorem 18 show that $m = k$ sending channels have been used, but we cannot explicitly certify the quality of the channel. However, the exact soundness statement, Theorem 16, suggests that even in the imperfect case, the test should be able to certify the quality of each individual operation used by the provers.

6.5. ESTIMATION VIEW

In this section we interpret our test in the context of estimation in order to obtain measures of confidence in the nodes' ability to perform the test. We assume that the nodes A and B are honest and follow the protocol. Specifically, we use the winning rate R in the teleportation-based ping-pong test, as a figure of merit to estimate the quality of the network. We then provide a consistency check which allows us to compare this to the quality one would expect from combining the individual devices. Furthermore, we use the statistics of the test to estimate the performance of k-round protocols.

Throughout this section we will use a tilde to denote noisy counterparts of operations, for example $\tilde{\mathcal{T}}_\kappa$ will denote a noisy realization of the κ-round teleportation-based ping-pong test $\mathcal{T}_\kappa$, Test 2.

6.5.1. PRELIMINARIES

In this section we introduce mathematical tools which will be useful for *(i)* checking whether the test is consistent when the honest nodes use devices of a certain quality, Section 6.5.2, and *(ii)* drawing conclusions about the performance of k-round protocols, Section 6.5.3 and 6.5.4.

We describe the quality of individual devices with a noise model. Specifically, we assume that the individual operations used in the test, i.e. memories M_j and gates C_j, have been tested individually for each round j, to obtain an estimate on their performance. More formally, let the quality of a noisy gate $\tilde{C}_j$ at round j, be described with the average fidelity, $\bar{F}(\tilde{C}_j) = \int \mathrm{d}\psi \,\mathrm{Tr}\left[\tilde{C}_j(|\psi\rangle\langle\psi|)\cdot C_j(|\psi\rangle\langle\psi|)\right]$, for all $j = 1,\ldots,k$. Furthermore, let the average fidelity have an empirical estimate r_{C_j}, which is known with certain precision [19], such that

$$\Pr\left[|r_{C_j} - \bar{F}(\tilde{C}_j)| \leq \epsilon_{C_j}\right] \geq 1 - \delta_{C_j}, \tag{6.12}$$

where $\delta_{C_j} = 2e^{-2n_{C_j}\epsilon^2_{C_j}}$. Here n_{C_j} is the number of repetitions with which the estimate r_{C_j} was obtained. Similarly, for $\tilde{M}_j^{\mathcal{T}}$ a noisy quantum memory at round j, average fidelity is $\bar{F}(\tilde{M}_j^{\mathcal{T}}) = \int \mathrm{d}\psi \,\mathrm{Tr}\left[\tilde{M}_j^{\mathcal{T}}(|\psi\rangle\langle\psi|)\cdot M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|)\right]$. This average fidelity has an empirical estimate $r_{M_j^{\mathcal{T}}}$ and a precision bound

$$\Pr\left[|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| \leq \epsilon_{M_j^{\mathcal{T}}}\right] \geq 1 - \delta_{M_j^{\mathcal{T}}}, \tag{6.13}$$

where $\delta_{M_j^{\mathcal{T}}} = 2e^{-2n_{M_j^{\mathcal{T}}}\epsilon^2_{M_j^{\mathcal{T}}}}$. Furthermore, we assume that the nodes can locally and perfectly prepare and measure a quantum state.

The teleportation-based ping-pong test, Test 2, is performed the total of n times. Note that one can easily record which executions i were performed for depths κ, states ψ and strings of Clifford gates $\vec{c}_\kappa$. Then, in analogy to Eq. (6.5), we can define the winning rate for a *fixed* depth κ and string $\vec{c}_\kappa$,

$$R_{\vec{c}_\kappa,\kappa} = \frac{1}{n_{\vec{c}_\kappa,\kappa}} \sum_i v^i_{\vec{c}_\kappa,\kappa}, \tag{6.14}$$

where $n_{\vec{c}_\kappa,\kappa}$ is a total number of executions for fixed κ and $\vec{c}_\kappa$, and $v^i_{\vec{c}_\kappa,\kappa}$ is a corresponding random variable assuming values 0 and 1 for 'lose' and 'win' events respectively. Analogously, we can record which executions correspond to a fixed depth κ only. We define

$$R_\kappa = \frac{1}{n_\kappa} \sum_i v^i_\kappa \tag{6.15}$$

as the winning rate for a fixed κ. Here n_κ is a total number of executions for depth κ and v_κ^i is a corresponding random variable recording the wins in the test.

Now we will relate the above winning rates to the measures of quality of the test. Intuitively, the higher the winning rate the better the test performs and the less noise is present in the setup. In the remaining part of this section we make that statement rigorous.

Lemma 15. *Let the average fidelity of a noisy realization of Test 2, $\tilde{\mathcal{T}}_\kappa$, for a fixed depth κ and a fixed string of Clifford gates $\vec{c}_\kappa$ be defined as $\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa) = \int \mathrm{d}\psi \,\mathrm{Tr}\big[\tilde{\mathcal{T}}_\kappa(|\psi\rangle\langle\psi|)\cdot\Pi_\kappa^{\checkmark}\big]$, where $\mathcal{T}_\kappa$ is defined as in Eq. 6.6. The expected value of the winning rate $R_{\vec{c}_\kappa,\kappa}$ over the set of states X, is equal to the average fidelity of the test $\tilde{\mathcal{T}}_\kappa$,*

$$\mathbb{E}\left[R_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa). \tag{6.16}$$

Idea of the proof. The first step of the proof is to notice that the expected value of the variable $v^i_{\vec{c}_\kappa,\kappa}$ is the probability of success in a single round averaged over all the states in X,

$$\mathbb{E}\left[v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}}\left(p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\cdot 1 + p_{\times|\psi,\vec{c}_\kappa,\kappa}\cdot 0\right) = \frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}}\mathrm{Tr}\left[\tilde{\mathcal{T}}_\kappa(|\psi\rangle\langle\psi|)\cdot\Pi_\kappa^{\checkmark}\right] \tag{6.17}$$

The second step is based on relating the above quantity to the average fidelity. Here the key idea is to observe that the expression under the trace contains only polynomials of degree 2 in $|\psi\rangle\langle\psi|$. Therefore one can use the 2-design properties of the set X to equate the discrete averaging over the six Pauli states to the continuous Haar averaging over the whole state space in average fidelity. The details of the proof can be found in Section 6.7.6. □

The above lemma has a simple useful corollary, namely, that the average fidelity and the winning rate $R_{\vec{c}_\kappa,\kappa}$ can be related through the Hoeffding inequality,

$$\Pr\left[|R_{\vec{c}_\kappa,\kappa} - \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa)| \geq \epsilon_{\vec{c}_\kappa,\kappa}\right] \geq 1 - 2e^{-2n_{\vec{c}_\kappa,\kappa}\epsilon^2_{\vec{c}_\kappa,\kappa}}. \tag{6.18}$$

Before we make a similar connection for the rate R_κ, let us define a useful quantity.

Definition 22 (double-averaged fidelity)**.** Let $\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa)$ be the average fidelity of a the teleportation-based ping-pong test, Test 2, defined for a fixed depth κ and a fixed sting of Clifford gates $\vec{c}_\kappa$. We define the quantity

$$\bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa) := \int \mathrm{d}C_1 ... \int \mathrm{d}C_\kappa \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa). \tag{6.19}$$

as double-averaged fidelity. The averaging for every gate C_j is taken according to the Haar measure.

Lemma 16. *The expected value of the winning rate R_κ in Test 2, for a fixed depth κ, taken over the set of states X and set of Clifford gates, is equal to the double-averaged fidelity of the test $\tilde{\mathcal{T}}_\kappa$,*

$$\mathbb{E}\left[R_\kappa\right]_{\mathsf{X},\mathsf{Cliff}} = \bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa). \tag{6.20}$$

The intuition behind the above lemma is that discrete averaging in $\mathbb{E}[R_\kappa]_{\mathsf{X},\mathsf{Cliff}}$ over the Clifford gates is equal to the continuous averaging in the definition of $\bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa)$. This statement follows from the unitary 2-design properties of the Clifford set, see Section 6.7.6 for details.

Finally, the probability that the empirical data R_κ differs from double-averaged fidelity by more than ϵ_κ is bounded by the Hoeffding inequality,

$$\Pr\left[|R_\kappa - \bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa)| \leq \epsilon_\kappa\right] \geq 1 - 2e^{-2n_\kappa \epsilon_\kappa^2}. \tag{6.21}$$

6.5.2. CONSISTENCY CHECK

In the following we demonstrate how to use the winning rates defined above to check for consistency, i.e. that devices with certain fidelities were used *together* in Test 2. Specifically, we provide a relation between the quality of the test in terms of $R_{\vec{c}_\kappa,\kappa}$ and what one may expect given individual devices with estimates of average fidelities $r_{M_j^{\mathcal{T}}}$ and r_{C_j}. Not satisfying this consistency-check relation implies that there is an internal contradiction in the reported values of individual average fidelities and observed rate $R_{\vec{c}_\kappa,\kappa}$.

Theorem 19 (consistency check)**.** *Let $r_{M_j^{\mathcal{T}}}$ and r_{C_j}, $j = 1,\ldots,k$, be empirical estimates of the average fidelity of all individual memories and gates respectively. Moreover let $R_{\vec{c}_\kappa,\kappa}$ be an empirical estimate of the average fidelity of the teleportation-based ping-pong test, Test 2, for a fixed depth κ and a fixed string of Clifford gates $\vec{c}_\kappa$. Devices with estimates $r_{M_j^{\mathcal{T}}}$ and r_{C_j} were used together in the test $\tilde{\mathcal{T}}_\kappa$ if the following inequality is satisfied [20],*

$$R_{\vec{c}_\kappa,\kappa} \geq \frac{2\cos^2\left(\sum_{j=1}^{\kappa} \operatorname{acos}\sqrt{\frac{3r_{M_j^{\mathcal{T}}}-1}{2}} + \operatorname{acos}\sqrt{\frac{3r_{C_j}-1}{2}}\right)+1}{3} - \epsilon_{\vec{c}_\kappa,\kappa} \tag{6.22}$$

The bound holds for any 2κ quantum channels such that $\sum_{j=1}^{\kappa} \operatorname{acos}\sqrt{\frac{3r_{M_j^{\mathcal{T}}}-1}{2}} + \operatorname{acos}\sqrt{\frac{3r_{C_j}-1}{2}} \leq \frac{\pi}{2}$, and $\epsilon_{\vec{c}_\kappa,\kappa}$ is given by Eq. (6.18).

Recall that the individual estimates are known with certain confidence. That means that the above consistency check will be satisfied with a certain probability. We state it formally in the corollary below.

Corollary 2. Given the estimates of average fidelities for memories $r_{M_j^{\mathcal{T}}}$ and gates r_{C_j} are known with confidence $\epsilon_{M_j^{\mathcal{T}}}$ and ϵ_{C_j} respectively, the bound from Theorem 19 is satisfied by noisy devices with probability at least $1 - 2\sum_{j=1}^{\kappa}\left(e^{-2n_{C_j}\epsilon_{C_j}^2} + e^{-2n_{M_j^{\mathcal{T}}}\epsilon_{M_j^{\mathcal{T}}}^2}\right)$.

Idea of the proof. The probability that the bound (6.22) is satisfied is equal to the unity, minus the probability that at least one of the bounds for individual devices is not satisfied. By properties of probability one arrives at the statement above, see Section 6.7.6 for details. □

6.5.3. PERFORMANCE OF k-ROUND PROTOCOLS

In this section we investigate the implications of Test 2 for the performance of more general k-round protocols $\tilde{\mathscr{P}}^k$, see Definition 18. We show that their performance can be bounded using the winning rate R_κ (Section 6.5.1) in the teleportation-based ping-pong test.

To explore the performance of protocols $\tilde{\mathscr{P}}^k$ we consider the diamond distance [21], $\| \Pi \circ \tilde{\mathscr{P}}^k \circ \text{Prep} - \Pi \circ \mathscr{P}^k \circ \text{Prep} \|_\diamond$. However, since Prep and Π are perfect by assumption, the above diamond distance is upper-bounded by $\| \tilde{\mathscr{P}}^k - \mathscr{P}^k \|_\diamond$, which we fix to be the figure of merit in this section. It can be shown that the diamond distance is related to the average fidelity in the following way [22],

$$\| \tilde{\mathscr{P}}^k - \mathscr{P}^k \|_\diamond \leq 2\sqrt{6}\sqrt{\left(1 - \bar{F}_{k,\vec{g}_k}(\tilde{\mathscr{P}}^k)\right)}, \tag{6.23}$$

where $\bar{F}_{k,\vec{g}_k}(\tilde{\mathscr{P}}^k) = \int \mathrm{d}\psi \, \mathrm{Tr}\left[\tilde{\mathscr{P}}^k(|\psi\rangle\langle\psi|) \cdot \mathscr{P}^k(|\psi\rangle\langle\psi|)\right]$ is the average fidelity of a protocol $\tilde{\mathscr{P}}^k$ of a fixed depth k and for a fixed string of gates $\vec{g}_k$. Note that the average fidelity differs depending on the sequence of gates one chooses to apply. Therefore, to estimate the behavior of protocol $\tilde{\mathscr{P}}^k$ one would have to know fidelities $\bar{F}_{k,\vec{g}_k}(\tilde{\mathscr{P}}^k)$ for all possible gate sequences $G_1, ..., G_k$, which is unfeasible in practice. For this reason, it is much more convenient to use double-averaged fidelity to bound the performance of a protocol $\tilde{\mathscr{P}}^k$. We formalize this argument in the following theorem.

Theorem 20 (Performance of k-round protocols)**.** *The performance of single-qubit k-round protocols, Definition 18, can be bounded in terms of an estimate for the double-averaged fidelity R_k of the k-round teleportation-based ping-pong test, Test 2, in the following way*

$$\| \tilde{\mathscr{P}}^k - \mathscr{P}^k \|_\diamond \leq 2\sqrt{6}\sqrt{|\mathsf{Cliff}|^k \left(1 - R_k + \epsilon_k\right)} \tag{6.24}$$

where $|\mathsf{Cliff}|$ *is the size of the Clifford group for dimension* 2 *and* ϵ_k *is given by Eq.* (6.21)*. The bound is satisfied with probability* $1 - e^{-2n_\kappa \epsilon_\kappa^2}$.

Idea of the proof. To prove the theorem, one first needs to observe that the double-averaged fidelity, $\bar{\bar{F}}(\tilde{\mathscr{P}}^k)$, can be lower-bounded by $\bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k)$ minimized over all possible strings of gates $\vec{g}_k$, see Section 6.7.6 for details.

Moreover we have that $\bar{\bar{F}}_k(\tilde{\mathscr{P}}^k) = \bar{\bar{F}}_{\kappa=k}(\tilde{\mathscr{T}}^{\kappa=k})$. It follows from the fact that averaging over the Clifford group is equivalent to averaging over the entire unitary group, since the Clifford group forms a 2-design. Furthermore, the equality is possible, since we have put $M_j^{\mathscr{T}} \equiv M_j \circ \mathscr{E}_j$, and $M_j^{\mathscr{T}}$ encompasses operations associated with sending (in the test – teleporting) and storing the qubit. Combining the above with Eqs. (6.20) and (6.23) yields the desired result. □

Finally, observe the above results can be straightforwardly generalized to bound the performance of protocols $\tilde{\mathscr{P}}^K$ for depth $K > k$. Since the teleportation-based ping-pong test is performed for all $1 \leq \kappa \leq k$, we can define a set S such that $\sum_{\kappa \in S} \kappa = K$. Then $\tilde{\mathscr{P}}^K = \bigcirc_{\kappa \in S} \tilde{\mathscr{P}}^\kappa$. Using the triangle inequality for the diamond distance, Theorem 20 can

be, therefore, rewritten as

$$\| \tilde{\mathscr{P}}^K - \mathscr{P}^K \|_\diamond \leq 2\sqrt{6} \sum_{\kappa \in S} \sqrt{|\mathsf{Cliff}|^\kappa (1 - R_\kappa + \epsilon_\kappa)}, \tag{6.25}$$

where ϵ_κ is given by Eq. (6.21).

6.5.4. SIMULATED RESULTS

To gain intuition on how the test performs in this section we consider a few numerical examples. First, we discuss the implications of the consistency check, Theorem 19 and articulate the relation between the average fidelity of individual devices and the maximal depth of the test k. Second, we discuss the performance of the test under common noise models, depolarizing and dephasing noise. Finally, we comment on bounding the noisy protocols $\tilde{\mathscr{P}}^k$ based on numerical results from the teleportation-based ping-pong test.

Assume a test of maximum depth $k = 2$, where we teleport a single qubit state at most two times between A and B. Moreover, for simplicity say that A and B have access to memories and gates of equal fidelities, $r_{M_j^{\mathscr{T}}} = r_{C_j} = r$. Observe that the higher depth of the test κ, i.e. the more devices one is testing, the higher individual fidelities should be, see Figure 6.4. Finally, note that the bound used for consistency check (6.22) was derived for a generic noise model and it was shown to be tight [20]. This means that if one does not have any additional knowledge about the noise present in the devices then the results presented here cannot be further improved.

Let us now look at two specific noise models. Namely, let us model memories and gates to be *(i)* single-qubit depolarizing channels, i.e. $\mathscr{D}(\rho) = p\rho + (1-p)\mathbb{1}/2$ and *(ii)* single-qubit dephasing channels, i.e. $\mathscr{F}(\rho) = q\rho + (1-q)(Z\rho Z^\dagger)/2$, where Z is the Pauli Z gate. Again, in these two cases let us fix the average fidelity estimate of individual devices r. Figure 6.5 presents the simulated behavior of the test as a function of individual estimates r in the two cases. Observe that the test performs according to intuitive expectations – if the noise is modeled as dephasing, the average fidelity of the test is higher than in the case of depolarizing noise, since the dephasing channel subjects any input state only to the Z component of the Pauli noise, whereas depolarizing channel to all X, Y and Z components. Therefore, we expect "more" noise when the state is subjected to the depolarizing noise.

Although in our network model we assume that the state preparation is perfect, it is interesting to see the behavior of the test once imperfect states are used. Figure 6.5 shows a result of simulation of the test when the initial state is submitted to a small dephasing noise, such that fidelity of the input state is 0.9. Note that if one has access to the average fidelity estimate of the noisy channel acting on the initial state, then one can use it in the consistency check (6.22), simply treating the noise of the state as an additional channel in the protocol.

Let us also comment on the bound from Theorem 20. Already for a single qubit one obtains a constant prefactor of $2\sqrt{d(d+1)} \approx 4.9$. In addition to that, bound (6.24) contains a factor associated with the size of the Clifford group – for a single qubit $|\mathsf{Cliff}| = 24$. If one considers protocols of maximum depth $k = 2$ then to obtain a non-trivial bound on the behavior of protocols in the class, the estimate of double-averaged fidelity must be of order $R_\kappa = 1 - 10^{-5}$. This puts a very high precision requirement on double-averaged

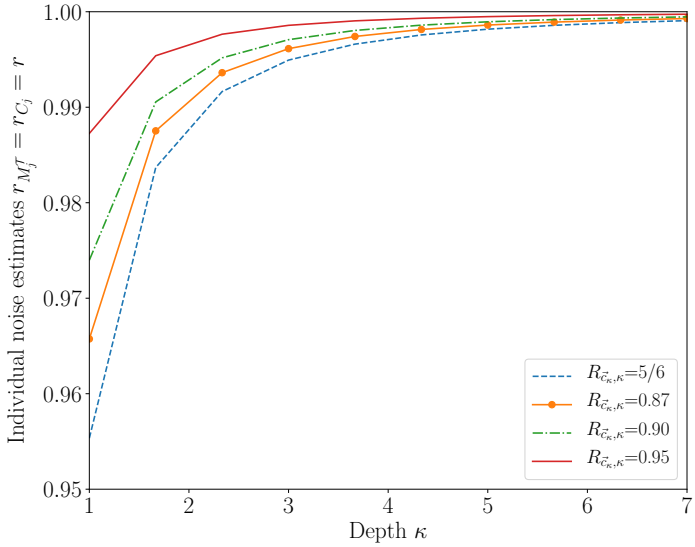


Figure 6.4: Minimum average fidelity r of individual operations (individual noise estimates) as a function of fixed depth κ for different winning rates $R_{\vec{c}_\kappa,\kappa}$. The plot shows the bound derived in Eq. (6.22).

fidelity and, consequently, on individual devices.

As an example consider the quantum gambling (QG) protocol [23]. In the protocol, A chooses one of the states $\{|0_z\rangle, |0_x\rangle\}$ and sends it to B. After receiving the state B stores the state and communicates classically his guess on the state sent by A. A upon receiving the classical message from B, communicates back whether B won or lost. After this round of communication B measures the state either in Z basis or X basis. Let the protocol be described with a map $\mathscr{P}_{QG}$ which consists of local operations on the state (except measurement and state preparation, as before). Then $\mathscr{P}_{QG}$ consists of $k = 2$ rounds of communication during which B has to store the state. Assume that in the protocol quantum memory is modeled as a depolarizing channel with fidelity $1 - 10^{-5}$. Then explicit evaluation of the diamond distance $\| \tilde{\mathscr{P}}_{QG} - \mathscr{P}_{QG} \|_\diamond$ yields value $6 \cdot 10^{-5}$. On the other hand if one uses a two-round test to bound the behavior of the protocol, without explicit *a priori* knowledge about the noise model of the memories then the bound from Theorem 20 has the value 0.7436. However, note that in the quantum gambling protocol one does not perform any gates. Using this explicit knowledge about the protocol one could in principle tailor a ping-pong teleportation-based test without any gates. In this case, there would be no need to average over gates and therefore, the bound from Theorem 20 would not carry the $|\mathsf{Cliff}|^k$ term. Consequently, the bound could be improved to value 0.0310.

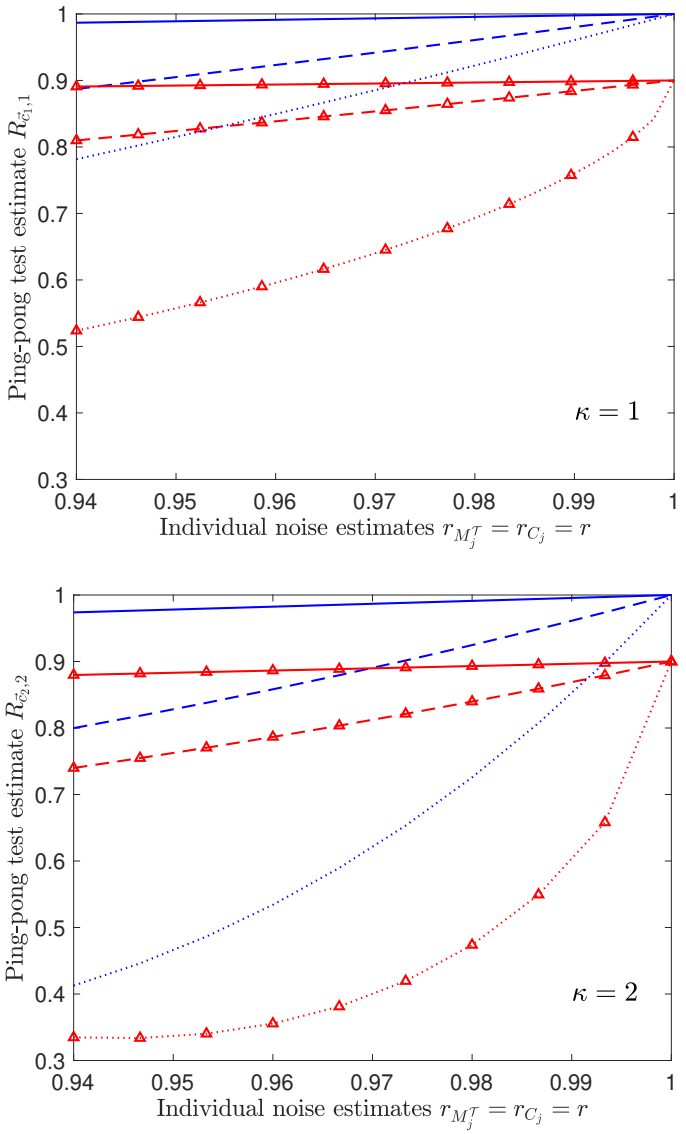


Figure 6.5: Average fidelity of the test as a function of the average fidelity of individual devices r, left plot for $\kappa = 1$, right plot for $\kappa = 2$. Solid lines represent simulation of the test with the dephasing channel $\mathscr{D}$, dashed lines the simulation of the test with the depolarizing channel $\mathscr{F}$, and dotted lines the value of the bound (6.22). No markers (blue color) correspond to the case where the input state is perfect, whereas the triangle markers (red color) to the case where the input state is dephased to initial fidelity 0.9.

6.5.5. MORE NOISE

In our network model we have assumed that state preparation, measurement, sending qubits as well as preparing a EPR pair can be done perfectly. In particular, this implies that in our test teleportation is carried out perfectly. However, the test can still be performed without major changes if one wishes to take into account noisy teleportation.

We consider two main noise sources arising in teleportation – noise coming from performing imperfect Bell measurement and recovery operation, and noise originating from creation of a EPR pair. In Section 6.7.3 we show that in a single round j of our test both of these noise types can be absorbed into the noise coming from the memory $\tilde{M}_j^{\mathcal{T}}$, for all j. For the former noise source we assume a noise model where the imperfections follow the Bell measurement but precede recovery operation. For the latter noise source, we assume that noise is local for each half of the EPR pair and that it can be modeled as mixed-unitary noise. That is, each half of the EPR pair is subjected to $N(\cdot) = \sum_l p_l U_l^\dagger(\cdot)U_l$, where U_l is a unitary operation, and p_l is a probability. Then all the teleportation noise can be included in the noise of the memory and we can carry out the test as described above, i.e. by sending qubits via perfect teleportation.

Similarly to the analysis outlined in the previous paragraph, we can treat the noise of the state preparation as if it arose in the teleportation. Indeed, one can absorb the noise in the initial state similarly to the analysis in Section 6.7.3. Note that in Figure 6.5 we indicate what one might expect from the test if the initial state is noisy. As for the noise in the final measurement, if we consider that the noisy measurement is described by a noise map N followed by a perfect measurement, then N can be treated as another noisy memory applied to the state before measuring. In this case, the analysis carried out in Lemma 20 of Section 6.7.4 still holds.

Finally, we remark that our test can be extended onto multi-qubit settings, where the number of qubits in the k-round protocol is Q. For a detailed description we refer the reader to Section 6.7.7.

6.6. CONCLUSIONS AND OUTLOOK

In this work we considered the problem of certifying that a quantum network achieves the ability to perform a subset of protocols within a certain stage of development, i.e. a stage called quantum memory network. We designed the first testing protocol, which certifies that nodes have the capability to control and send qubits around the network k times. We provided completeness and soundness statements for our protocol and expressed them in the interactive proof language. Moreover, in an honest implementation, we demonstrated that passing our test allows us to estimate statistical quantities about the devices used in the test and conclude about the performance of other k-round protocols in a quantum network.

An important question is how our estimate of performance for the class of multi-round protocols can be improved. Note that in our simple analysis we bound a very general class of protocols using a single test – we bound the behavior of any unitary gate in terms of behavior of a small subset of gates. Therefore, it is not surprising that there must exist a trade-off between universality of the protocols and the precision of estimating their performance. One improvement could result from designing tests for a more

specific (and therefore smaller) class of protocols. Alternatively, tailoring tests using additional knowledge of the underlying noise in a quantum network could improve the bound on the performance of k-round protocols.

Furthermore, as mentioned before, our test does not certify that any universal gate can be implemented. Due to the mathematical structures of unitary designs that we used, we can only make a statement about implementability of the gates from the Clifford set or any gate set with 2-design properties. It is, therefore, an open problem how to test a quantum memory in the presence of the set powerful enough to generate any unitary operation. Such a universal set is, for example, a Clifford set extended with a T gate [24, 25].

6.7. TECHNICAL STATEMENTS

In the following we present technical details of our work. We first provide mathematical preliminaries necessary for our further considerations in Section 6.7.1. Then, in Section 6.7.2 we give a detailed mathematical description of the general ping-pong test, Test 1, and the teleportation-based ping-pong test, Test 2. In Section 6.7.3 we justify why in the teleportation-based ping-pong test, it is possible to absorb the (possibly noisy) teleportation channel into a memory $M_j^{\mathcal{T}}$. Next, we discuss 2-design properties of sets of Pauli states and Clifford gates in Section 6.7.4. In Section 6.7.5 we prove completeness and soundness statements of our Test 2. Then, in Section 6.7.6 we give proofs of statements discussed in the estimation view of our test. Finally, we discuss how to extend our results to Q-qubit protocols in Section 6.7.7.

6.7.1. PRELIMINARIES

Communication between nodes of a quantum network can be described by quantum channels. A quantum channel can be described by a completely positive trace-preserving (CPTP) linear map $\Lambda : \mathbb{D}(\mathscr{H}) \to \mathbb{D}(\mathscr{H})$, where $\mathbb{D}(\mathscr{H})$ denotes the space of density operators acting on Hilbert space $\mathscr{H}$. In a realistic setup, quantum channels are not perfect (or ideal) and instead of applying a perfect channel Λ one applies its noisy counterpart $\tilde{\Lambda}$. If the perfect Λ is unitary, then without loss of generality, a noisy channel $\tilde{\Lambda}$ can be written as a noise map N followed by a perfect channel Λ, i.e. $\tilde{\Lambda} = \Lambda \circ N$. A sequence of n operations can be represented as a composition of n maps, $\tilde{\Lambda}_n \circ ... \circ \tilde{\Lambda}_1$.

One can quantify the difference between a noisy channel and its perfect implementation using the average fidelity.

Definition 23 (Average fidelity)**.** The average fidelity of the channel $\tilde{\Lambda}$ (to Λ) is defined as

$$\bar{F}(\tilde{\Lambda}) = \int \mathrm{d}\psi \, \mathrm{Tr}\left[\tilde{\Lambda}(|\psi\rangle\langle\psi|)\, \Lambda(|\psi\rangle\langle\psi|)\right], \tag{6.26}$$

where $\mathrm{d}\psi$ is the Haar measure on pure states.

Average fidelity is a quantity which can be accessed empirically and as such it is widely used as a parameter estimating the quality of a quantum channel. One cannot hope, however, to empirically average over the continuum of all pure states. Realisti-

cally, to access average fidelity one can use the properties of so called *quantum state designs*. Intuitively, a quantum design is a probability distribution over pure states, which replicates the properties of the Haar averaging over the entire space of pure states.

Definition 24 (Projective t-design)**.** A projective t-design is a distribution $\{q_\psi, \psi\}$ over some finite set of states such that

$$\sum_\psi q_\psi \left|\psi\right\rangle\!\left\langle\psi\right|^{\otimes t} = \int \mathrm{d}\psi \ \left|\psi\right\rangle\!\left\langle\psi\right|^{\otimes t}. \tag{6.27}$$

An example of a projective 2-design for qubits is given by a set of six Pauli eigenstates, X chosen with equal probability $\frac{1}{6}$. A similar definition can be used when talking about averaging over the unitary group $U(d)$ of dimension d, see [26] for details.

Definition 25 (Unitary 2-design)**.** A set $U(d)$ of unitary matrices is 2-design if for any quantum channel Λ holds that [27]

$$\frac{1}{|\mathscr{Y}|}\sum_{U_l\in\mathscr{Y}} U_l^\dagger \Lambda(U_l \rho U_l^\dagger) U_l = \int \mathrm{d}U \, U^\dagger \Lambda(U\rho U^\dagger) U \tag{6.28}$$

where $\mathrm{d}U$ denotes the Haar measure on $U(d)$. An example of a 2-design for a unitary group $U(d)$ is the Clifford group $\mathsf{Cliff}(d)$ with uniform probability of each element.

Another useful figure of merit for channels is the diamond distance [21].

Definition 26 (Diamond distance)**.** The diamond distance between two operators, $\tilde{\Lambda}$ and Λ, is defined through a distance measure on the space of density operators, maximized over all density operators ρ,

$$\| \tilde{\Lambda} - \Lambda \|_\diamond = \sup_\rho \| \tilde{\Lambda} \otimes \mathbb{1}(\rho) - \Lambda \otimes \mathbb{1}(\rho) \|_1, \tag{6.29}$$

where $\| \cdot \|_1$ is the trace distance. The operational meaning behind the diamond distance definition is that it quantifies the worst-case distinguishability of any two quantum channels when one is given access to entanglement with an auxiliary system.

From the properties of the diamond distance it follows that,

$$\| \tilde{\Lambda}_N \circ \ldots \circ \tilde{\Lambda}_1 - \Lambda_N \circ \ldots \circ \Lambda_1 \|_\diamond \leq \sum_{j=1}^{N} \| \tilde{\Lambda}_j - \Lambda_j \|_\diamond . \tag{6.30}$$

Note that such a relation cannot be easily found for average fidelity, since, unlike the diamond distance, fidelity is not a metric.

Although the diamond distance offers a convenient theoretical description, it is not as practical as average fidelity. But, since average fidelity and diamond distance both estimate the quality of a quantum channel, there exists a relation between the two. Indeed, it can be shown CIT that

$$\| \tilde{\Lambda} - \Lambda \|_\diamond \leq 2\sqrt{d(d+1)}\sqrt{1 - \bar{F}(\tilde{\Lambda})}, \tag{6.31}$$

where d is the dimension of the underlying quantum system.

While performing an experiment, for example estimating the average fidelity, one gathers empirical data. To compare the data with theoretical expectation one can use the Hoeffding's inequality [19]. It states that the probability of the empirical mean and its expectation differing by more than ϵ is exponentially small in n.

Lemma 17 (Hoeffding's inequality)**.** *If $v_1,...,v_n$ are independent random variables, $0 \leq v_i \leq 1$, with empirical mean defined as*

$$R = \frac{v}{n} = \frac{\sum_{i=1}^{n} v_i}{n}, \tag{6.32}$$

then an upper bound on the probability that the mean of random variables deviates from its expected value is given by

$$\Pr[|R - \mathbb{E}[R]| \geq \epsilon] \leq 2e^{-2n\epsilon^2}. \tag{6.33}$$

Lemma 18 (Choi isomorphism)**.** *For a map $\Omega : \mathscr{H}_{S_1} \to \mathscr{H}_{S_2}$ the following identity holds:*

$$\mathrm{Tr}\Big[|\psi\rangle\langle\psi|_{S_2}\ \Omega_{S_1\to S_2}(|\psi\rangle\langle\psi|_{S_1})\Big] = \tag{6.34}$$

$$= |S_1|\,\mathrm{Tr}\Big[|\psi\rangle\langle\psi|_{S_2} \otimes |\psi\rangle\langle\psi|_{S_1'}\ \omega^{\Gamma}_{S_2S_1'}\Big], \tag{6.35}$$

where $\omega^{\Gamma}_{S_2S_1'}$ is a Choi state associated with the map $\Omega_{S_1\to S_2}$ of the form $\omega^{\Gamma}_{S_2S_1'} = \Omega_{S_1\to S_2} \otimes \mathbb{1}_{S_1'}(\Phi)$, with $\Phi = \sum_{i,j} |ii\rangle\langle jj| / |S_1'|$ being the maximally entangled state. Γ denotes partial transposition of ω on the system S_1', and $|S_1|$ ($|S_1'|$) is a size of Hilbert space $\mathscr{H}_{S_1}$ ($\mathscr{H}_{S_1'}$).

6.7.2. THE TEST – DETAILED DESCRIPTION

In this section we provide a mathematical detailed description of our tests. First we consider a general case of the ping-pong test, Test 1. Then we discuss the specific case of the teleportation-based ping-pong test, Test 2.

GENERAL PING-PONG TEST

We describe a general test Test 1 as a CPTP map which we will denote $\mathscr{S}_\kappa$. We first consider all the registers available to the nodes. We call κ the *depth* of the test and assume that κ is a natural number upper-bounded by given k. The time for performing one round $j = 1,...,\kappa$ of the protocol is equal for all the rounds, i.e. $\Delta t = t_{j+1} - t_j = t_{\mathrm{send}} + t_M + \ell$.

We will describe a *round* where node A initiates sending of the state, which implies that j is odd. However, this description is fully symmetric and for even j it is enough to interchange registers of A with registers of B. A sends the qubit $|\psi\rangle\langle\psi|_{A_j^{\mathrm{in}}}$ to node B using channel $\mathscr{E}_{A_j^{\mathrm{in}}\to B_j}$ which takes time upper-bounded by t_{send}. After time $t_{\mathrm{send}} + t_M$ the verifier chooses a gate according to distribution p_{G} and gives its classical description $|g_j\rangle\langle g_j|_{G_j}$ to B. B applies the quantum gate that corresponds to the description and that we describe with a CPTP map $G_{G_jB_j\to G_j}$. This takes time ℓ. After this, at time $t_{\mathrm{send}} + t_M + \ell$

the verifier distributes a challenge bit $|f_j\rangle\langle f_j|_{F_j}$ chosen uniformly at random (0 means 'teleport back', 1 means 'output'). Depending on the challenge, B applies $IN_{F_jB_j^{\mathrm{EPR}}\to B_{j+1}^{\mathrm{in}}}$ for $f_j = 0$ and $OUT_{F_jB_j\to B_j^{\mathrm{out}}}$ for $f_j = 1$.

Definition 27. (Honest round j) Round j of a general test, where provers are honest, can be described as

$$\hat{\Lambda}_{A_j^{\mathrm{in}}F_jG_j\to B_{j+1}^{\mathrm{in}}} = IN_{F_jB_j^{\mathrm{EPR}}\to B_{j+1}^{\mathrm{in}}} \circ G_{G_jB_j\to B_j} \circ M_{B_j\to B_j} \circ \mathscr{E}_{A_j^{\mathrm{in}}\to B_j} \tag{6.36}$$

whenever the challenge bit is 0, or

$$\hat{\Lambda}_{A_j^{\mathrm{in}}F_jG_j\to B_j^{\mathrm{out}}} = OUT_{F_jB_j\to B_j^{\mathrm{out}}} \circ G_{G_jB_j\to B_j} \circ M_{B_j\to B_j} \circ \mathscr{E}_{A_j^{\mathrm{in}}\to B_j} \tag{6.37}$$

whenever the challenge bit is 1.

Note that challenge bits form a string of length κ, $f_1 \dots f_\kappa$, in registers $F_1 \dots F_\kappa$, consisting of $\kappa - 1$ ones and a single zero bit on κ-th position. We denote such a string by $\vec{f}$, i.e. $\vec{f}_\kappa = \underbrace{1\dots10}_{\kappa}$. For simplicity we will use a short notation for multiple registers, e.g. $F_{[1,\kappa]} \equiv F_1 \dots F_\kappa$. Similarly, we will denote by $\vec{g}_\kappa$ a sequence of κ gates chosen by the verifier, each of the gates chosen at the time step defined above. By $G_{[1,\kappa]} \equiv G_1 \cdots G_k$ we denote k registers for the choice of a gate.

Definition 28. The ping-pong testing protocol of depth κ for a state $|\psi\rangle\langle\psi| \in \mathscr{X}$, a sequence of gates $\vec{g}_\kappa \in \mathscr{G}^\kappa$ and a string of challenges $\vec{f}_\kappa = 1\dots10$ is defined as a CPTP map $\mathscr{S}_\kappa$ such that

$$\mathscr{S}_\kappa \equiv \mathscr{S}_{A_1^{\mathrm{in}}F_{[1,\kappa]}G_{[1,\kappa]}\to B_\kappa^{\mathrm{out}}}\left(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,\kappa]}} \otimes |\vec{g}_\kappa\rangle\langle\vec{g}_\kappa|_{G_{[1,\kappa]}}\right) = \tag{6.38}$$

$$= \hat{\Lambda}_{A_j^{\mathrm{in}}F_jG_j\to B_j^{\mathrm{out}}} \circ \bigcirc_{j=1}^{\kappa-1} \hat{\Lambda}_{A_j^{\mathrm{in}}F_jG_j\to B_{j+1}^{\mathrm{in}}}\left(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,\kappa]}} \otimes |\vec{g}_\kappa\rangle\langle\vec{g}_\kappa|_{G_{[1,\kappa]}}\right) \tag{6.39}$$

TELEPORTATION-BASED TEST

We now describe a single round j of the test when the quantum communication is performed with teleportation, $\mathscr{T}_\kappa$ (see Test 2). Let node A initiate the teleportation, i.e. j is odd. A round j starts with placing the state to be teleported $|\psi\rangle\langle\psi|_{A_j^{\mathrm{in}}}$ in an input register of A, A_j^{in}. Nodes generate an EPR pair between each other, $\Phi^+_{A_j^{\mathrm{EPR}}B_j^{\mathrm{EPR}}}$. A, using the generated pair, teleports the state $|\psi\rangle\langle\psi|_{A_j^{\mathrm{in}}}$ to B by performing a Bell state measurement and sending a classical message $m \in M$. This action is described by a CPTP map $\mathscr{B}_{A_j^{\mathrm{in}}A_j^{\mathrm{EPR}}\to M}$. At the same time B applies quantum memory to his half of the EPR pair while waiting for the classical message from A to arrive, which takes time t_M. We describe the action of the memory with a CPTP map $M_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}}$. Upon receiving classical message B now applies a recovery map $\mathscr{R}_{MB_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}}$ to recover the state which A teleported. Then, B

applies a random gate chosen by the verifier from the set of Clifford gates $\mathsf{Cliff}(2)$. This choice is announced by the verifier with a classical register $|c_j\rangle\langle c_j|_{C_j}$. B then applies the gate to his recovered state, which we describe with a CPTP map $C_{C_j B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}}$. This operation takes time ℓ.

Now, at time $t_M + \ell$ the verifier announces a flag in register F_j with the challenge bit, 0: teleport back, 1: output. The choice of the challenge is uniform and random. Depending on the challenge, B applies $IN_{F_j B_j^{\mathrm{EPR}} \to B_{j+1}^{\mathrm{in}}}$ for $f_j = 0$ and $OUT_{F_j B_j^{\mathrm{EPR}} \to B_j^{\mathrm{out}}}$ for $f_j = 1$. The whole round j takes time $\Delta t = t_M + \ell$.

Definition 29. (Round j of the teleportation-based test) We define a j-th round of teleportation as a sequence of following maps

$$\Lambda_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}} F_j C_j \to B_{j+1}^{\mathrm{in}}} = IN_{F_j B_j^{\mathrm{EPR}} \to B_{j+1}^{\mathrm{in}}} \circ C_{C_j B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{R}_{M B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \tag{6.40}$$

$$\circ M_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M} \tag{6.41}$$

whenever the challenge bit is 0, or

$$\Lambda_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}} F_j C_j \to B_j^{\mathrm{out}}} = OUT_{F_j B_j^{\mathrm{EPR}} \to B_j^{\mathrm{out}}} \circ C_{C_j B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{R}_{M B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \tag{6.42}$$

$$\circ M_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M} \tag{6.43}$$

whenever the challenge bit is 1.

Note that, for simplicity, in the main text we denote $M_j^{\mathscr{T}} = \mathscr{R}_{M B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ M_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M}$.

Having defined a single round of a protocol we describe the ping-pong teleportation protocol of depth κ. Such a protocol is simply a κ-round teleportation, where first $\kappa - 1$ maps have form (6.40) and the last map outputs the state and so has the form (6.42).

Definition 30. The teleportation-based ping-pong testing protocol of depth κ for a state $|\psi\rangle\langle\psi| \in \mathsf{X}$, a sequence of gates $\vec{c}_\kappa \in \mathsf{Cliff}^\kappa$ and a string of challenges $\vec{f}_\kappa = 1 \ldots 10$ is defined as a CPTP map $\mathscr{T}_\kappa$ such that

$$\mathscr{T}_\kappa \equiv \mathscr{T}_{A_1^{\mathrm{in}} A_{[1,\kappa]}^{\mathrm{EPR}} B_{[1,\kappa]}^{\mathrm{EPR}} F_{[1,\kappa]} C_{[1,\kappa]} \to B_\kappa^{\mathrm{out}}} = \Lambda_{A_\kappa^{\mathrm{in}} A_\kappa^{\mathrm{EPR}} B_\kappa^{\mathrm{EPR}} F_\kappa C_\kappa \to B_\kappa^{\mathrm{out}}} \circ \bigcirc_{j=1}^{\kappa-1} \Lambda_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}} F_j C_j \to B_{j+1}^{\mathrm{in}}} \tag{6.44}$$

applied to the input state

$$|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}} \otimes \bigotimes_{j=1}^{\kappa} \Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,\kappa]}} \otimes |\vec{c}_\kappa\rangle\langle\vec{c}_\kappa|_{C_{[1,\kappa]}} \tag{6.45}$$

where Λ's are defined as in Definition 29.

MEASUREMENTS

Upon receiving requested state from either A or B, V must check its consistency with the distributed state, as well as confirm applying desired gates. This can be achieved by projecting outcomes onto the state $C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}}$, which is the original state rotated with κ Clifford channels.

Definition 31 (POVM elements for the node V)**.** Measurements performed by V in the teleportation-based ping-pong test can be described by POVM elements,

$$\Pi^{\kappa}_{\checkmark} = C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B^{\text{out}}_\kappa} \tag{6.46}$$

$$\Pi^{\kappa}_{\times} = \mathbb{1} - C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B^{\text{out}}_\kappa} \tag{6.47}$$

for all $\kappa = 1, \ldots, k$. κ denotes here the output register of the κ-th party, depending on the parity either A or B.

RENAMING TELEPORTATION CHANNEL

Now that we have formalized the testing protocol in detail, we will justify using notation for a teleportation channel used in the main text. That is, we will show that a teleportation channel with noisy memory acting on $|\psi\rangle\langle\psi| \otimes \Phi^+$ can be viewed as a channel $M^{\mathcal{T}}_j$ acting only on $|\psi\rangle\langle\psi|$.

Recall Definition 29. In a single round j of the protocol A performs a Bell measurement on the state $|\psi\rangle\langle\psi|_{A^{\text{in}}_j}$ and her part of EPR pair. This action is described described by an operator $\mathscr{B}_{A^{\text{in}}_j A^{\text{EPR}}_j \to M}$, acting on two registers on A's side and producing a classical message $m \in M$ which is then sent to B. The initial state $|\psi\rangle\langle\psi|_{A^{\text{in}}_j} \otimes \Phi^+_{A^{\text{EPR}}_j B^{\text{EPR}}_j}$ becomes

$$\begin{aligned}\mathscr{B}_{A^{\text{in}}_j A^{\text{EPR}}_j \to M}(|\psi\rangle\langle\psi|_{A^{\text{in}}_j} \otimes \Phi^+_{A^{\text{EPR}}_j B^{\text{EPR}}_j}) = \text{Tr}_{A^{\text{in}}_j A^{\text{EPR}}_j}\Big[\sum_{m\in M} p_m \Psi'_{A^{\text{in}}_j A^{\text{EPR}}_j, m} \otimes (U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B^{\text{EPR}}_j} \\ \otimes |m\rangle\langle m|_M \Big] = \\ = \sum_{m\in M} p_m (U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B^{\text{EPR}}_1} \otimes |m\rangle\langle m|_M\end{aligned} \tag{6.48}$$

where $\Psi'_{A^{\text{in}}_j A^{\text{EPR}}_j, m}$ is one of four Bell states resulting from the Bell measurement, $p_m \geq 0$, $\sum_m p_m = 1$ is a probability of an outcome m occurring. $(U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B^{\text{EPR}}_j}$ is a state on B's register after the Bell measurement. Note that this is simply a unitary applied to the initial state. $|m\rangle\langle m|$ is a classical message register, which A sends to B in order for him to correct the state. Next, B applies a memory $M_{B^{\text{EPR}}_j \to B^{\text{EPR}}_j}$ to his share of the state:

$$\begin{aligned}M_{B^{\text{EPR}}_j \to B^{\text{EPR}}_j} \circ \mathscr{B}_{A^{\text{in}}_j A^{\text{EPR}}_j \to M}(|\psi\rangle\langle\psi|_{A^{\text{in}}_j} \otimes \Phi^+_{A^{\text{EPR}}_j B^{\text{EPR}}_j}) = M_{B^{\text{EPR}}_j \to B^{\text{EPR}}_j} \sum_{m\in M} p_m (U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B^{\text{EPR}}_j} \\ \otimes |m\rangle\langle m|_M \\ = \sum_{m\in M} p_m M_{B^{\text{EPR}}_j \to B^{\text{EPR}}_j}(U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B^{\text{EPR}}_j} \\ \otimes |m\rangle\langle m|_M\end{aligned} \tag{6.49}$$

Upon receiving a classical message m B undoes the unitary operations to recover the teleported state. This operation is described by a map $\mathscr{R}_{MB^{\text{EPR}}_j \to B^{\text{EPR}}_j}(\cdot) = \text{Tr}_M[\sum_m U_m(\cdot)U_m^\dagger \otimes$

$|m\rangle\langle m|_M]$,

$$\begin{aligned}
&\mathscr{R}_{MB_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} \circ M_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}}\to M}(|\psi\rangle\langle\psi|_{A_j^{\mathrm{in}}} \otimes \Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}}) \\
&= \mathrm{Tr}_M \left[\sum_{m\in M} p_m U_m^\dagger M_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}}(U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B_j^{\mathrm{EPR}}} U_m \otimes |m\rangle\langle m|_M \right] \\
&= \sum_{m\in M} p_m U_m^\dagger M_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}}(U_m |\psi\rangle\langle\psi| U_m^\dagger)_{B_j^{\mathrm{EPR}}} U_m \\
&= \sum_{m\in M} p_m \mathscr{U}_m^\dagger \circ M_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} \circ \mathscr{U}_m(|\psi\rangle\langle\psi|) =: M_j^{\mathscr{T}}(|\psi\rangle\langle\psi|)
\end{aligned} \tag{6.50}$$

Then, the test of depth κ can be described as in the main text

$$\begin{aligned}
\mathscr{T}^\kappa &= \mathscr{T}_{A_1^{\mathrm{in}} A_{[1,\kappa]}^{\mathrm{EPR}} B_{[1,\kappa]}^{\mathrm{EPR}} F_{[1,\kappa]} C_{[1,\kappa]}\to B_\kappa^{\mathrm{out}}} \left(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}} \otimes \bigotimes_{j=1}^{\kappa} \Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,k]}} \otimes |\vec{c}_\kappa\rangle\langle\vec{c}_\kappa|_{C_{[1,k]}} \right) \\
&\equiv \bigcirc_{j=1}^{\kappa} \Lambda_j = \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathscr{T}}\left(|\psi\rangle\langle\psi|\right)
\end{aligned} \tag{6.51}$$

6

6.7.3. TELEPORTATION AND QUANTUM MEMORY

ABSORBING TELEPORTATION NOISE INTO THE MEMORY

As it is often done in the estimation literature for quantum computing, see e.g. [8–10] , we will model teleportation as a perfect operation followed (or preceded) by noise. This will allow us to consider teleportation as a perfect operation i.e. with perfect Bell measurement and recovery operation as well as perfect EPR pair, and absorb all the associated noise into the quantum memory.

Noisy operations. Assume a Bell state measurement is followed by a local noise, $\mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}}\to M} \equiv N^{\mathscr{B}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}}\to M}$. Assume further that the recovery operation is also noisy, but in this case the map is preceded by the noise, $\mathscr{R}_{MB_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} \equiv \mathscr{R}_{MB_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} \circ N^{\mathscr{R}}$. Looking at Definition 29 it is now clear that one can redefine $M'_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} = N^{\mathscr{R}} \circ M_{B_j^{\mathrm{EPR}}\to B_j^{\mathrm{EPR}}} \circ N^{\mathscr{B}}$ and use M' as a new memory channel.

Noisy EPR pairs. The situation is similar for a noisy EPR pair. Assume a EPR pair is affected by local noise, i.e. teleportation occurs on a state $N_{A_j^{\mathrm{EPR}}} \otimes N_{B_j^{\mathrm{EPR}}}\left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}}\right)$. Here the maps N are mixed-unitary channels, i.e. have the form $N(\cdot) = \sum_l p_l U_l(\cdot) U_l^\dagger$, with p_l being a probability and U_l a unitary. Note that this is not the most general type of noise, however the most common ones (e.g. depolarizing, dephasing) can be modeled this way. Moreover, note that for an EPR pair it holds that

$$U_{A_j^{\mathrm{EPR}}} \otimes U_{B_j^{\mathrm{EPR}}}\left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}}\right) = \mathrm{id}_{A_j^{\mathrm{EPR}}} \otimes U_{B_j^{\mathrm{EPR}}} U^T_{A_j^{\mathrm{EPR}}}\left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}}\right). \tag{6.52}$$

Therefore, using an explicit form of maps N and the above statement, we can write,

$$N_{A_j^{\mathrm{EPR}}} \otimes N_{B_j^{\mathrm{EPR}}} \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) = \sum_{l,l'} p_{l,l'} U_{A_j^{\mathrm{EPR}}} \otimes U_{B_j^{\mathrm{EPR}}} \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.53}$$

$$= \sum_{l,l'} p_{l,l'} \mathrm{id}_{A_j^{\mathrm{EPR}}} \otimes U_{B_j^{\mathrm{EPR}}} U^T_{A_j^{\mathrm{EPR}}} \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.54}$$

$$=: \mathrm{id}_{A_j^{\mathrm{EPR}}} \otimes N'_{B_j^{\mathrm{EPR}}} \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.55}$$

In particular, this means that noise acting on the EPR pair, which has the mixed-unitary form, can be absorbed into the memory map,

$$M'_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M} \circ \left(N_{A_j^{\mathrm{EPR}}} \otimes N_{B_j^{\mathrm{EPR}}} \right) \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.56}$$

$$= M'_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M} \circ \left(\mathrm{id}_{A_j^{\mathrm{EPR}}} \otimes N'_{B_j^{\mathrm{EPR}}} \right) \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.57}$$

$$= M'_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ N'_{B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M} \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.58}$$

$$\equiv M''_{B_j^{\mathrm{EPR}} \to B_j^{\mathrm{EPR}}} \circ \mathscr{B}_{A_j^{\mathrm{in}} A_j^{\mathrm{EPR}} \to M} \left(\Phi^+_{A_j^{\mathrm{EPR}} B_j^{\mathrm{EPR}}} \right) \tag{6.59}$$

6.7.4. 2-DESIGNS

In this appendix we show that for the ping-pong test, the average of the probability $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ over the six Pauli states is equal to its average over the whole state space according to the Haar measure. To do so, we use the fact that the uniform distribution over set X is a 2-design [26] and $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ contains a polynomial of degree 2 in $|\psi\rangle$. Next, we prove a similar statement when averaging over the Clifford group.

PAULI STATES

Lemma 19. *Averaging the probability of success for a single execution of Test 2, $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$, over Pauli states is equal to averaging over all qubit states according to the Haar measure,*

$$\frac{1}{|\mathsf{X}|} \sum_{\psi \in \mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi \; p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}. \tag{6.60}$$

Proof of Lemma 15. We can write the left-hand side explicitly as,

$$\frac{1}{|\mathsf{X}|} \sum_{\psi \in \mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \frac{1}{|\mathsf{X}|} \sum_{\psi} \mathrm{Tr}\left[\mathscr{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}}) \cdot \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}} \right] \tag{6.61}$$

where we explicitly write A and B's input and output registers. Let $X, Y \in \mathscr{L}(\mathscr{H})$ be linear operators over the Hilbert space. The inner product $\langle X \rangle Y := \mathrm{Tr}\left[X^\dagger Y\right]$ is invariant $\forall U : \mathscr{L}(\mathscr{H}) \to \mathscr{L}(\mathscr{H})$, i.e. $\langle U(X) \rangle U(Y) = \mathrm{Tr}\left[(U(X))^\dagger \cdot U(Y)\right] = \mathrm{Tr}\left[X^\dagger \cdot Y\right] = \langle X \rangle Y$. Note

that $\bigcirc_{j=1}^{\kappa} C_j$ is a unitary channel and therefore, we can write,

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \frac{1}{|\mathsf{X}|}\sum_{\psi}\mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ\mathscr{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ\bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}}\right] \tag{6.62}$$

$$= \frac{1}{|\mathsf{X}|}\sum_{\psi}\mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ\mathscr{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot|\psi\rangle\langle\psi|_{B_\kappa^{\mathrm{out}}}\right] \tag{6.63}$$

Now, using Choi-Jamiolkowski theorem, see Lemma 18, we can write

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \frac{1}{|\mathsf{X}|}\sum_{\psi}|A_1^{\mathrm{in}'}|\,\mathrm{Tr}\left[|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}}\otimes|\psi\rangle\langle\psi|_{B_\kappa^{\mathrm{out}}}\,\omega^{\Gamma}_{A_1^{\mathrm{in}'}B_\kappa^{\mathrm{out}}}\right] \tag{6.64}$$

$\omega^{\Gamma}_{A_1^{\mathrm{in}'}B_\kappa^{\mathrm{out}}}$ is a Choi-Jamiolkowski state associated with the map $\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ\tilde{\mathscr{T}}_\kappa$. It is now clear that averaging is taken over a polynomial of degree 2 under the trace and we can use properties of a 2-design. Therefore,

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi\,|A_1^{\mathrm{in}'}|\,\mathrm{Tr}\left[|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}}\otimes|\psi\rangle\langle\psi|_{B_\kappa^{\mathrm{out}}}\,\omega^{\Gamma}_{A_1^{\mathrm{in}'}B_\kappa^{\mathrm{out}}}\right] \tag{6.65}$$

$$= \int \mathrm{d}\psi\,\mathrm{Tr}\left[\mathscr{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot\bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}}\right] \tag{6.66}$$

$$= \int \mathrm{d}\psi\; p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \tag{6.67}$$

where we used Choi-Jamiolkowski isomorphism and properties of the trace again. We define $\bar{F}_{\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi\; p_{\checkmark|\psi,\vec{c}_\kappa,kt}$ as the average fidelity. □

CLIFFORD GATES

Now we will prove that averaging $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ over the Clifford set reproduces averaging over the whole unitary set taken according to the Haar measure.

Lemma 20. *Averaging the probability of success for a single execution of Test 2, $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$, over Pauli states and over Clifford gates is equal to averaging over all qubit states and all 2-qubit unitary gates according to the Haar measure,*

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi\int \mathrm{d}C_1\cdots\int \mathrm{d}C_\kappa\; p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}. \tag{6.68}$$

Proof. Just like in the previous lemma, let us first use cyclicity of the trace,

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^\kappa} \sum_{\vec{C}_\kappa} \mathrm{Tr}\Big[\Big(\bigcirc_{j=1}^{\kappa} C_j\Big)^{-1} \circ \mathscr{T}_\kappa(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\Big] \tag{6.69}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^\kappa} \sum_{\vec{C}_\kappa} \mathrm{Tr}\Big[C_1^\dagger \circ \cdots \circ C_\kappa^\dagger \circ C_\kappa \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathscr{T}} \circ \cdots \circ C_1 \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\Big] \tag{6.70}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \sum_{C_1,\ldots,C_{\kappa-1}\in\mathsf{Cliff}} \mathrm{Tr}\Big[C_1^\dagger \circ \cdots \circ C_{\kappa-1}^\dagger \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathscr{T}} \circ \cdots \circ C_1 \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\Big] \tag{6.71}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \sum_{C_1,\ldots,C_{\kappa-2}\in\mathsf{Cliff}} \mathrm{Tr}\Big[C_1^\dagger \circ \cdots \circ C_{\kappa-2}^\dagger \Big(\sum_{C_{\kappa-1}\in\mathsf{Cliff}} C_{\kappa-1}^\dagger \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1}\Big) \circ M_{\kappa-1}^{\mathscr{T}} \circ \cdots \tag{6.72}$$

$$\circ C_1 \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\Big], \tag{6.73}$$

where in the last step we pulled the summation over $\kappa-1$ under the trace. Note that $\big(\sum_{C_{\kappa-1}} C_{\kappa-1}^\dagger \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1}\big)$ is an unnormalized twirl over Cliff and therefore it commutes with all Clifford gates $C \in \mathsf{Cliff}$. By repeating pulling the summation under the trace, we can write,

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \sum_{C_1,\ldots,C_{\kappa-3}\in\mathsf{Cliff}} \mathrm{Tr}\Big[C_1^\dagger \circ \cdots \circ C_{\kappa-3}^\dagger \Big(\sum_{C_{\kappa-2}\in\mathsf{Cliff}} C_{\kappa-2}^\dagger \circ M_{\kappa-1}^{\mathscr{T}} \circ C_{\kappa-2}\Big) \tag{6.74}$$

$$\circ \Big(\sum_{C_{\kappa-1}\in\mathsf{Cliff}} C_{\kappa-1}^\dagger \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1}\Big) \circ M_{\kappa-2}^{\mathscr{T}} \circ \cdots \circ C_1 \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\Big] \tag{6.75}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \mathrm{Tr}\Big[\bigcirc_{j=1}^{\kappa-1} \Big(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\Big) \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\Big]. \tag{6.76}$$

Now we are left with a rather awkward map $M_1^{\mathscr{T}}$ which is not twirled. However, since the Haar measure is invariant under unitary transformations, for all $E \in \mathsf{Cliff}$ it holds that

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \mathrm{Tr}\Big[\bigcirc_{j=1}^{\kappa-1} \Big(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\Big) \circ M_1^{\mathscr{T}} \circ E(|\psi\rangle\langle\psi|) \cdot E(|\psi\rangle\langle\psi|)\Big] \tag{6.77}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa}} \sum_{E\in\mathsf{Cliff}} \mathrm{Tr}\Big[\bigcirc_{j=1}^{\kappa-1} \Big(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\Big) \circ M_1^{\mathscr{T}} \circ E(|\psi\rangle\langle\psi|) \cdot E(|\psi\rangle\langle\psi|)\Big] \tag{6.78}$$

where in the last line we used the fact that the value of the expression does not depend on E. Now, using cyclicity of the trace and commutativity properties of E, we get

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa}} \mathrm{Tr}\Big[\bigcirc_{j=1}^{\kappa-1} \Big(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\Big) \circ \Big(\sum_{E\in\mathsf{Cliff}} E^\dagger \circ M_1^{\mathscr{T}} \circ E\Big)(|\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi|)\Big]. \tag{6.79}$$

Now we can change discrete averaging to the continuous one by definition of the unitary 2-design, see Definition 25 and [27]. We have

$$\text{LHS} = \int \mathrm{d}\psi \ \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1}\left(\int \mathrm{d}C_j \ C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\right) \circ \left(\int \mathrm{d}E \ E^\dagger \circ M_1^{\mathscr{T}} \circ E\right)(|\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi|)\right]. \tag{6.80}$$

To get back to the expression for $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$, we can invert the procedure we just applied, i.e.

$$\begin{aligned}
\text{LHS} &= \int \mathrm{d}\psi \int \mathrm{d}E \ \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1}\left(\int \mathrm{d}C_j \ C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\right) \circ \left(E^\dagger \circ M_1^{\mathscr{T}} \circ E\right)(|\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi|)\right] \\
&= \int \mathrm{d}\psi \int \mathrm{d}E \ \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1}\left(\int \mathrm{d}C_j \ C_j^\dagger \circ M_{j+1}^{\mathscr{T}} \circ C_j\right) \circ M_1^{\mathscr{T}} \circ E(|\psi\rangle\langle\psi|) \cdot E(|\psi\rangle\langle\psi|)\right] \\
&= \int \mathrm{d}\psi \int \mathrm{d}E \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_{\kappa-1} \ \mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-1}^\dagger \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathscr{T}} \circ \cdots \circ C_1 \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \\
&= \int \mathrm{d}\psi \int \mathrm{d}E \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_{\kappa-1} \ \mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-1}^\dagger \circ E^\dagger \circ E \circ M_\kappa^{\mathscr{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathscr{T}} \circ \cdots \circ C_1 \circ \right. \\
&\qquad \left. \circ M_1^{\mathscr{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right]
\end{aligned} \tag{6.81}$$

If now we put $E = C_\kappa$ we obtain the desired result. We define $\bar{\bar{F}}_\kappa = \int \mathrm{d}\psi \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_\kappa \ p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ as double-averaged fidelity. □

6.7.5. COMPLETENESS AND SOUNDNESS

EXACT COMPLETENESS AND SOUNDNESS

To keep this section more compact, we use notation from the main text. That is we express Test 2 as $\mathscr{T}_\kappa = \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathscr{T}}$, see Eq. (6.6).

Proof of Theorem 15. First, we prove that Test 2 is exactly correct when the winning threshold $P_\checkmark = 1$. That is, for honest A and B and for any $1 \leq \kappa \leq k$ after κ rounds the state that the verifier obtains at output κ is $\bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)$. To prove this, we need to make sure that for all the rounds preceding κ the state at outputs $j = 1, \ldots, \kappa$ are correct. The above can be proven by induction. For $\kappa = 1$ the verifier measures $C_1(|\psi\rangle\langle\psi|)$. On the other hand, $C_1 \circ M_1^{\mathscr{T}} = C_1(|\psi\rangle\langle\psi|)$, since the setup is perfect. Repeating this step inductively we get for all κ,

$$\bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathscr{T}}(|\psi\rangle\langle\psi|) = \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|) \tag{6.82}$$

Hence, $P_\checkmark = 1$. □

Before proving Theorem 16 we formally prove a known fact related to no-cloning theorem [17].

Lemma 21. *Let $V_{A\to A'B}$ be an arbitrary isometry, and let for any qubit state $|\psi\rangle_A$, $|\Psi\rangle_{A'B} := V|\psi\rangle_A$. If for all $|\psi\rangle$, $\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{A'B}) = |\psi\rangle\langle\psi|_{A'}$, then $|\Psi\rangle_{A'B} = |\psi\rangle_{A'} \otimes |\mathrm{junk}\rangle_B$, where $|\mathrm{junk}\rangle$ is a pure state independent of $|\psi\rangle$.*

Proof. If the above is true for all $|\psi\rangle$ it is in particular true for $|0\rangle$, namely, $V|0\rangle = |0\rangle\otimes|\sigma_0\rangle$. Similarly $V|1\rangle = |1\rangle\otimes|\sigma_1\rangle$. When now computing the action of V on the state $|+\rangle$, we have $V|+\rangle = \frac{|0\rangle\otimes|\sigma_0\rangle+|1\rangle\otimes|\sigma_1\rangle}{\sqrt{2}}$. But since $\mathrm{Tr}_B(V|+\rangle\langle+|V^\dagger) = |+\rangle\langle+|$, we must have $|\sigma_0\rangle = |\sigma_1\rangle =: |\mathrm{junk}\rangle$ □

Corollary 3. Let $\Omega_{A\to A'B}$ be an arbitrary CPTP map, and let for any qubit state $|\psi\rangle\langle\psi|_A$, $\rho_{A'B} := \Omega(|\psi\rangle\langle\psi|_A)$. If for all $|\psi\rangle$, $\mathrm{Tr}_B(\rho_{A'B}) = |\psi\rangle\langle\psi|_{A'}$, then $\rho_{A'B} = |\psi\rangle\langle\psi|_{A'}\otimes \mathrm{junk}_B$, where junk is a state independent of $|\psi\rangle\langle\psi|$.

Proof. By Stinespring dilation $\exists V_{A\to A'BE}\ \Omega(\cdot) = \mathrm{Tr}_E(V(\cdot)V^\dagger)$. Since $\mathrm{Tr}_B(\rho_{A'B}) = |\psi\rangle\langle\psi|_{A'} = \mathrm{tr}_{BE}(V|\psi\rangle\langle\psi|V^\dagger)$ we must have by the above lemma that

$$V|\psi\rangle\langle\psi|V^\dagger = |\psi\rangle\langle\psi|_{A'}\otimes|\mathrm{junk}'\rangle\langle\mathrm{junk}'|_{BE}, \tag{6.83}$$

and therefore $\rho_{A'B} = |\psi\rangle\langle\psi|_{A'}\otimes\mathrm{Tr}_E(|\mathrm{junk}'\rangle\langle\mathrm{junk}'|_{BE}) = |\psi\rangle\langle\psi|_{A'}\otimes\mathrm{junk}_B$. □

Proof of Theorem 16. Now we prove that Test 2 is exactly sound. That is, if the average probability of success $P_\checkmark = 1$, then nodes A and B have the ability to correctly execute Test 2. The intuition behind our proof is that challenges given by the verifier impose a certain structure on the provers strategy. We first show that if the nodes win the test with probability 1, then their strategy must produce the correct state at each time step κ. Then, we argue that this implies that the nodes must have passed the state around, and therefore use a quantum channel between them exactly κ times.

Lemma 22. *Let $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ be an arbitrary strategy of the provers, which can depend on the information available throughout the protocol, i.e. depth κ and Clifford string $\vec{c}_\kappa$. If the average probability of success in Test 2 is $P_\checkmark = 1$, then for all depths $\kappa = 1,\dots,k$, all Clifford strings $\vec{c}_\kappa$ and all input states $\psi\in\mathsf{X}$, $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ outputs the correct state.*

Proof. This statement is essentially the inverse of the exact completeness statement. Let us explicitly write the average probability of success,

$$P_\checkmark = \frac{1}{k}\sum_\kappa \frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa\in\mathsf{Cliff}^\kappa}\mathrm{Tr}\left[\mathcal{Q}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right] = 1. \tag{6.84}$$

This implies that for all states, gates and depths the trace must be equal to 1,

$$\forall\psi\in\mathsf{X},\ \forall\vec{c}_\kappa\in\mathsf{Cliff}^\kappa,\ \forall\kappa = 1,\dots,k:\quad \mathrm{Tr}\left[\mathcal{Q}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right] = 1. \tag{6.85}$$

Therefore,

$$\forall\psi\in\mathsf{X},\ \forall\vec{c}_\kappa\in\mathsf{Cliff}^\kappa,\ \forall\kappa = 1,\dots,k:\quad \mathcal{Q}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right) = C_\kappa\circ\cdots\circ C_1(|\psi\rangle\langle\psi|) \tag{6.86}$$

and the state at every κ must be exactly the one requested by the verifier. □

Lemma 23. *If the average probability of success in Test 2 is $P_\checkmark = 1$, then for all depths $\kappa = 1,\dots,k$, all Clifford strings $\vec{c}_\kappa$ and all input states $\psi\in\mathsf{X}$, $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ uses an exact sending channel κ times and apply an operation equivalent to the one described by $\vec{c}_\kappa$.*

Proof. In our test at every time step κ the provers must produce some state. Since at every time step a state has to be defined, $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ can be described by

$$\mathcal{Q}_{\vec{c}_\kappa,\kappa} = \bigcirc_{j=1}^{\kappa} \mathcal{E}_{\vec{c}_j,j} \tag{6.87}$$

Let $\hat{\Gamma}_{A_{\kappa-1}}$ and $\hat{\Gamma}_{B_{\kappa-1},B_\kappa}$ denote CPTP maps which act on registers of A and B respectively, and output qubit states, and let $\Gamma_{A_{\kappa-1}}$ and $\Gamma_{B_{\kappa-1},B_\kappa}$ be $\mathrm{Tr}_{B_{\kappa-1},B_\kappa}[\hat{\Gamma}_{A_{\kappa-1}}(\cdot)]$ and $\mathrm{Tr}_{A_{\kappa-1}}[\hat{\Gamma}_{B_{\kappa-1},B_\kappa}(\cdot)]$ respectively. The above fact together with Lemma 19 and 23 implies that at time steps κ and $\kappa-1$

$$\int \mathrm{d}\psi \,\mathrm{Tr}\left[\mathcal{E}_{\vec{c}_\kappa,\kappa} \circ \mathcal{Q}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right) \cdot \Pi_{\checkmark}^{\kappa}\right] = 1 \Rightarrow \sup_{\Gamma_{B_{\kappa-1},B_\kappa}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_\kappa-1,B_\kappa}\left(\mathcal{E}_{\vec{c}_\kappa,\kappa}\left(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\right) \cdot \Pi_{\checkmark}^{\kappa}\right] = 1 \tag{6.88}$$

$$\int \mathrm{d}\psi \,\mathrm{Tr}\left[\mathcal{Q}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right) \cdot \Pi_{\checkmark}^{\kappa-1}\right] = 1 \Rightarrow \sup_{\Gamma_{A_{\kappa-1}}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{A_{\kappa-1}}\left(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right) \cdot \Pi_{\checkmark}^{\kappa-1}\right] = 1 \tag{6.89}$$

Moreover, we've put $\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1} := \mathcal{Q}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)$ to denote a joint state of A and B at time step $\kappa-1$. Observe that for all κ, $\Pi_{\checkmark}^{\kappa} = C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)$ projects onto a pure state. Therefore, for all κ, the states at output registers $\kappa-1$ for A, and κ for B, must be pure,

$$\Gamma_{B_{\kappa-1},B_\kappa}\left(\mathcal{E}_{\vec{c}_\kappa,\kappa}\left(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\right) = C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B_\kappa} \tag{6.90}$$

$$\Gamma_{A_{\kappa-1}}\left(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right) = C_{\kappa-1} \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{A_{\kappa-1}} \tag{6.91}$$

Let $\sigma^{\psi} = (\hat{\Gamma}_{A_{\kappa-1}} \otimes \mathbb{1})(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1})$ be the joint state of A and B at time step $\kappa-1$, and after applying $\hat{\Gamma}_{A_{\kappa-1}}$ on A. Using Eq. (6.91) we have that,

$$\mathrm{Tr}_{B_{\kappa-1}}(\sigma^{\psi}) = C_{\kappa-1} \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{A_{\kappa-1}}, \tag{6.92}$$

which is a pure state on A, and therefore any extension of this state has tensor product form across A and B, in particular,

$$\sigma^{\psi} = C_{\kappa-1} \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{A_{\kappa-1}} \otimes \sigma_{B_{\kappa-1}}, \tag{6.93}$$

where $\sigma_{B_{\kappa-1}}$ is a state on B independent of ψ by Corr. 3. Therefore the (maximum) average fidelity of the state on B's side is,

$$\sup_{\Gamma_{B_{\kappa-1}}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_{\kappa-1}}\left(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right) \cdot \Pi_{\checkmark}^{\kappa-1}\right] = \sup_{\Gamma_{B_{\kappa-1}}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\sigma_{B_{\kappa-1}} \cdot \Pi_{\checkmark}^{\kappa-1}\right] = \sup_{\Gamma_{B_{\kappa-1}}} \mathrm{Tr}\left[\sigma_{B_{\kappa-1}} \cdot \frac{\mathbb{1}}{2}\right] = \frac{1}{2} \tag{6.94}$$

This, together with Eq. (6.88), implies that $\mathcal{E}_{\vec{c}_\kappa,\kappa}$ is an exact sending channel at time step κ. Since the statement holds for all κ, the provers necessarily use the exact sending channel k times.

□

□

COMPLETENESS AND SOUNDNESS

Proof of Theorem 17. Completeness. As stated in the main text, we assume that the quality of operations is quantified by average fidelity and that at every round j the quality of operations is the same, i.e. for all j, $\bar{\mu} = \int \mathrm{d}\psi \,\mathrm{Tr}\Big[C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot C_j(|\psi\rangle\langle\psi|)\Big]$. In the following we bound the average probability of success $P_{\checkmark}$ in terms of $\bar{\mu}$. Let us write $P_{\checkmark}$ explicitly,

$$P_{\checkmark} = \frac{1}{k}\sum_{\kappa}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^{\kappa}}\sum_{\vec{c}_{\kappa}}\mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|)\cdot\Pi_{\kappa}^{\checkmark}\right] \tag{6.95}$$

From Lemma 20 we have that

$$P_{\checkmark} = \frac{1}{k}\sum_{\kappa}\int \mathrm{d}\psi \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_{\kappa}\,\mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1} \circ \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|)\cdot|\psi\rangle\langle\psi|\right], \tag{6.96}$$

$$= \frac{1}{k}\sum_{\kappa}\int \mathrm{d}\psi\,\mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa}\left(\int \mathrm{d}C_j\; C_j^{\dagger}\circ M_j^{\mathcal{T}}\circ C_j\right)(|\psi\rangle\langle\psi|)\cdot|\psi\rangle\langle\psi|\right]. \tag{6.97}$$

Observe that $(M_j^{\mathcal{T}})_{twirl} = \int \mathrm{d}C_j\; C_j^{\dagger}\circ M_j^{\mathcal{T}}\circ C_j$ is a twirl of the operator $M_j^{\mathcal{T}}$ [28]. Furthermore, twirling any map is equivalent to the action of a depolarizing channel, i.e. $(M_j^{\mathcal{T}})_{twirl}(\rho) = \mathscr{D}_j(\rho) = p\rho + (1-p)\mathbb{1}/2$, for some parameter p and any state ρ. Using properties of the depolarizing channel we can write,

$$P_{\checkmark} = \frac{1}{k}\sum_{\kappa}\int \mathrm{d}\psi\,\mathrm{Tr}\Big[\bigcirc_{j=1}^{\kappa}(M_j^{\mathcal{T}})_{twirl}(|\psi\rangle\langle\psi|)\cdot|\psi\rangle\langle\psi|\Big] \tag{6.98}$$

$$= \frac{1}{k}\sum_{\kappa}\int \mathrm{d}\psi\,\mathrm{Tr}\Big[\bigcirc_{j=1}^{\kappa}\mathscr{D}_j(|\psi\rangle\langle\psi|)\cdot|\psi\rangle\langle\psi|\Big] \tag{6.99}$$

$$= \frac{1}{k}\sum_{\kappa}\prod_{j=1}^{\kappa}\bar{F}(\mathscr{D}_j) \tag{6.100}$$

$$= \frac{1}{k}\sum_{\kappa}\prod_{j=1}^{\kappa}\bar{F}\left((M_j^{\mathcal{T}})_{twirl}\right) \tag{6.101}$$

$$\tag{6.102}$$

Additionally, the average fidelity of a twirled map is equal to the average fidelity of the same map without a twirl [28], therefore, $P_{\checkmark} = \frac{1}{k}\sum_{\kappa}\prod_{j=1}^{\kappa}\bar{F}\left(M_j^{\mathcal{T}}\right)$. By assumption, $\forall\, j\ \bar{F}\left(M_j^{\mathcal{T}}\right) = \bar{\mu}$, and

$$P_{\checkmark} = \frac{1}{k}\sum_{\kappa}\bar{\mu}^{\kappa} = \frac{1}{k}\frac{\bar{\mu}(\bar{\mu}^k - 1)}{k(\bar{\mu}-1)} = h_k(\bar{\mu}). \tag{6.103}$$

If we demand that $P_{\checkmark} \geq t$ then $\bar{\mu} \geq h_k^{-1}(t)$. □

Proof of Theorem 18. Soundness. In the case when the nodes A and B are honest, the soundness statement is the converse of the completeness, see the proof above. Here we

prove soundness of Test 2 in the case when the nodes are dishonest (m-cheating). Just like before, we will assume that output for a fixed κ happens at node B.

The idea behind this proof is that we bound the average probability of success of the provers when they use a quantum channel between them, and when they do not. More specifically, let $\rho_{A_{\kappa-1}^{\text{out}}}$ be a state available at A's output at time step $\kappa-1$ and $\rho_{B_\kappa}^{\text{out}}$ be a state available at B's at time step κ. We show that whenever the provers use the channel, the average fidelity between these two states is bounded by 1. However, whenever they do not use the channel, the average fidelity between these two states is at most as large as the average fidelity between the states at time step $\kappa-1$, i.e. $\rho_{A_{\kappa-1}^{\text{out}}}$ and $\rho_{B_{\kappa-1}^{\text{out}}}$. This average fidelity is intrinsically bounded by the approximate cloning theorem [18], and here takes value $\frac{5}{6}$. If the provers are m-cheating, they use the channel between at least m times. We prove that, as a consequence, their overall average probability of winning $P_{\checkmark}$ is upper-bounded by $\frac{1}{k}(m+\frac{5}{6}(k-m))$.

When the provers are m-cheating they adapt an arbitrary strategy $\mathcal{Q}^m_{\vec{c}_\kappa,\kappa}$ which depends on the maximum number of channel uses m between the nodes. It can also depend on all the information available throughout the protocol, i.e. the challenges and gates distributed by the verifier. We assume that the executions of the test are IID (independent and identically distributed) and the probability of winning a single execution $i=1,\ldots,n$ is expressed as

$$\forall\ \vec{c}_\kappa,\kappa,\psi \quad p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \mathrm{Tr}\left[\mathcal{Q}^m_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_{\checkmark}\right]. \tag{6.104}$$

The configuration of channel uses, i.e. at which time step the provers use the channel between them, does not need to be fixed. At each execution, the provers can choose a particular strategy $\mathcal{Q}^{m,\nu}$ which describes a configuration ν of channel uses between the nodes. We assume that the provers are *non-adaptive* and throughout an execution i their strategy does not change. Therefore, the fact whether the provers choose to send the state or not, is independent of the information available throughout the protocol. I.e. ν is independent of κ and $\vec{c}_\kappa$, and we have $q_\nu \geq 0$, $\sum_\nu q_\nu = 1$, such that

$$\mathcal{Q}^m_{\vec{c}_\kappa,\kappa} = \sum_\nu q_\nu \mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}. \tag{6.105}$$

Note that there are $\binom{k}{m}$ such strategies. Furthermore, let us define

$$p_{\checkmark|\nu,\psi,\vec{c}_\kappa,\kappa} := \mathrm{Tr}\left[\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_{\checkmark}\right]. \tag{6.106}$$

Let us rewrite the average probability of success, Eq. (6.7),

$$P_{\checkmark} = \frac{1}{2}\left(\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} + \frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\right). \tag{6.107}$$

Now, we will move the summation in the second component of the sum over κ – instead of going through $(1,2,\ldots,k-1,k)$ we will set it to go $(k,1,2,\ldots,k-1)$,

$$P_{\checkmark} = \frac{1}{2}\left(\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} + \frac{1}{k}\sum_{\kappa=k}^{k-1}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\right). \tag{6.108}$$

Let us define $p_{✓|\psi,\vec{c}_0,0} := 1$ for round $\kappa = 0$, which one can interpret as simply giving the state to node A and immediately requesting it back. Now since for $\kappa = k$ it holds that $p_{✓|\psi,\vec{c}_k,k} \leq 1$, we have $p_{✓|\psi,\vec{c}_k,k} \leq p_{✓|\psi,\vec{c}_0,0}$. Therefore,

$$P_✓ \leq \frac{1}{2}\left(\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{✓|\psi,\vec{c}_\kappa,\kappa} + \frac{1}{k}\sum_{\kappa=0}^{k-1}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{✓|\psi,\vec{c}_\kappa,\kappa}\right). \tag{6.109}$$

Now we write the expression as a single summation,

$$P_✓ \leq \frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}\frac{p_{✓|\psi,\vec{c}_\kappa,\kappa} + p_{✓|\psi,\vec{c}_{\kappa-1},\kappa-1}}{2} \tag{6.110}$$

$$= \sum_{\nu} q_\nu \frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}\frac{1}{2}\left(p_{✓|\nu,\psi,\vec{c}_\kappa,\kappa} + p_{✓|\nu,\psi,\vec{c}_{\kappa-1},\kappa-1}\right) \tag{6.111}$$

$$= \sum_{\nu} q_\nu \frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_\kappa,\kappa} + \bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right) \tag{6.112}$$

In line (6.111) we used the linearity property of the trace, and in line (6.112) we used 2-design properties of the set X (see argument in Section 19) together with the fact that $\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}$ does not depend on the state.

In our test at every time step κ the provers must produce some state. Since at every time step a state has to be defined, $\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}$ can be described by

$$\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa} = \bigcirc_{j=1}^{\kappa}\mathscr{E}^{m,\nu}_{\vec{c}_j,j} \tag{6.113}$$

Now our goal is to bound the probability of winning $P_✓$ if $\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}$ has exactly m sending channels $\mathscr{E}$, as defined in Definition 20. We will consider two cases: when the channel $\mathscr{E}$ is a sending channel and when it is not.

1. *$\mathscr{E}$ is a sending channel.* In this case the provers can output the correct state at both time steps, $\kappa-1$ and κ. Therefore, in this case we use the trivial bound that each of the fidelities is upper-bounded by 1, and

$$\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_\kappa,\kappa} + \bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right) \leq 1. \tag{6.114}$$

2. *$\mathscr{E}$ is not a sending channel.* Consider average fidelity expressions at time steps κ and $\kappa-1$ for the same execution i, and assume that κ is odd and output is requested at B's side. Each of the fidelities can be upper-bounded by its supremum,

$$\bar{F}_{\nu,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi \,\mathrm{Tr}\left[\mathscr{E}^{m,\nu}_{\vec{c}_\kappa,\kappa}\circ\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^{\kappa}_{✓}\right] \tag{6.115}$$

$$\leq \sup_{\Gamma_{B_{\kappa-1},B_\kappa}}\int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_\kappa-1,B_\kappa}\left(\mathscr{E}^{m,\nu}_{\vec{c}_\kappa,\kappa}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\right)\cdot\Pi^{\kappa}_{✓}\right] \tag{6.116}$$

and

$$\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1} = \int \mathrm{d}\psi \,\mathrm{Tr}\left[\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^{\kappa-1}_{✓}\right] \tag{6.117}$$

$$\leq \sup_{\Gamma_{A_{\kappa-1}}}\int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{A_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_{✓}\right]. \tag{6.118}$$

Here $\Gamma_{A_{\kappa-1}}$ and $\Gamma_{B_{\kappa-1},B_\kappa}$ denote CPTP maps which trace out additional registers of A and B and output a qubit state. Moreover, we've put $\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1} := \mathscr{Q}^{m,\nu}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)$ to denote a joint state of A and B at time step $\kappa-1$.

According to Definition 20 if the channel is not sending then we can bound

$$\sup_{\Gamma_{B_{\kappa-1},B_\kappa}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_{\kappa-1},B_\kappa}\left(\mathscr{E}^{m,\nu}_{\vec{c}_\kappa,\kappa}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right] \leq \sup_{\Gamma_{B_{\kappa-1}}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa}_{\checkmark}\right] \tag{6.119}$$

and hence,

$$\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_\kappa,\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right) \leq \frac{1}{2}\Bigg(\sup_{\Gamma_{B_{\kappa-1}}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right] + \tag{6.120}$$

$$+ \sup_{\Gamma_{A_{\kappa-1}}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{A_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right]\Bigg) \tag{6.121}$$

The right-hand side of the above equation is bounded by $\frac{5}{6}$ due to the approximate cloning theorem [18]. Therefore, we have

$$\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_\kappa,\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right) \leq \frac{5}{6}. \tag{6.122}$$

There are at most $k-m$ time steps $\kappa = 1,\ldots,k$ such that the channel $\mathscr{E}$ is not sending. Therefore, using Eqs. (6.114) and (6.122) we can write (6.112)

$$P_{\checkmark} \leq \sum_\nu q_\nu \frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}\frac{\bar{F}_{\nu,\vec{c}_\kappa,\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}}{2} \tag{6.123}$$

$$\leq \sum_\nu q_\nu \frac{1}{k}\left(m\cdot 1+(k-m)\cdot\frac{5}{6}\right) \tag{6.124}$$

$$= \frac{1}{k}\left(m+\frac{5}{6}(k-m)\right) \tag{6.125}$$

where in the last line we used the fact that $\sum_\nu q_\nu = 1$. □

6.7.6. OTHER PROOFS

In this appendix we present remaining proofs from Section 6.5.3. First we prove two statements about expected value of the rate of wins and average fidelity. Then we calculate the probability that our consistency check is satisfied. Finally, we derive a bound on the performance of k-round protocols in terms of double-average fidelity.

PROOF OF LEMMA 15

Here we prove that the expected value of rate $R_{\vec{c}_\kappa,\kappa}$, for specific depth κ and string of Clifford gates $\vec{c}_\kappa$, is equal to fidelity $\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathscr{T}}_\kappa)$ averaged over the state space.

Proof of Lemma 15. By definition, the expected value of $v^i_{\vec{c}_\kappa,\kappa}$ as,

$$\mathbb{E}\left[v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \frac{1}{|\mathsf{X}|}\sum_\psi\left(p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\cdot 1 + p_{\boldsymbol{\times}|\psi,\vec{c}_\kappa,\kappa}\cdot 0\right) = \frac{1}{|\mathsf{X}|}\sum_\psi p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \tag{6.126}$$

From the 2-design properties of set X, Lemma 19, we have that

$$\mathbb{E}\left[\nu^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \int \mathrm{d}\psi \; p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathscr{T}}_\kappa) \tag{6.127}$$

By linearity property of expected value,

$$\mathbb{E}\left[\sum_i \nu^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \sum_i \mathbb{E}\left[\nu^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \sum_i \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathscr{T}}_\kappa) = n_{\vec{c}_\kappa,\kappa}\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathscr{T}}_\kappa). \tag{6.128}$$

And therefore,

$$\mathbb{E}\left[R_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \mathbb{E}\left[\frac{\sum_i \nu^i_{\vec{c}_\kappa,\kappa}}{n_{\vec{c}_\kappa,\kappa}}\right]_{\mathsf{X}} = \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathscr{T}}_\kappa) \tag{6.129}$$

□

PROOF OF LEMMA 16

Here we present a proof that is analogous to the previous one, and shows that expected value of rate R_κ for a fixed depth κ, is equal to double-average fidelity.

Proof of Lemma 16. By definition, the expected value $\mathbb{E}\left[\nu^i_\kappa\right]_{\mathsf{X},\mathsf{Cliff}}$ as

$$\mathbb{E}\left[\nu^i_\kappa\right]_{\mathsf{X},\mathsf{Cliff}} = \frac{1}{|\mathsf{Cliff}|^\kappa}\frac{1}{|\mathsf{X}|}\sum_{C_1,\ldots,C_\kappa\in\mathsf{Cliff}}\sum_{\psi\in\mathsf{X}}\left(p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\cdot 1 + p_{\boldsymbol{\times}|\psi,\vec{c}_\kappa,\kappa}\cdot 0\right) \tag{6.130}$$

$$= \frac{1}{|\mathsf{Cliff}|^\kappa}\frac{1}{|\mathsf{X}|}\sum_{C_1,\ldots,C_\kappa\in\mathsf{Cliff}}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \tag{6.131}$$

By 2-design properties of the Clifford set, Lemma 20, we have that

$$\mathbb{E}\left[\nu^i_\kappa\right]_{\mathsf{X},\mathsf{Cliff}} = \int \mathrm{d}\psi \int C_1 \cdots \int C_\kappa \; p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \bar{\bar{F}}(\tilde{\mathscr{T}}_\kappa). \tag{6.132}$$

Since $\mathbb{E}\left[R_\kappa\right]_{\mathsf{X},\mathsf{Cliff}} = \frac{\sum_i^{n_\kappa}\mathbb{E}\left[\nu^i_\kappa\right]_{\mathsf{X},\mathsf{Cliff}}}{n_\kappa}$, with n_κ being a total number of executions for a fixed κ, we have that $\mathbb{E}\left[R_\kappa\right]_{\mathsf{X},\mathsf{Cliff}} = \bar{\bar{F}}_\kappa(\tilde{\mathscr{T}}_\kappa)$. □

PROOF OF COROLLARY 2

Next, we prove that the consistency check, Theorem 19, is satisfied with a certain probability, determined by the estimates on the performance of individual devices.

Proof of Corollary 2. The probability that the bound (6.22) is satisfied is equal to probability that all the individual bounds are satisfied, i.e. $\Pr\left[\left(\bigwedge_{j=1}^{\kappa}\left(|r_{M_j^{\mathscr{T}}} - \bar{F}(\tilde{M}_j^{\mathscr{T}})| > \epsilon_{M_j^{\mathscr{T}}} \wedge |r_{C_j} - \bar{F}(\tilde{C}_j)| > \epsilon_{C_j}\right)\right)\right]$ This is equal to

$$\Pr\left[\left(\bigwedge_{j=1}^{\kappa}\left(|r_{M_j^{\mathscr{T}}} - \bar{F}(\tilde{M}_j^{\mathscr{T}})| > \epsilon_{M_j^{\mathscr{T}}} \wedge |r_{C_j} - \bar{F}(\tilde{C}_j)| > \epsilon_{C_j}\right)\right)\right] = \tag{6.133}$$

$$= 1 - \Pr\left[\left(\bigvee_{j=1}^{\kappa}\left(|r_{M_j^{\mathscr{T}}} - \bar{F}(\tilde{M}_j^{\mathscr{T}})| \leq \epsilon_{M_j^{\mathscr{T}}} \vee |r_{C_j} - \bar{F}(\tilde{C}_j)| \leq \epsilon_{C_j}\right)\right)\right]. \tag{6.134}$$

Since $\Pr[A \vee B] \leq \Pr[A] + \Pr[B]$, we can write that

$$\Pr\left[\left(\bigvee_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{F}}} - \bar{F}(\tilde{M}_j^{\mathcal{F}})| \leq \epsilon_{M_j^{\mathcal{F}}} \vee |r_{C_j} - \bar{F}(\tilde{C}_j)| \leq \epsilon_{C_j}\right)\right)\right] \leq \tag{6.135}$$

$$\leq \sum_{j=1}^{\kappa} \Pr\left[|r_{M_j^{\mathcal{F}}} - \bar{F}(\tilde{M}_j^{\mathcal{F}})| \leq \epsilon_{M_j^{\mathcal{F}}}\right] + \Pr\left[|r_{C_j} - \bar{F}(\tilde{C}_j)| \leq \epsilon_{C_j}\right] \tag{6.136}$$

$$\leq 2\sum_{j=1}^{\kappa}\left(e^{-2n_{C_j}\epsilon_{C_j}^2} + e^{-2n_{M_j^{\mathcal{F}}}\epsilon_{M_j^{\mathcal{F}}}^2}\right) \tag{6.137}$$

where in the last line we used Hoeffding inequality, Eq. (6.12) and (6.13). Hence, we can write that

$$\Pr\left[\left(\bigwedge_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{F}}} - \bar{F}(\tilde{M}_j^{\mathcal{F}})| > \epsilon_{M_j^{\mathcal{F}}} \wedge |r_{C_j} - \bar{F}(\tilde{C}_j)| > \epsilon_{C_j}\right)\right)\right] \geq 1 - 2\sum_{j=1}^{\kappa}\left(e^{-2n_{C_j}\epsilon_{C_j}^2} + e^{-2n_{M_j^{\mathcal{F}}}\epsilon_{M_j^{\mathcal{F}}}^2}\right).$$

□

6

PROOF OF THEOREM 20

Here we prove our bound on the performance of k-round protocols in terms of winning rate R_κ in Test 2. The core of this theorem is the following lemma, which relates the diamond distance between the ideal and real implementation of a k-round protocol, and the double-average fidelity.

Lemma 24. *The performance of a k-round protocol can be bounded by the double-averaged fidelity in the following way*

$$\| \tilde{\mathscr{P}}^k - \mathscr{P}^k \|_\diamond \leq 2\sqrt{d(d+1)|\mathsf{Cliff}|^k\left(1 - \bar{\bar{F}}(\tilde{\mathscr{P}}^k)\right)} \tag{6.138}$$

where d is the dimension of the underlying Hilbert space, and $|\mathsf{Cliff}|$ is a size of the Clifford group for dimension d.

Proof of Lemma 24. To prove the inequality from Lemma 24 one needs to show dependence between $\bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k)$ and $\bar{\bar{F}}(\tilde{\mathscr{P}}^k)$. In particular, to preserve the direction of inequality we want that $\bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k) \geq \bar{\bar{F}}(\tilde{\mathscr{P}}^k)$. Firstly, we trivially have that

$$\bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k) \geq \min_{\vec{g}_k} \bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k) \tag{6.139}$$

On the other hand,

$$\bar{\tilde{F}}(\tilde{\mathscr{P}}^k) = \int \mathrm{d}G_1 \cdots \int \mathrm{d}G_k \bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k) \tag{6.140}$$

$$= \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_k \bar{F}_{\vec{c}_k}(\tilde{\mathscr{P}}^k) \tag{6.141}$$

$$= \frac{1}{|\mathrm{Cliff}|^k} \sum_{\vec{c}_k \in \mathrm{Cliff}} \bar{F}_{\vec{c}_k}(\tilde{\mathscr{P}}^k) \tag{6.142}$$

$$= \frac{1}{|\mathrm{Cliff}|^k} \left(\bar{F}_{\vec{c}_k^{\min}}(\tilde{\mathscr{P}}^k) + \sum_{\vec{c}_k \neq \vec{c}_k^{\min}} \underbrace{\bar{F}_{\vec{c}_k}(\tilde{\mathscr{P}}^k)}_{\leq 1} \right) \tag{6.143}$$

$$\leq \frac{1}{|\mathrm{Cliff}|^k} \bar{F}_{\vec{c}_k^{\min}}(\tilde{\mathscr{P}}^k) + 1 - \frac{1}{|\mathrm{Cliff}|^k} = 1 - \frac{1}{|\mathrm{Cliff}|^k} \left(1 - \bar{F}_{\vec{c}_k^{\min}}(\tilde{\mathscr{P}}^k)\right), \tag{6.144}$$

where in lines (6.141) and (6.142) we used Lemma 20, and in line (6.143) we separated the minimum element out of the summation and in line (6.144) we bounded each element under the sum by 1.

Now let us relate the minimum over the Clifford group to a minimum over the whole unitary group. Note that the Clifford group rotated by any unitary $\mathscr{U}$ remains a Clifford group. Therefore, let us rotate every C_j by a constant $\mathscr{U}_j$, $j = 1, \ldots, k$, such that the minimum over the Clifford sets corresponds to the minimum over the whole unitary group. Let us write $\vec{u}_k = \mathscr{U}_1, \ldots \mathscr{U}_k$,

$$\bar{F}_{\vec{u}_k \vec{c}_\kappa^{\min}}(\tilde{\mathscr{P}}^k) = \min_{\vec{g}_k} \bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k). \tag{6.145}$$

We obtain

$$\bar{\tilde{F}}(\tilde{\mathscr{P}}^k) \leq 1 - \frac{1}{|\mathrm{Cliff}|^k} \left(1 - \min_{\vec{g}_k} \bar{F}_{\vec{g}_k}(\tilde{\mathscr{P}}^k)\right) \tag{6.146}$$

and so

$$\| \tilde{\mathscr{P}}^k - \mathscr{P}^k \|_\diamond \leq 2\sqrt{d(d+1)} \sqrt{|\mathrm{Cliff}|^k \left(1 - \bar{\tilde{F}}(\tilde{\mathscr{P}}^k)\right)}. \tag{6.147}$$

□

Now we will relate the double-average fidelity of a k-round protocol to the double-average fidelity of the test. Indeed, we will show that these quantities are equal.

Lemma 25. *Double-averaged fidelity of a k-round protocol $\tilde{\mathscr{P}}^k$ of depth k is equal to double averaged fidelity of the test $\tilde{\mathscr{T}}_\kappa$ of the same depth, $\kappa = k$,*

$$\bar{\tilde{F}}(\tilde{\mathscr{P}}^k) = \bar{\tilde{F}}(\tilde{\mathscr{T}}_\kappa) \tag{6.148}$$

Proof. As stated in the main text, the proof of this lemma follows from noticing that the expression for double-averaged fidelity contains only polynomials of degree 2 in every Clifford gate C_j. Therefore, here averaging over the Clifford group is equivalent to averaging over the entire unitary group, since the Clifford group forms a 2-design. Furthermore, the equality is possible, since we have put $M_j^{\mathscr{T}} \equiv M_j \circ \mathscr{E}_j$, and $M_j^{\mathscr{T}}$ encompasses operations associated with sending and storing the qubit. □

The above two lemmas, combined with the Hoeffding bound on R_κ, Eq. 6.21 complete the proof Theorem 20.

6.7.7. Q-QUBIT PROTOCOLS

In this section we provide a description of a Q-qubit extension of our class of protocols. The structure of our description is exactly the same as the one from Section 6.3.2 with the difference that all the operations are carried out on more than one qubit.

In a Q-qubit k-round protocol nodes have a total of Q qubits available. At each round $j = 1,\ldots,k$ of the protocol nodes A and B can send any subset of the local qubits to one another. We denote all of the sending operations in round j by $\mathscr{E}_j$. Moreover, the nodes can store local qubits in the quantum memory and apply local gates. We denote these operations by $M_{A_j}^{(q_j)}$ and $G_{A_j}^{(q_j)}$ for node A, and $G_{B_j}^{(Q-q_j)}$ and $M_{B_j}^{(Q-q_j)}$ for node B. Here q_j and $Q-q_j$ denote the number of local qubits at A or B's side at round j, respectively, *after* the sending operation $\mathscr{E}_j$. Therefore, we describe a Q-qubit k-round protocol can with a map

$$\mathscr{P}^{k,(Q)} = \bigcirc_{j=1}^{k} \left[\left(G_{A_j}^{(q_j)} \circ M_{A_j}^{(q_j)} \right) \otimes \left(G_{B_j}^{(Q-q_j)} \circ M_{B_j}^{(Q-q_j)} \right) \right] \circ \mathscr{E}_j \tag{6.149}$$

In the presence of noise, we assume the following noise model for Q-qubit k-round protocols:

- the noise on gates is independent of the applied gate;
- the noise from memories, gates and transmission channels acts individually on each qubit;
- for each round j, the qubits are submitted to the same kind of noise on node A and node B (noise can differ from round to round).

Formally, we assume the following

$$\begin{aligned} \tilde{M}_{A_j}^{(q_j)} &= \tilde{M}_j^{\otimes q_j}, \quad \tilde{M}_{B_j}^{(Q-q_j)} = \tilde{M}_j^{\otimes Q-q_j} \\ \tilde{G}_{A_j}^{(q_j)} &= G_{A_j}^{(q_j)} \circ N_j^{\otimes q_j}, \quad \tilde{G}_{B_j}^{(Q-q_j)} = G_{B_j}^{(q_j)} \circ N_j^{\otimes Q-q_j} \end{aligned} \tag{6.150}$$

A bipartite Q-qubit, k-round protocol between any two nodes A and B consists of the following operations:

1. Local preparation of Q perfect qubit states, $|\psi\rangle_A \in \mathbb{D}(\mathscr{H}_A^{\otimes q})$ and $|\psi\rangle_B \in \mathbb{D}(\mathscr{H}_B^{\otimes Q-q})$. Here the superscript denotes the number of qubits on A's or B's side.
2. Sending any subset of local qubits from node A to node B and vice versa. We denote all exchanging of qubits in a round j by $\mathscr{E}_j$
3. Storing all local qubits, $M_A^{(q)} = M_A^{\otimes q}$, where $M_A \in U(\mathscr{H}_A)$, and $M_B^{(Q-q)} = M_A^{\otimes Q-q}$, where $M_B \in U(\mathscr{H}_B)$. Again, the superscript denotes the number qubits on A or B's side. Storage can take up to kt_M, where t_M is time necessary for creating one EPR pair and communicating classically between two most distant nodes. A noisy memory is denoted by a tilde, $\tilde{M}_A^{(q)}$ and accordingly for B.

4. Applying an arbitrary local operation by any node on any subset of local qubits. We describe this operation by a unitary gate $G_A^{(q)} \in U(\mathcal{H}_A^{\otimes q})$ and $G_B^{(Q-q)} \in U(\mathcal{H}_A^{\otimes Q-q})$. $\tilde{G}_A^{(q)} = G_A^{(q)} \circ N_A^{(q)}$ denotes the noisy counterpart, where $G_A^{(q)}$ is a perfect gate and $N_A^{(q)} = N_A^{\otimes q}$ is a noise map independent of the applied gate. Similarly for gates on B's side. Applying any gate takes a known finite time $\ell \ll t_M$.

5. Local measurement of all local qubits at the end of the protocol, $\Pi_A^{(q)} \in \mathrm{Proj}(\mathcal{H}_A^{\otimes q})$ and $\Pi_B^{(Q-q)} \in \mathrm{Proj}(\mathcal{H}_B^{\otimes Q-q})$. As stated before, we assume that the measurement can be performed perfectly.

Steps 2. – 4. are performed in rounds $j = 1, ..., k_{\mathscr{P}}$ a total of k times. We denote memories and gates that are used by A and B at a j-th round by $M_{A_j}^{(q_j)}, \tilde{G}_{A_j}^{(q_j)}$ and $M_{B_j}^{(Q-q_j)}, \tilde{G}_{B_j}^{(Q-q_j)}$ respectively. Such a protocol operates on a total number of Q qubits. Note that we model noise map as a product for each of Q qubits.

Definition 32 (k-round protocols)**.** Let $\mathcal{H}^{\otimes Q}$ be the Hilbert space of a two-partite quantum network. We define a k-round protocol as a CPTP map of the form $\Pi^{(Q)} \circ \tilde{\mathscr{P}}^{k,(Q)} \circ \mathrm{Prep}^{(Q)}$, where:

- $\mathrm{Prep}^{(Q)}$ corresponds to preparation of Q local qubits $|\psi\rangle_A \in \mathbb{D}(\mathcal{H}_A^{\otimes q_1})$ and $|\psi\rangle_B \in \mathbb{D}(\mathcal{H}_B^{\otimes Q-q_1})$ (Step 1.).
- $\tilde{\mathscr{P}}^{k,(Q)}$ is a map describing k rounds of local operations – memories and gates, as well as sending qubits from A to B (Step 2. – 4.),

$$\tilde{\mathscr{P}}^{k,(Q)} = \bigcirc_{j=1}^{k_{\mathscr{P}}} \left[\left(\tilde{G}_{A_j}^{(q_j)} \circ M_{A_j}^{(q_j)} \right) \otimes \left(\tilde{G}_{B_j}^{(Q-q_j)} \circ M_{B_j}^{(Q-q_j)} \right) \right] \circ \mathscr{E}_j. \tag{6.151}$$

- $\Pi_A^{(q)} \otimes \Pi_B^{(Q-q)}$ is a local measurement of all the local qubits. (Step 5.)

Now let us describe a test that certifies the above functionality. It is a straightforward extension of the ping-pong test we have discussed before. The idea of the Q-qubit teleportation-based ping-pong test is instead of teleporting a single qubit, to teleport all Q qubits back and forth between nodes A and B and sample a random Q-qubit Clifford gate ($\mathsf{Cliff}(2^Q)$) at line 3: of Test 2. The initial state of Q qubits $|\psi\rangle\langle\psi|^{(Q)}$ is chosen uniformly at random from a 2-design of Q-qubit states. In this case the test can be described with a map

$$\mathscr{T}^{\kappa,(Q)} = \bigcirc_{j=1}^{\kappa} C_j^{(Q)} \circ M_j^{\mathscr{T}(Q)}, \tag{6.152}$$

where, as before, the parity of j indicates on which side all the qubits are, and $M_j^{\mathscr{T}(Q)} \equiv M_j^{(Q)} \circ \mathscr{E}_j$ accounts for operations associated with transmission (here teleportation). Note that $M_j^{\mathscr{T}(Q)}$ can still be written in the product form, i.e. acting individually on each qubit, since we have assumed that $M_j^{(Q)}$ and $\mathscr{E}_j$ are both in the product form. Therefore, in the presence of noise, we employ the same model as for k-round Q-qubit protocols, i.e. $\tilde{M}_j^{\mathscr{T}(Q)} = (\tilde{M}_j^{\mathscr{T}})^{\otimes Q}$ and $\tilde{C}_j^{(Q)} = C_j^{(Q)} \circ N_j^{\otimes Q}$.

Based on the average fidelity estimate of this test $r(\tilde{\mathcal{T}}^{\kappa,(Q)})$ one can, again, check whether memories and gates were used together by satisfying an analog of the bound (6.22). This can be done provided one has access to estimates of quality of memories $\bar{F}(\tilde{M}_j^{(Q)}) = \int \mathrm{d}\psi^{(Q)} \operatorname{Tr}\left[(\tilde{M}_j^{\mathcal{T}})^{\otimes Q}(|\psi\rangle\langle\psi|^{(Q)}) \cdot |\psi\rangle\langle\psi|^{(Q)}\right]$ and gates $\bar{F}(N_j^{(Q)}) = \int \mathrm{d}\psi^{(Q)} \operatorname{Tr}\left[N_j^{\otimes Q}(|\psi\rangle\langle\psi|^{(Q)}) \cdot |\psi\rangle\langle\psi|^{(Q)}\right]$, for all j. Note that here we necessarily use the fidelity of $\tilde{M}_j^{(Q)}$ and $N_j^{(Q)}$ evaluated on the space of all Q-qubit states.

Now we can extend Theorem 20 onto Q-qubit protocols using the noise assumptions on the class of protocols. We arrive at the following statement.

Theorem 21 (Bounding the behavior of Q-qubit k-round protocols)**.** *Given the noise model is the same for all Q qubits at each round j, the performance of any Q-qubit Q-qubit k-round protocol, can be bounded in terms of an estimate for the double-averaged fidelity $R(\tilde{\mathcal{T}}^{\kappa,(Q)})$ of the Q-qubit test in the following way*

$$\| \tilde{\mathscr{P}}^{k,(Q)} - \mathscr{P}^{k,(Q)} \|_\diamond \leq 2\sqrt{d(d+1)} \sum_\kappa \sqrt{|\mathsf{Cliff}(d)|^\kappa \left(1 - R(\tilde{\mathcal{T}}^{\kappa,(Q)})\right)} \tag{6.153}$$

where $d = 2^q$ is the dimension of the underlying Hilbert space, and $|\mathsf{Cliff}(d)|$ is a size of the Clifford group for dimension d.

The proof of that statement is analogous to the single-qubit case, with the difference that here one uses the properties of the unitary 2-design given by the Clifford group of dimension 2^Q.

REFERENCES

[1] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[2] A. K. Ekert, *Quantum cryptography based on bell's theorem,* Phys. Rev. Lett. **67**, 661 (1991).

[3] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead,* Science **362** (2018), 10.1126/science.aam9288.

[4] I. L. Chuang and M. A. Nielsen, *Prescription for experimental determination of the dynamics of a quantum black box,* Journal of Modern Optics **44**, 2455 (1997).

[5] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Complete characterization of a quantum process: The two-bit quantum gate,* Phys. Rev. Lett. **78**, 390 (1997).

[6] S. T. Merkel, J. M. Gambetta, J. A. Smolin, S. Poletto, A. D. Córcoles, B. R. Johnson, C. A. Ryan, and M. Steffen, *Self-consistent quantum process tomography,* Phys. Rev. A **87**, 062119 (2013).

[7] R. Blume-Kohout, J. K. Gamble, E. Nielsen, J. Mizrahi, J. D. Sterk, and P. Maunz, *Robust, self-consistent, closed-form tomography of quantum logic gates on a trapped ion qubit,* (2013), arXiv:quant-ph/1310.4492 .

[8] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators,* Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005).

[9] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates,* Phys. Rev. A **77**, 012307 (2008).

[10] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and robust randomized benchmarking of quantum processes,* Phys. Rev. Lett. **106**, 180504 (2011).

[11] C. Pfister, M. A. Rol, A. Mantri, M. Tomamichel, and S. Wehner, *Capacity estimation and verification of quantum channels with arbitrarily correlated errors,* Nature Communications **9**, 27 (2018).

[12] A. Montanaro and R. de Wolf, *A survey of quantum property testing,* Theory of Computing, Graduate Surveys **7**, 1 (2016).

[13] J.-D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, *Device-independent certification of an elementary quantum network link,* arXiv e-prints , arXiv:1812.09117 (2018), arXiv:1812.09117 [quant-ph] .

[14] B. W. Reichardt, F. Unger, and U. Vazirani, *Classical command of quantum systems,* Nature **496**, 456 (2013).

[15] U. Mahadev, *Classical Verification of Quantum Computations,* 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (2018), 10.1109/FOCS.2018.00033.

[16] T. Vidick and J. Watrous, *Quantum Proofs* (now, 2016).

[17] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned,* Nature **299**, 802 (1982).

[18] N. Gisin and S. Massar, *Optimal quantum cloning machines,* Phys. Rev. Lett. **79**, 2153 (1997).

[19] W. Hoeffding, *Probability inequalities for sums of bounded random variables,* Journal of the American Statistical Association **58**, 13 (1963).

[20] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, *Efficiently characterizing the total error in quantum circuits,* New Journal of Physics **21**, 053016 (2019).

[21] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[22] J. J. Wallman and S. T. Flammia, *Randomized benchmarking with confidence,* New Journal of Physics **16**, 103032 (2014).

[23] L. Goldenberg, L. Vaidman, and S. Wiesner, *Quantum gambling,* Phys. Rev. Lett. **82**, 3356 (1999).

[24] G. Nebe, E. M. Rains, and N. J. A. Sloane, *The invariants of the clifford groups,* Designs, Codes and Cryptography **24**, 99 (2001).

[25] P. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, *On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis,* in *40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)* (IEEE Comput. Soc, 1999).

[26] A. Roy and A. J. Scott, *Unitary designs and codes,* Designs, Codes and Cryptography **53**, 13 (2009).

[27] D. Gross, K. Audenaert, and J. Eisert, *Evenly distributed unitaries: On the structure of unitary designs,* Journal of Mathematical Physics **48**, 052104 (2007).

[28] M. A. Nielsen, *A simple formula for the average gate fidelity of a quantum dynamical operation,* Physics Letters A **303**, 249 (2002).

7

CONCLUSIONS

7.1. SUMMARY OF RESULTS

In this thesis we analyzed protocols for quantum networks in the context of quantum resource requirements. We addressed the question of reducing the number of qubits necessary to realize certain tasks and we analyzed the resource states in terms of robustness to common types of noise. Moreover, we designed the first testing protocol certifying that a quantum network has the ability to support protocols at a certain stage of development. The main contributions presented in this thesis can be summarized as follows.

- **Chapter 3.** We presented a protocol for quantum anonymous transmission using the W state, and proved its security in the semi-active adversary scenario, i.e. when the adversary is active and the source of a quantum state is trusted. Moreover, we analyzed the behavior of our protocol under the action of common noise models that occur in a realistic quantum network. We compared the performance of our protocol with previously proposed protocols that use the GHZ state and Bell pairs as resource states. We quantified the performance of protocols by the fidelity of the transmitted quantum state. We found that, in many cases, our W-state based protocol tolerates more noise than the other protocols and achieves higher fidelity of the transmitted state. Additionally, we showed that our protocol can tolerate one non-responsive node, e.g. if one of the qubits of a multipartite state gets lost. In contrast, the protocol using the GHZ state cannot be carried out at all in this case, since the loss of a single qubit destroys the entanglement of the state. We also addressed the performance of the protocol based on using Bell pairs, and we showed that in the presence of noise, the performance of the protocol depends on the ordering of the sender and the receiver of the anonymous message in the network.

- **Chapter 4.** We proposed a protocol that achieves the task of sharing a quantum secret in a verifiable way, which reduces the number of qubits necessary to realize it.

In our scheme each of the n network nodes requires an n-qubit quantum memory and a workspace of at most $3n$ qubits in total. We achieved this by using few-qubit error correcting codes and by executing the protocol in a way that sequentially distributes ancilla states necessary to perform verification. By combining classical encryption with a quantum scheme we showed that we can construct a variety of verifiable hybrid schemes attaining maximum secrecy, i.e. schemes which do not reveal any information to any group of less than half of the n nodes participating in the protocol. We proved that our protocol is secure in the presence of active non-adaptive adversary. The security proof of our protocol expands on the approach suggested in the previous work of [1], which we believe might be of independent interest. Furthermore, we constructed explicit examples of our protocol which can be realized on small quantum networks.

- **Chapter 5.** We developed a protocol for secure multi-party quantum computation where each node holds single-qubit shares, with the approach based on quantum error correcting codes. Since our interest lied in reducing the quantum resources necessary to realize the protocol, we allowed the protocol to abort if the initial encoding of the shares is incorrect, as opposed to the existing approach. Thanks to this, we were able to execute the protocol with less qubits. What is more, we developed a procedure for a distributed verification of any logical state that is stabilized by a Clifford gate. This allowed us to perform distributed gate teleportation and implement a universal set of gates. We believe that this technique can be of independent interest. What is more, we followed the approach taken in our work for verifiable hybrid secret sharing, which allows for a sequential execution of the verification of the inputs. This solution reduced the operational workspace to n^2+4n qubits per node from $\Omega(n^3+n^2s^2\log n)$ [1], where s is the security parameter. We showed that our protocol is secure in the presence of active non-adaptive cheaters. Finally, we showcased our protocol on a small example for 7 nodes using Steane's 7-qubit code.

- **Chapter 6.** We also considered the problem of certifying that a quantum network achieves the ability to perform a subset of protocols within a certain stage of development, i.e. a stage called quantum memory network. We designed the first testing protocol, which certifies that nodes have the capability to control and send qubits around the network k times. We provided security statements for our protocol and expressed them in the interactive proof language. Moreover, in an honest implementation, we demonstrated that passing our test allows us to estimate average quality measures of the devices used in the test and conclude about the performance of other k-round protocols in a quantum network.

Concretely, based on the results of this thesis, given a quantum network supporting local control and storage of a *single qubit*, one can run an quantum anonymous transmission protocol. This can be achieved using either GHZ, W or Bell states as a resource, provided that the quality of an entangled link between the sender and the receiver is sufficiently high, see Chapter 3. For such a network, one can also test its ability to perform ping-pong-type protocols defined in Chapter 6. For larger quantum networks we give an

example of a verifiable hybrid secret sharing protocol, which requires simultaneous control over 21 qubits per node. Moreover, in a network supporting a workspace of 28 qubits per node, one can already run a demonstration of an multi-party quantum computation protocol performing a distributed CNOT gate between any two inputs. Both verifiable hybrid secret sharing and multi-party computation can be scaled up to work on larger networks, see Chapters 4 and 5.

7.2. OPEN QUESTIONS

In this section we discuss some open questions which might be an extension of the work presented in this thesis.

- **Verification of W states in a resource-efficient way in the presence of noise.** Answering this question positively would allow for removing an assumption about the trusted source in Chapter 3. Then our security proof could be extended to the case where the source might be corrupted, i.e. the fully active adversary scenario. For the noiseless W state protocol, it may be possible to achieve full security by employing self-testing techniques [2, 3]. However, this solution is very costly in resources and completely removes the assumptions on the devices used (so called, device-independent scenario). The problem of certifying the resource state efficiently, while keeping the assumptions about trusted devices remains therefore an open problem.

- **Comprehensive comparison of performance of protocols from Chapter 3.** In our comparison of anonymous transmission protocols we did not take into account generation rates of particular resource states. The reason for this is that very little is know about actual generation rates of multipartite states in a realistic quantum network. A more refined comparison of the performance of different protocols should account for the generation rates and resources required to produce the states in every particular experimental setup.

- **Lifting the number of cheaters to $2t$.** This question concerns both verifiable hybrid secret sharing (Chapter 4) and secure multi-party quantum computation (Chapter 5) protocols. Lifting the number of cheaters to the number $2t$ of erasure errors tolerable by the underlying error correcting code could be using authentication schemes [4]. In this case an authenticated quantum channel acts as a flag saying which qubits have not been transmitted correctly. Thanks to that, the power of the error correcting code increases to $2t$. An original idea of [4] involves authentication schemes based on error correcting codes [5], which is very costly in qubits. Indeed, sent each qubit requires s' further qubits to be authenticated, where the probability of an error in the authentication scales exponentially in s'. Therefore, it is an interesting question whether more efficient authentication schemes could reduce the quantum resources necessary to implement such schemes.

- **Performance of protocols in the presence of noise.** This question again applies both verifiable hybrid secret sharing (Chapter 4) and secure multi-party quantum computation (Chapter 5) protocols. Realistic quantum networks will inevitably

experience some sort of noise. Therefore, the tolerance of these protocols to the noise present, for example while sending qubits in the network, is an important question. Additionally, it would be interesting to investigate the scaling of security parameters with the amount of noise in the network. We remark that the first step toward this kind of analysis has already been taken in [6].

- **More general adversarial model.** The security definitions used for anonymous transmission, verifiable hybrid secret sharing and secure multi-party quantum computation explicitly assume that the set of cheaters is determined at the beginning of the protocol and says fixed throughout its execution (non-adaptive adversary). It is an open problem to consider an adaptive adversary which chooses which nodes to corrupt as the protocol is being executed. For the secret sharing and multi-party quantum computation protocols this could possibly be done by assuming that the environment of the protocol somehow records which nodes and when were corrupted. We conjecture that in order to achieve this a generalization of the quantum-to-classical reduction used in the security proof would be necessary. Furthermore, it could be interesting (but perhaps more difficult) to establish universal composable security of all protocols considered in Chapters 3, 4 and 5. Indeed, this would allow these protocols to be used as a subroutine of larger protocols without concerns about security.

- **Relaxing assumptions in the certification protocol of Chapter 6.** In the certification procedure in Chapter 6 we assume that each execution of the test is independent and identically distributed (IID). It could be interesting to explore whether this assumption could be relaxed. We believe that, given some extra work, deriving the soundness statement in the prover-verifier view of the test should be possible while relaxing the IID assumption. Another direction of study could be to generalize our test to the (partially or fully) device independent scenario, where the verifier does not trust her devices. Moreover, to complete the certification procedure, it would be desirable to derive a bound for explicit certification of the quality of the sending channel between the tested nodes. Finally, certifying other protocols within the quantum memory stage and even protocols within other stages of development, remains an open problem.

7.3. OUTLOOK

Building quantum networks is an exciting and ambitious enterprise. It requires a lot of effort on both hardware and software side to achieve a functioning quantum internet. Here we provide a short overview of current efforts and we place our work in the larger context.

First, it is important to establish and verify a quantum link between spatially separated locations. Some efforts have already been made in this direction, by establishing links on the ground [7], or in free space using satellites [8]. The links on the ground can use photonic systems, sending single photons over the commercial fiber. The main challenge here is that directly transmitted photons can be lost after traveling some distance in a fiber, due to the attenuation of the fiber. To overcome this, quantum networks need to be equipped with *quantum repeaters* [9] – stations which allow for establishing

a quantum channel between two nodes. This solution can be advantageous in linking two short-distance locations. On the other hand, creating an entangled link using satellites can be used to create entangled links on a global scale. However, it also faces many technical challenges at the moment, for example, photonic links can only be generated in locations with minimum light pollution (i.e. on a cloudless night).

One cannot predict with absolute certainty the exact direction that the development of the quantum internet will take. However, it is reasonable to speculate that quantum communication will follow a similar path to the one taken by the modern classical internet. Therefore, it is important to learn from the current internet architecture and design network layers able to manage the quantum network tasks, for example creation of entanglement. Some steps have already been taken in this direction, by defining layers able to manage point-to-point quantum connections [10] or multiple connections [11]. Although the physical entangled links at a distance are still an ongoing effort, there already exists dedicated software [12, 13] which simulates, among many, entangled links at a distance. This allows for early testing of network layer protocols, such that they can already be run when the physical entanglement between two locations is complete.

Some of the efforts at the level of quantum internet applications can also be paralelized. Firstly, since early networks will likely support only a few qubits per node, it is important to improve resource efficiency of existing protocols beyond quantum key distribution. Performance and security analysis for realistic implementations is also of considerable importance. Such analysis allows for establishing parameter regimes and benchmarking quantum networks, similar to the efforts taken in the domain of quantum computing [14–16]. This way, the quantum network architecture can be optimized to support specific applications, which can be later demonstrated in real life. These are the areas we hope to have contributed to with this thesis. Furthermore, with the existing simulation tools we can already start a search for new protocols, by creating a public end-user interface running applications on a simulated quantum network. Finally, it is important to identify and align the development of applications with industrial interest. Examples of such include quantum key distribution allowing for providing secure communication services by telecom industry or providing access to quantum computing in the cloud.

REFERENCES

[1] C. Crépeau, D. Gottesman, and A. Smith, *Secure multi-party quantum computation,* in *Proceedings of the Thirty-fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (ACM, New York, NY, USA, 2002) pp. 643–652.

[2] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, *Self-testing multipartite entangled states through projections onto two systems,* New Journal of Physics **20**, 083041 (2018).

[3] M. Fadel, *Self-testing Dicke states,* (2017), arXiv:quant-ph/1707.01215 .

[4] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, *Secure multiparty quantum computation with (only) a strict honest majority,* in *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)* (2006) pp. 249–260.

[5] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, *Authentication of quantum messages,* in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* (2002) pp. 449–458.

[6] Álvaro Gomez Iñesta, *Verifiable hybrid secret sharing in the presence of noise*, Master's thesis, Delft University of Technology (2020).

[7] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Provably secure and practical quantum key distribution over 307 km of optical fibre,* Nature Photonics **9**, 163 (2015).

[8] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, *Satellite-relayed intercontinental quantum network,* Physical Review Letters **120** (2018), 10.1103/physrevlett.120.030501.

[9] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Optimal architectures for long distance quantum communication,* Scientific Reports **6** (2016), 10.1038/srep20463.

[10] A. Dahlberg, J. de Oliveira Filho, R. Hanson, S. Wehner, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, and R. Knegjens, *A link layer protocol for quantum networks,* in *Proceedings of the ACM Special Interest Group on Data Communication - SIGCOMM '19* (ACM Press, 2019).

[11] W. Kozlowski and S. Wehner, *Towards large-scale quantum networks,* in *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication - NANOCOM '19* (ACM Press, 2019).

[12] A. Dahlberg and S. Wehner, *SimulaQron—a simulator for developing quantum internet software,* Quantum Science and Technology **4**, 015001 (2018).

[13] T. Coopmans, A. Dahlberg, M. Skrzypczyk, F. Rozpedek, R. ter Hoeven, L. Wubben, R. Knegjens, J. A. de Oliveira Filho, D. Elkouss, and S. Wehner, *Simulation of a 1025-node quantum repeater chain of nv centres with netsquid, a new discrete-event quantum-network simulator,* (2019).

[14] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators,* Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005).

[15] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates,* Phys. Rev. A **77**, 012307 (2008).

[16] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and robust randomized benchmarking of quantum processes,* Phys. Rev. Lett. **106**, 180504 (2011).

ACKNOWLEDGEMENTS

When I started my PhD I had no idea what an adventure and experience it would become. A huge part of it is thanks to the amazing people I got to come across. In this final part of my thesis I'd like to an informal moment to thank all of you whose presence was very special to me over these past four years.

First and foremost, **Stephanie**, I'd like to thank you for your patience and guidance throughout this process. Having a female supervisor like you in an environment so heavily dominated by men was a great honor. I learned not only what a good paper and presentation should be about, but also the dedication and hard work it takes to truly pursue your goals. Thank you for guiding me through the process of becoming an independent researcher and leading by example of your own excellent scientific integrity. It's a lesson I'll carry with me for life.

To my committee members: **Prof. Tittel**, **Prof. Vandersypen**, **Prof. Kashefi** and **Dr. Elkouss**, many thanks for taking the time to read this thesis and for participating in my PhD defense.

My incredible paranymps and friends, Maxime and Kenneth. Thank you both for the time and support in the preparations leading up to the defense. **Maxime**, thank you for being there through thick and thin, through far away trips and evenings on a couch with take-out, through broken hearts and broken ankles. You've been an extraordinary friend and inspiration, and I'm very proud of who you are. I'm looking forward to our next adventures. **Kenneth**, thanks for being such a bae, for your jokes and constant support. For inventing the good-enough counter and being an amazing zouk dance partner.

Jérémy, thanks for your incredible understanding of the most twisted things, for all the lunches and hours spent on deriving security proofs, when I learnt a great deal of math from you. **Gláucia**, thank you for the support, brunches, cakes on unconventional occasions and these late-night submissions to QCrypt followed by shots of Jagermeister. **Mark**, thanks for the extremely clever wit and the trips to the kebab place I never took. **Jonas**, thanks for teaching me that strawberries and not berries and for making my days not so aggressively mediocre.

Álvaro, thank you for being the best master's student anyone could hope for. I hope you learned as much from me as I did from you. **Bas**, thanks for being an awesome and chill travel buddy and a very easy-going officemate. **Thinh**, thanks for teaching me so much about cptps and having the patience to finish the certification paper. **Ramiro**, thanks for the trips, the drinking and the dancing, I always have a blast. And for supporting my music so closely! **Leo Di Carlo**, thank you for all of the rehearsals and performances, I had a blast every time. **Axel, Wojtek** thanks for sharing B201 at some point and making it the best office there ever was. **Kaushik, Valentina, Thinh, Filip, Nelly, Matt, Carlo, Tim, David M., Francisco, Guus, Corsin, Constantijn, Kanvi, Andre, Boxi, Julian, Leon, Scarlett, Sebastian, Hana** and everyone who's ever been in the group – thank you for making my PhD experience so much more enjoyable and memorable. Many thanks

to all of the past and current QuTech members, for making this environment feel like home. Finally, a huge thank you to **Helena** and **Chantal** for being the best management assistants and for being able to solve any big or small problem.

Annemiek, thank you for being such an easy going dude and my dancing super star, I always learn so much from you. **Leonie**, thank you for all the stay-overs, rum, and having a toothbrush at my place. **Shadia**, thanks for cooking the Shadia's special for me almost every time and for making me feel like I can invite myself over and unbutton my pants. **Gioia**, thanks for all the deep talks over food and incredible dances. **Deniz**, thanks for your warmth and kindness, and for those almond croissants at Michele's. **Bianka** and **Dominika**, thank you for being my oldest friends and for always making me feel like the last time we talked was yesterday. **Luuk** and **Heleen**, thank you for the support, the gigs, and so kindly looking after me all this time. **Kelvin**, for all those training sessions, and discussing the nuances of science and life. **Timothy**, for being a real friend in the music industry and the kindest and most hard-working producer I have ever had the pleasure to collaborate with. **Mousa** and **León**, for those crazy nights dancing salsa and bachata all over the place.

And finally, the biggest thank you to my extraordinary **parents**. Thank you for doing such an amazing job raising me. Thank you for all the love, and time, and effort, and money, and moving me across countries more times than I can count. Thank you for celebrating my publications, my dance moves, my song releases, my new shoes, and for your constant support when things get tough. Thank you for giving me such a strong foundation to go and explore the world, but still knowing that I always have a home to come back to. I look in the mirror now and I see a girl that I really like, and that's hugely thanks to you. I feel like whatever I say cannot express my love and gratitude towards you guys. I dedicated this thesis to you – I hope this symbolic gesture can begin to tell you how much I love you both.

CURRICULUM VITÆ

Victoria LIPINSKA

01-12-1992 Born in Slawno, Poland.

EDUCATION

2008-2011 High school
Slupsk, Pomerania, Poland

2011-2014 Undergraduate in Physics
University of Warsaw, Poland

2014-2016 Master's in Theoretical Physics
Stockholm University, Sweden

2015-2016 Master's Thesis in Quantum Information
ICFO, The Institute of Photonic Sciences, Barcelona, Spain

2016-2020 PhD in Quantum Information
Delft University of Technology, The Netherlands
Thesis: Quantum resource-saving protocols for early quantum networks
Promotor: Prof. dr. S. D. C. Wehner

List of Publications

6. **V. Lipinska**, J. Ribeiro, S. Wehner, *Secure multiparty quantum computation with few qubits*, Phys. Rev. A 102, 022405 (2020).

5. **V. Lipinska**, G. Murta, J. Ribeiro, S. Wehner, *Verifiable hybrid secret sharing with few qubits*, Phys. Rev. A 101, 032332 (2020).

4. **V. Lipinska**, T. Phuc Le, J. Ribeiro, S. Wehner, *Certification of a functionality in a quantum network stage*, Quantum Sci. Technol. 5 035008 (2020).

3. **V. Lipinska**, G. Murta, S. Wehner, *Anonymous transmission in a noisy quantum network using the W state*, Phys. Rev. A 98, 052320 (2018).

2. **V. Lipinska**, F. J. Curchod, A. Máttar, A. Acín, *Towards an equivalence between maximal entanglement and maximal quantum nonlocality*, New J. Phys. 20 063043 (2018).

1. M. Jarzyna, **V. Lipinska**, A. Klimek, K. Banaszek, M. G. A. Paris, *Phase noise in collective binary phase shift keying with Hadamard words*, Opt. Express 24(2), 1693-1698 (2016).