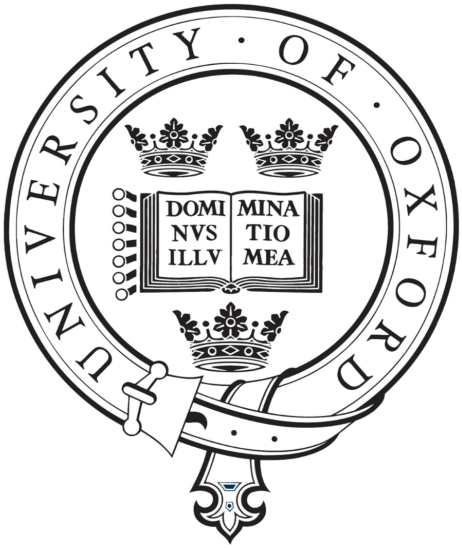
Enforcing trust in quantum networks

Anupama Unnikrishnan

Trinity College

University of Oxford



A thesis presented for the degree of

Doctor of Philosophy

Trinity Term 2019

To Amma and Achan,

and to Muthacha.

Abstract:
Enforcing trust in quantum networks

Anupama Unnikrishnan
Trinity College, University of Oxford
A thesis presented for the degree of Doctor of Philosophy, Trinity Term 2019

The phenomenal progress in quantum technologies over the past decades has laid the groundwork for the construction of quantum networks, which will channel the power of quantum theory to guarantee secure and efficient communication, computation, and much more. This thesis studies the notion of trust in quantum networks. In our information age, protecting the security or anonymity of data is a key requirement. We investigate certain protocols that are fundamental to the operation and applications of quantum networks, and propose ways to test and analyse their security, in spite of adversarial intervention. Our focus is on practical methods of verifying the untrusted components, which could be incorporated into realistic networks in the near future.

To begin, we propose a protocol for authenticated communication of quantum messages, by verifying the entanglement required for quantum teleportation in an experimentally feasible way. We model the performance of our scheme in the presence of noise. Furthermore, we explore such an authenticated teleportation in the one-sided device-independent scenario, where some devices used for verification may be corrupted. We derive error-tolerant self-testing bounds and extend our results to a realistic experimental setting, demonstrating the compatibility of our protocol with state-of-the-art technology. We then study anonymity, an essential feature for communication across networks. Combining the power of classical and quantum subroutines, we build a practical protocol for anonymous communication of quantum messages, without the need to trust the players in our network, their computational power, or the entanglement they share. We end by considering the verification of graph states distributed across a network of possibly dishonest players, applying our scheme to specific graph states that are central to quantum communication and computation schemes.

Acknowledgements

I owe many thanks to many people who have been a source of inspiration, support and distraction over these past few years.

To my supervisor, Vlatko Vedral, for his contagious sense of excitement about quantum mechanics, and for giving me the freedom to follow any research path I wanted to. To Damian Markham, for his guidance along this path, for warmly hosting me in his group, and moreover for his unending encouragement and humour; thank you for everything.

A huge thank you to my wonderful colleagues of the QI team at LIP6, Sorbonne Université for making my months in Paris so lively, rewarding, and immensely fun. I really couldn't have asked for a more welcoming group to visit. There are too many names to thank but I'll do it anyway: Mathieu, Nathan, Natansh, P1, Rawad, Robert, Raja, Rhea, Shane, Shouvik, Shraddha, Simon, Ulysse, Victor, Andrea, Clément, Dominik, Ellen, Federico, Francesco, Gözde, Léo, Luka and Luis. To Niraj, for being a great source of entertainment and proofreader. To Elham and Fred, for your enthusiasm and encouragement (and a special thanks to Elham for inspiring the title of this thesis). To Eleni and Iordanis, thank you for being brilliant collaborators and lovely humans. And to Mathieu, for being the best Paris (and cheese) guide, and for getting me through all the ups and downs.

To my Oxford group, particularly to Ben, Felix, Tristan, Nana, Cormac, Tian, Tom and Reevu, thank you for all the guidance, support and pub trips. To Nathan and Helen, I'm so grateful for your advice during a particularly tough time and for leading me towards quantum cryptography, and to Matty for his ability to explain things so well. To the organisations that have generously funded me: the EPSRC, Sorbonne Université, and Trinity College.

To my friends at the Trinity College MCR, for being such a warm community during those first few years, and especially to Hannah, Alex and Chih for being lovely friends, housemates and roast dinner chefs. To Belinda, who was always there for a chat when I needed it. To Deena, Jasmeet and Harmeet, for the long talks and much-needed weekends in London and Bristol. To the friends that brightened up my time in Oxford or Paris by coming to visit, all the way from California (Kelsey, Rachel, Cory, David, Marlee, Bianca, Rae, Lilly) and from closer (Hannah, Fatema, Sarah, Divya, Nikita). To my long-distance best friends of twenty-one years, Lekshmi and Parchi: is it too late to become fashion designers? And to all of my family in India, from the tiniest of cousins to my grandparents, thank you for your never-ending love, food, and starring in my short films.

Lastly, the biggest thank yous go to my mum, dad and Sangi, for putting up with my ridiculousness and being a constant source of kindness, support and warmth, especially through these past few years.

Contents

Chapter 1

Introduction

1.1 Preface

Quantum theory, with all its peculiarities and absurdities, has radically changed our perception of how the world works. From the pioneering groundwork of scientists in the early twentieth century [3–8], we are now in an unprecedented era. The counterintuitive features of quantum systems are being applied to create remarkably new technologies, which could go on to transform disciplines as varied as data security, navigation and medicine, to energy, imaging and fundamental science.

Some early revolutionary ideas have been the driving force behind much of the research in quantum-inspired technology. In 1982, Feynman suggested building a computer based purely on the laws of quantum physics [9], further developed by Deutsch with the first description of a universal *quantum computer* [10]. The ability of quantum bits (qubits) to exist in a superposition of 0 and 1, as opposed to classical bits, as well as decidedly nonclassical features such as entanglement, come together to promise a supreme computational advantage for certain tasks. This field has since exploded, with proposals for qubits ranging from photons [11], trapped ions [12], and nitrogen-vacancy centres in diamond [13], to quantum dots [14], Josephson junctions [15], and organic molecules [16]. Further, there is now a whole selection of quantum algorithms that can perform tasks more efficiently than classical computers, from

factoring of large numbers [17] and unstructured database search [18], to boson sampling [19] and even techniques in machine learning [20].

On the other hand, any breakthrough in quantum computing would have an adverse effect on the existing measures put in place to secure our data, which rely on certain problems being too hard to solve with classical computing [21]. Thankfully, the year 1984 had already witnessed the birth of cryptography based on quantum theory, with the observation by Bennett and Brassard that two people can agree on a secure key, even in the presence of an eavesdropper, using the principle that measurement disturbs a quantum system [22]. This prompted a new field of research to ensure security in a world of quantum technologies.

Parallel to the gradual development of a quantum computer is another technological dream, the *quantum internet* [23]. With the aim of allowing quantum communication between people anywhere in the world, at this moment it is the common goal of a large alliance of researchers all over Europe [24]. Such a quantum internet would be composed of network nodes, which are quantum processors at different locations, and channels that connect the nodes and transmit information stored in quantum states. To fight lossy channels, quantum networks must also have repeaters that facilitate long-distance transmission [25].

Building such a large-scale quantum network would enable us to harness the tremendous power of quantum information processing for a variety of useful tasks. The inherently quantum properties of entanglement, leading to nonclassical correlations that hold over long distances, or the impossibility of copying an unknown quantum state, for example, give quantum technologies an edge over what can be achieved classically. By exploiting this, we can guarantee secret communication secure even against a quantum computer [22], synchronise clocks all over the world with great precision [26], allow possibly faulty systems from a range of locations to reach consensus on the value of a bit [27], and much more. Such network tasks may require differing levels of technology, and in fact, many have already been implemented [28–33].

With the pace of progress in quantum technologies over the past decades, it is of paramount importance to think about trust. Do we trust that a quantum computer claim-

ing to be fully functional over on the other side of the world actually does what we ask? Or could it be manipulating us and our data, feeding us the wrong output that we have no way of checking? Do we trust the links and nodes in the global quantum network that we use regularly for secure communication? Or could some of the nodes be malfunctioning, or even worse, trying to disrupt or intercept our secrets?

To combat these worrying questions about the future we are heading towards, an array of clever ideas were put forward, leading to the field of *verification*. Through the tools that build up this area, we can now rest assured that our entanglement source can be thoroughly tested even if the devices in our laboratory have been hijacked by an adversary [34, 35]; a quantum computer with the ability to perform increasingly complex computations can be caught trying to trick us [36, 37]; our quantum messages can be sent securely [38] and anonymously [39].

Unfortunately, this is often true only in a theoretic sense. Verification in the real world frequently demands such an advanced level of experimental technology that it simply cannot be implemented in the near future. The situations described above, although satisfying the security concerns of even the most paranoid person, rely on assumptions such as little-to-no errors or noise in the experimental setup, the creation of millions more states than can be generated while retaining stability, or performing circuits that encode data in complex quantum error-correcting codes. The missing link here is practical verification: a way to test untrusted resources that is compatible with our current technology.

This thesis draws together the issues of trust and verification for realistic quantum networks. By building and employing practical methods of verifying the honest behaviour of equipment and network nodes (which we designate as players), and incorporating these into essential network protocols, we aim to guarantee trustworthy communication and computation with existing experimental toolkits.

1.2 Overview

Let us now give an outline of the contents of this thesis. Broadly speaking, our focus is on certifying the functioning of particular protocols that we expect to be central to the operation of

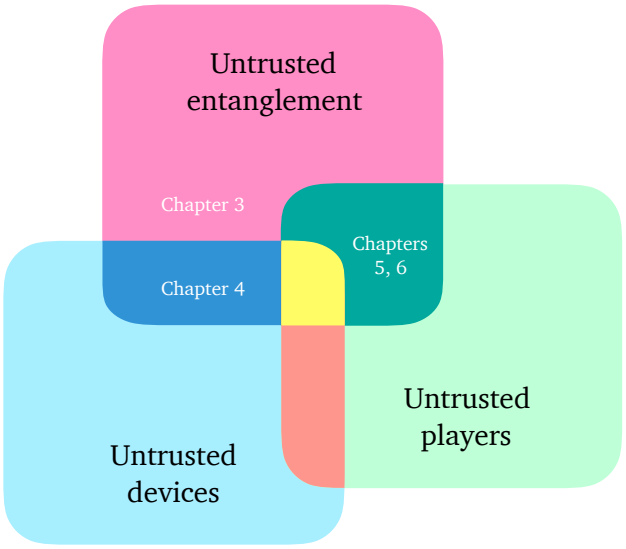


Figure 1.1: The possible untrusted components of our quantum networks.

quantum networks, such as sending quantum messages over long distances, or communicating these messages anonymously. In each setting, we analyse how to verify the entanglement required in a practical way, despite varying levels of trust in our network. In addition, we see how similar techniques can be applied to certify an important class of multipartite entangled states known as graph states, which would have wide-ranging applications in distributed protocols for communication and computation. (See Figure 1.1 for the trust levels we consider in our network.) We now present an overview of each Chapter.

We begin in Chapter 2 with an introduction to the preliminaries of quantum mechanics, focused on the framework and tools we will use throughout our work. In particular, here we discuss the stabiliser formalism, device-independent quantum cryptography, and semidefinite programming, among others.

Chapter 3 introduces the state verification problem, and applies it to authenticate a quantum channel between two players that may then be used for sending quantum messages through teleportation. Here, we are interested in a realistic experimental setting, and so we analyse the influence of noise on the measurement devices and states, deriving security bounds in each case. It is based on the following upcoming manuscript:

A. Unnikrishnan and D. Markham, *Authenticated teleportation in a noisy network*.

In Chapter 4, we investigate the realm of one-sided device-independence for authenticated teleportation, where one player may not trust their devices. Our aim is to bridge the gap between theoretical and experimental progress in this area, employing numerical techniques such as self-testing to derive robust results. Further, we remove some common self-testing assumptions and build a practical protocol for authenticated quantum communication with one-sided trust. It is based on the following publication:

[1] A. Unnikrishnan and D. Markham, *Authenticated teleportation with one-sided trust*, Phys. Rev. A **100**, 032314.

Chapter 5 addresses an important issue in quantum networks, that of anonymous communication. We combine six protocols, both classical and quantum, to construct a scheme for communicating quantum messages anonymously over a network, in the presence of both dishonest players and an untrusted source of entanglement. Our proposal takes into account realistic imperfections in networks. It is based on the following publication:

[2] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, *Anonymity for practical quantum networks*, Phys. Rev. Lett. **122**, 240501.

Further, this work is a part of the Quantum Protocol Zoo [40] developed by the QI team of the Laboratoire d'Informatique de Paris 6 and the Quantum Internet Alliance, and has been featured in a popular science article [41].

Moving on to another important issue in networks, in Chapter 6 we consider verification of graph states, which are the central resource in many quantum communication and computation protocols, shared between an untrusted network. We derive a general result for an arbitrary graph state and any number of dishonest players in the network, and give more specific, resource-efficient results for certain useful classes of graph states. It is based on the following upcoming manuscript:

A. Unnikrishnan and D. Markham, *Verification of graph states in an untrusted network*.

We conclude with a discussion of the scope and applications of our work, along with future perspectives, in Chapter 7.

1.3 Notation

A list of mathematical symbols and notation used throughout this thesis can be found below.

$\dagger$	Hermitian conjugate
$\mathbb{1}$	identity matrix
$\mathbf{0}$	zero matrix
$\lvert\cdot\rvert$	absolute value
$\lceil\cdot\rceil$	ceiling function
$\lVert\cdot\rVert$	norm
${}^{n}C_{r}$	$\dfrac{n!}{r!(n-r)!}$
$\ln$	natural logarithm
$\log_2$	base-2 logarithm
δ_i^j	Kronecker delta function (1 if $i = j$; 0 otherwise)
$i \wedge j$	AND operation (1 if $i = 1$ and $j = 1$; 0 otherwise)
$i \vee j$	OR operation (1 if $i = 1$ and/or $j = 1$; 0 otherwise)
$i \oplus j$	XOR operation (1 if $i = 1$ or $j = 1$; 0 otherwise)

Chapter 2

Preliminaries

We start by covering some of the basic topics in quantum information theory that will be useful for understanding this thesis, and then outline some relevant applications. For a more in-depth introduction, see [42].

2.1 Mathematical background

2.1.1 States

A Hilbert space $\mathcal{H}$ is a complex vector space with an inner product. A quantum state, $|\psi\rangle \in \mathcal{H}$, is a unit vector in a Hilbert space. Consider a two-dimensional Hilbert space $\mathcal{H}^2$ with basis vectors $\{|0\rangle, |1\rangle\}$, known as the computational basis. A state $|\psi\rangle \in \mathcal{H}^2$ is known as a *qubit*, and can exist in a linear combination of these basis states as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \tag{2.1}$$

where α, β are complex amplitudes. This is known as a *superposition*. Since a quantum state is a unit vector, the inner product between $|\psi\rangle$ and its dual vector $\langle\psi|$ is given by $\langle\psi|\psi\rangle = 1$, which leads to the normalisation condition, $|\alpha|^2 + |\beta|^2 = 1$. We will also use the basis $\{|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$.

While in this thesis we will only deal with qubits in this abstract form, note that in prac-

tice, they are realised by physical systems. For example, in polarisation encoding, information is stored in the polarisation degrees of freedom of a photon. In this case, the computational basis corresponds to rectilinear polarisation, where $|0\rangle$ is horizontal and $|1\rangle$ is vertical polarisation, and similarly the $\{|+\rangle, |-\rangle\}$ basis corresponds to diagonal polarisation. More general quantum states corresponding to d-level systems are called *qudits*; however, in this thesis we will only concern ourselves with qubits.

States that can be represented as $|\psi\rangle$ are known as *pure states*. It is useful to refer to the state of a quantum system in terms of a density matrix ρ, which is Hermitian ($\rho^\dagger = \rho$) and positive semidefinite ($\rho \geq 0$). The density matrix corresponding to a pure state $|\psi\rangle$ is given by $\rho = |\psi\rangle\langle\psi|$. A quantum system may be in a *mixed state*, which is a probabilistic mixture of pure states given by

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

This can be interpreted as the quantum system being in the state $|\psi_i\rangle$ with probability p_i. While density matrices always have trace 1, the density matrix of a pure state satisfies $\text{Tr}(\rho^2) = 1$, whereas for a mixed state it satisfies $\text{Tr}(\rho^2) < 1$.

To describe systems of multiple qubits, we use the *tensor product*, denoted by $\otimes$. For example, the tensor product of the states of subsystems A, B, given by $|\psi\rangle \in \mathcal{H}_A, |\phi\rangle \in \mathcal{H}_B$, gives the state of the joint system AB, given by $|\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. We will also use the notation $|\psi\rangle^{\otimes n}$ for the state $|\psi\rangle$ tensored with itself n times.

Consider a density matrix $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$. The *reduced* density matrix for the subsystem A is given by

$$\rho_A = \text{Tr}_B(\rho) = \sum_i \langle i_B|\rho|i_B\rangle , \tag{2.3}$$

where Tr_B is known as the partial trace over the system B, and $|i_B\rangle$ is any basis of $\mathcal{H}_B$.

2.1.2 Operations

The evolution of an isolated quantum system can be represented by a *unitary* operator U. This is a linear, inner-product-preserving operator satisfying $U^\dagger U = UU^\dagger = \mathbb{1}$. One can transform a quantum state to another by means of a unitary operation, as $|\psi\rangle \xrightarrow{U} U|\psi\rangle$. Unitary transformations are reversible, as can be seen by applying their Hermitian conjugate $U|\psi\rangle \xrightarrow{U^\dagger} U^\dagger U|\psi\rangle = |\psi\rangle$. Some important single-qubit unitaries we will use throughout this thesis are the Pauli matrices $\sigma_X, \sigma_Y, \sigma_Z$, and the Hadamard matrix H:

$$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.4}$$

Controlled unitary operators act on two or more qubits. They apply some operation on the *target qubits* if the *control qubit* is 1, and do nothing if it is 0. Some important two-qubit controlled operations are the CX (which is also known as the $CNOT$) and the CZ, given by

$$CX = \begin{bmatrix} \mathbb{1} & \mathbf{0} \\ \mathbf{0} & \sigma_X \end{bmatrix}, CZ = \begin{bmatrix} \mathbb{1} & \mathbf{0} \\ \mathbf{0} & \sigma_Z \end{bmatrix}. \tag{2.5}$$

Unitary operators are in fact a subset of *isometries*, which are linear, inner-product-preserving maps $\Phi : \mathcal{H}_A \to \mathcal{H}_B$ that satisfy $\Phi^\dagger \Phi = \mathbb{1}$. We will make use of local isometries, which are isometries applied to each local subsystem separately.

More generally, all physical operations on a quantum system can be described by completely positive, trace-preserving maps (*CPTP maps*) that map an input density matrix in one Hilbert space to an output density matrix in another Hilbert space. A map $\mathcal{E}$ is positive if for any positive operator ρ, $\mathcal{E}(\rho) \geq 0$. For $\mathcal{E}$ to be completely positive, we additionally require that the action of $\mathcal{E}$ on a subsystem of a joint system still results in a valid density matrix. By trace-preserving, we mean that $\mathrm{Tr}\big[\mathcal{E}(\rho)\big] = \mathrm{Tr}(\rho)$. Unitaries and isometries can then be viewed as examples of CPTP maps.

2.1.3 Measurement

The *measurement* of a quantum system is described in general by a set $\{M_m\}$ of measurement operators, with m denoting the measurement outcome. This set of operators satisfies $\sum_m M_m^\dagger M_m = \mathbb{1}$. The probability of obtaining outcome m from the measurement on a pure state $|\psi\rangle$ or a mixed state ρ is respectively given by

$$\Pr[m] = \langle\psi|M_m^\dagger M_m|\psi\rangle\,, \quad \Pr[m] = \mathrm{Tr}(M_m^\dagger M_m \rho). \tag{2.6}$$

The state of the system after the measurement on $|\psi\rangle$ or ρ is respectively given by

$$|\psi\rangle \longrightarrow \frac{M_m\,|\psi\rangle}{\sqrt{\Pr[m]}}, \quad \rho \longrightarrow \frac{M_m \rho M_m^\dagger}{\Pr[m]}. \tag{2.7}$$

A special case is that of a projective measurement, associated with an *observable* M, given by

$$M = \sum_m m P_m, \tag{2.8}$$

where for $\{M_m\}$ we now have the set of projectors $\{P_m = |m\rangle\langle m|\}$, which are orthogonal ($P_m P'_m = \delta_m^{m'} P_m$), and satisfy $\sum_m P_m = \mathbb{1}$. The possible measurement outcomes, $\{m\}$, are the eigenvalues of M. The probability of obtaining outcome m is given by $\Pr[m] = \langle\psi|P_m|\psi\rangle$.

A useful result is the projector onto the ± 1 eigenstate (eigenspace) of a (tensor product of) Pauli measurement(s). Taking σ_Z as an example, we can write it as

$$\sigma_Z = +1 \times P_+ + -1 \times P_-, \tag{2.9}$$

where P_+ is the projector onto the $+1$ eigenstate of σ_Z, and P_- is the projector onto the -1 eigenstate of σ_Z. We know $P_+ + P_- = \mathbb{1}$, which gives $P_- = \mathbb{1} - P_+$. Substituting this, we get $\sigma_Z = 2P_+ - \mathbb{1}$, which gives

$$P_+ = \frac{\mathbb{1} + \sigma_Z}{2}, \quad P_- = \frac{\mathbb{1} - \sigma_Z}{2}. \tag{2.10}$$

By performing such projective measurements on many identical copies of the state $|\psi\rangle$, one can approximate the *expectation value* of the observable M on the state $|\psi\rangle$, given by

$$\langle M \rangle = \langle \psi | M | \psi \rangle \, . \tag{2.11}$$

This converges to the true expectation value as the number of copies tends to infinity.

Let us now define the most general type of measurement. Taking the positive operator $E_m = M_m^\dagger M_m$, we now have $\sum_m E_m = \mathbb{1}$, and $\Pr[m] = \langle \psi | E_m | \psi \rangle$. The set $\{E_m\}$ is known as a POVM (positive operator-valued measure), while each element E_m is known as a POVM element. Contrary to projective measurements, the elements of $\{E_m\}$ need not be orthogonal. It is important to note that any POVM can be realised as a projective measurement on a higher dimensional Hilbert space [43].

An important concept related to observables is the *commutator*. For two observables A, B, we define $[A, B] = AB - BA$ as the commutator, and $\{A, B\} = AB + BA$ as the anti-commutator. If $[A, B] = 0$, we say the observables A, B commute, which means they can be measured in any temporal order. It is worth noting that the Pauli matrices $\sigma_X, \sigma_Y, \sigma_Z$ anti-commute with each other.

2.1.4 Entanglement

Quantum systems can be correlated in a way that has no classical analogue. A pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be entangled if it cannot be expressed as

$$|\psi\rangle = |a\rangle \otimes |b\rangle \, , \tag{2.12}$$

where $|a\rangle \in \mathcal{H}_A$ and $|b\rangle \in \mathcal{H}_B$. Similarly, a mixed state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be entangled if it cannot be expressed as

$$\rho = \sum_i p_i \rho_a^i \otimes \rho_b^i, \tag{2.13}$$

where $\{p_i\}$ is a probability distribution, $\rho_a^i \in \mathcal{H}_A$ and $\rho_b^i \in \mathcal{H}_B$. In other words, quantum systems in an *entangled* state cannot be written as a tensor product of the states of separate systems. States that can be written in this way are said to be *separable*.

Entanglement is at the very root of quantum mechanics and is fundamental to quantum information, computation and cryptography. We will go further into the details of entanglement in Section 2.4, in the context of device-independent quantum cryptography.

Some common entangled states we refer to in this thesis include the Bell state [44], or EPR state, which is a two-qubit maximally entangled state given by one of the following:

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \left|\Phi^-\right\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad \left|\Psi^+\right\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad \left|\Psi^-\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.14}$$

The Bell states can be transformed from one to another using local operations. There are a multitude of applications of Bell states in quantum information, from quantum teleportation [45] and superdense coding [46], to tests of nonlocality (Section 2.4) and many more.

The Greenberger-Horne-Zeilinger (GHZ) state [47] is an n-qubit multipartite entangled state given by

$$|GHZ\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}. \tag{2.15}$$

GHZ states are fundamental resources in protocols as varied as quantum anonymous transmission (Chapter 5), quantum secret sharing [48] and quantum metrology [49].

2.1.5 Graph states and the stabiliser formalism

A mathematical graph $\mathcal{G}$ is given by a set of vertices V, connected by edges in the set E. A graph state, denoted by $|\mathcal{G}\rangle$, is a multipartite entangled state corresponding to a mathematical graph. The vertices represent qubits, while the edges represent entanglement between them.

The state corresponding to an n-qubit graph is given by

$$|\mathcal{G}\rangle = \prod_{(k,l)\in E} CZ_{k,l} \, |+\rangle^{\otimes n} . \tag{2.16}$$

The stabiliser formalism gives a compact and elegant way to specify a graph state. Stabilisers of an n-qubit state are a subgroup of the n-qubit Pauli group that always give a $+1$ outcome when measured on that state. Thus, a graph state $|\mathcal{G}\rangle$ can be uniquely represented in terms of its stabilisers, as it is the only simultaneous $+1$ eigenstate of its stabiliser operators. To find the stabilisers of $|\mathcal{G}\rangle$, we first determine the stabiliser generators corresponding to each qubit $i \in \{1, ..., n\}$, given by

$$K_i = X_i \prod_{e\in N(i)} Z_e, \tag{2.17}$$

where $N(i)$ is the neighbourhood of qubit i, which is the set of qubits connected to i by an edge. Then, the full stabiliser group is given by every possible product of the stabiliser generators, denoted by $\mathcal{S} = \langle K_1, ..., K_n \rangle$. There are 2^n elements in the full stabiliser group of an n-qubit state, each denoted by $\mathcal{S}_j$, where $j \in \{1, ..., 2^n\}$. Each stabiliser in a group commutes with every other stabiliser in the group. The stabiliser equation is given by

$$\mathcal{S}_j \, |\mathcal{G}\rangle = |\mathcal{G}\rangle \, , \tag{2.18}$$

and the projector onto the $+1$ eigenstate of a stabiliser $\mathcal{S}_j$ is $\frac{\mathbb{1}+\mathcal{S}_j}{2}$. The projector onto the graph state can be written as the normalised sum of the elements of its stabiliser group:

$$|\mathcal{G}\rangle \langle\mathcal{G}| = \frac{1}{2^n} \sum_{j=1}^{2^n} \mathcal{S}_j. \tag{2.19}$$

A graph is *connected* if there is a path between any vertex in the graph to any other vertex. A *complete* graph has edges between every pair of vertices in the graph. A *cycle* is a sequence of vertices such that the first vertex is also the last. (See Figure 2.1 for examples.) Two graphs

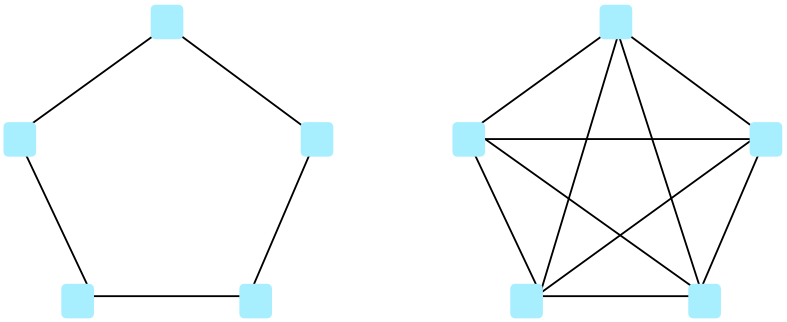


Figure 2.1: A cycle and complete graph. Both graphs are connected.

are locally equivalent if they can be transformed from one to the other by means of local operations only. For example, the n-qubit complete graph state is locally equivalent to the n-qubit GHZ state.

Graph states are the central resource in the paradigm of measurement-based quantum computation (MBQC) [50, 51]. Other applications of graph states include quantum secret sharing [28, 52] and quantum error correction [29].

2.1.6 Schmidt decomposition and purification

The *Schmidt decomposition* of a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is given by

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle , \tag{2.20}$$

where $|i_A\rangle \in \mathcal{H}_A, |i_B\rangle \in \mathcal{H}_B$ are orthonormal bases for A and B respectively, known as the Schmidt bases, and the λ_i are positive real numbers known as Schmidt coefficients. The number of non-zero λ_i is known as the Schmidt rank. A Schmidt rank of 1 means the state is separable; a Schmidt rank greater than 1 means the state is entangled.

The reduced states of systems A and B can then easily be expressed as

$$\rho_A = \sum_i \lambda_i^2 |i_A\rangle \langle i_A| , \quad \rho_B = \sum_i \lambda_i^2 |i_B\rangle \langle i_B| . \tag{2.21}$$

Another useful technique is that of *purification*, which often allows us to work with pure states instead of mixed states. Any mixed state $\rho \in \mathcal{H}_A$ can be seen as a pure state belonging

to a larger system $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, such that

$$\rho = \mathrm{Tr}_B(|\psi\rangle \langle\psi|). \tag{2.22}$$

Further, all purifications for the state ρ are unitarily equivalent.

We point out an interesting consequence of purification. By Stinespring's dilation theorem [53], a CPTP map is equivalent to a unitary operation on a higher dimensional Hilbert space. This may allow us to restrict our analysis to only unitary operations, as we will see later.

2.1.7 Closeness of states

To compare the closeness of two quantum states, we use the measures of *fidelity* and *trace distance*. We will use the following definitions for the fidelity between two quantum states:

$$\text{For pure states:} \quad F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2. \tag{2.23}$$

$$\text{For pure and mixed states:} \quad F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle. \tag{2.24}$$

$$\text{For mixed states:} \quad F(\rho, \sigma) = \left[\mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right]^2. \tag{2.25}$$

(Note that Equation (2.25) is the general definition, of which the others are special cases.)

The trace norm, or Schatten 1-norm, of an operator A is defined as $\|A\|_1 \equiv \mathrm{Tr}\sqrt{A^\dagger A}$. The trace distance between two quantum states ρ, σ is given by

$$D(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}\|\rho - \sigma\|_1. \tag{2.26}$$

The trace distance can also be defined as

$$D(\rho, \sigma) = \max_{0 \le P \le \mathbb{1}} \mathrm{Tr}[P(\rho - \sigma)], \tag{2.27}$$

where the maximisation is over all positive operators P.

We will make use of the following relations between fidelity and trace distance:

$$\text{For pure states:} \quad D(|\psi\rangle, |\phi\rangle) = \sqrt{1 - F(|\psi\rangle, |\phi\rangle)}. \tag{2.28}$$

$$\text{For pure and mixed states:} \quad 1 - F(|\psi\rangle, \rho) \leq D(|\psi\rangle, \rho) \leq \sqrt{1 - F(|\psi\rangle, \rho)}. \tag{2.29}$$

$$\text{For mixed states:} \quad 1 - \sqrt{F(\rho, \sigma)} \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)}. \tag{2.30}$$

2.1.8 No-cloning and quantum state discrimination

Here, we state some ideas that lie at the heart of much of quantum information and cryptography. The no-cloning theorem [54], which follows from the linearity of quantum theory, shows that it is impossible to copy an unknown quantum state, in direct contrast with classical information. The idea of discriminating between quantum states is closely linked to this. It is impossible to perfectly distinguish between two non-orthogonal quantum states; it would otherwise imply perfect quantum cloning [55, 56]. Let us see what kind of statements we can make instead. In general, let us consider a set of states $\{\rho_i\}_{i=1}^N$, each occurring with probability p_i, between which we wish to discriminate. Let $\{\pi_i\}$ be the set of corresponding POVM elements, each one associated to an outcome i. Then, the probability of successful discrimination, Pr[success], and the probability of making an error, Pr[error], are given by

$$\text{Pr[success]} = \sum_{i=1}^{N} p_i \text{Tr}(\pi_i \rho_i), \qquad \text{Pr[error]} = \sum_{i=1}^{N} p_i \sum_{j \neq i} \text{Tr}(\pi_j \rho_i). \tag{2.31}$$

2.2 Quantum teleportation

Quantum teleportation is a protocol by which an unknown quantum state can be transferred from one location to another, by means of local operations and classical communication alone, and was proposed by Bennett et al. in [45]. A prerequisite of the scheme is that the two players involved, Alice and Bob, share a Bell state.

The power of teleportation lies in the ability to transfer states without the need for an actual quantum channel linking Alice and Bob. This has great advantage for quantum state transmission over long distances, and more generally in quantum networks, computers and

Protocol 2.1 TELEPORTATION [45]

Input: Bell state $|\Phi^+\rangle$ shared between Alice and Bob.
Goal: Alice teleports state $|\phi\rangle$ to Bob.

1: Alice applies a CNOT operation, with her qubit to be teleported $|\phi\rangle$ as the control, and her qubit of the Bell state $|\Phi^+\rangle$ as the target.

2: Alice applies a Hadamard operation on her qubit to be teleported.

3: Alice measures her two qubits in the computational basis.

4: Alice sends her classical measurement outcomes b_1, b_2 to Bob.

5: Bob applies a transformation $Z^{b_1}X^{b_2}$ to his qubit of $|\Phi^+\rangle$ depending on the classical measurement outcomes, to recover $|\phi\rangle$.

simulators, while avoiding the inherent losses and noise that affect channels.

The teleportation protocol is given in Protocol 2.1. Let us see how this works. We will write the state to be teleported by Alice as a general qubit, given by $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. The state of the system at the beginning of the protocol, $|\psi_0\rangle$, is then

$$\begin{aligned}|\psi_0\rangle = |\phi\rangle\left|\Phi^+\right\rangle &= (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}\Big[\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)\Big]. \end{aligned} \tag{2.32}$$

After Alice's CNOT operation in Step 1, the state becomes

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)\Big]. \tag{2.33}$$

After Alice's Hadamard operation in Step 2, the state is given by

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{\sqrt{2}}\Big[\alpha(|{+}00\rangle + |{+}11\rangle) + \beta(|{-}10\rangle + |{-}01\rangle)\Big] \\ &= \frac{1}{2}\Big[\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\Big] \\ &= \frac{1}{2}\Big[\,|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]. \end{aligned} \tag{2.34}$$

After Alice's measurement in Step 3, we have the following possibilities:

$$b_1 = 0, b_2 = 0 \implies |\psi_3\rangle = |00\rangle (\alpha |0\rangle + \beta |1\rangle), \quad b_1 = 0, b_2 = 1 \implies |\psi_3\rangle = |01\rangle (\alpha |1\rangle + \beta |0\rangle),$$
$$b_1 = 1, b_2 = 0 \implies |\psi_3\rangle = |10\rangle (\alpha |0\rangle - \beta |1\rangle), \quad b_1 = 1, b_2 = 1 \implies |\psi_3\rangle = |11\rangle (\alpha |1\rangle - \beta |0\rangle). \tag{2.35}$$

Finally, after Bob's correction in Step 4, the overall state is either

$$b_1 = 0, b_2 = 0 \implies |\psi_4\rangle = |00\rangle (\alpha |0\rangle + \beta |1\rangle), \quad b_1 = 0, b_2 = 1 \implies |\psi_4\rangle = |01\rangle (\alpha |0\rangle + \beta |1\rangle),$$
$$b_1 = 1, b_2 = 0 \implies |\psi_4\rangle = |10\rangle (\alpha |0\rangle + \beta |1\rangle), \quad b_1 = 1, b_2 = 1 \implies |\psi_4\rangle = |11\rangle (\alpha |0\rangle + \beta |1\rangle). \tag{2.36}$$

In this way, the qubit $|\phi\rangle$ is teleported from Alice to Bob. The Steps 1 - 3 are referred to as a *Bell state measurement* (BSM), as this can be thought of as a projection of the state onto one of the four Bell states. Note that the teleportation procedure does not violate the no-cloning theorem, as the state no longer exists on Alice's side once it has been transferred to Bob. Further, it does not imply faster-than-light communication due to Step 4, which requires classical communication.

2.3 Quantum cryptography

The art of cryptography has intrigued humans for thousands of years. From early Egyptian hieroglyphics to the Enigma machines used during the war, it has always been of paramount importance for humankind to protect their secrets. As computer technology evolved, our methods of securing information grew more sophisticated. We began to rely on seemingly impossible problems, such as prime factorisation, and developing algorithms to secure our data that centred around such problems remaining hard to solve [21]. This is known as computational security.

Now at the beginning of a new era of quantum technologies, we must rebuild and re-define security. A quantum computer running Shor's algorithm [17] could crack the prime

factorisation problem in polynomial time. A new level of security was now necessary, that of information-theoretic security, which places no limits on the computational power of adversaries [57]. This led many scientists to ask the question: can we guarantee security based on physical principles alone?

The first ideas in this new realm of cryptography were by Wiesner with his proposal of quantum money [58], and Bennett and Brassard for quantum key distribution (QKD), which is now known as the BB84 protocol [22]. Their revolutionary idea was simple: Alice encodes a sequence of bits in photons polarised in either the rectilinear or diagonal bases, and sends them to Bob. He then chooses a basis in which to measure each photon's polarisation, and publicly announces his basis choices. They throw away any outcomes where Bob has measured in the wrong basis, and the remaining bits form their shared key. This key can then be used to encrypt a message using a one-time pad [59]. Crucially, the BB84 protocol protects against eavesdropping by virtue of some fundamental properties of quantum mechanics. If an eavesdropper, Eve, hoped to intercept Alice's photons, send a copy along to Bob and then wait for the basis announcement, this is prohibited by the no-cloning theorem. If she measures the intercepted photons, this will lead to some errors, as she does not know in which basis each bit is encoded. The players can detect this by checking a random subset of their key.

QKD has been an active research area ever since. For other significant early work, see Ekert's entanglement-based protocol [60] and Bennett's simplified version of the original protocol [61], while more recent prominent advances can be found in [32, 62–65]. Furthermore, the field of quantum cryptography has broadened, offering information-theoretic security for a variety of cryptographic tasks involving both classical and quantum information. This covers a range of subjects, from mistrustful cryptographic primitives such as coin flipping [30, 66] and bit commitment [67], and distributed tasks such as secret sharing [28, 48, 52, 68] and secure multiparty computation [69–71], to unforgeable quantum money [33, 72], anonymous transmission [2, 39, 73, 74], and many others. Moreover, there has been a multitude of works on the verification of quantum computation, where a client with limited computational capabilities must make use of an untrusted quantum server (for an overview, see [37]). As we will

go into more detail on specific topics within quantum cryptography in this thesis, we limit our discussion to this brief summary.

2.4 Device-independent quantum cryptography

2.4.1 Steering and nonlocality

To give the necessary background for device-independence, we must go all the way back to the thought experiment of Einstein, Podolsky and Rosen (EPR) in 1935 [75]. Their famous declaration that quantum mechanics is incomplete has led to a variety of scientists all over the world attempting (and succeeding) to prove them wrong. At the root of all this was entanglement. The EPR paradox, as it is now known, pointed out the following argument. If two players, say Alice and Bob, share an entangled pair of particles, measurements made by Alice on her particle will influence Bob's particle. However, how is this possible when they are separated by a long distance and their particles are no longer interacting? EPR claimed that there must be something we need to add to our quantum mechanical description of the systems, some so-called *hidden variables* that must be able to determine what happens when we measure any observable of the system, in order to be consistent with realism. Further, these variables must be *local*, so as to not require instantaneous communication.

Almost thirty years later, Bell proposed a test in the form of his now-famous Bell's inequality [44] that, if violated, would rule out the existence of such a local hidden variable theory, and prove the existence of *nonlocality* in quantum mechanics. Thus, a Bell test challenges local realism: the view that particles have properties irrespective of being observed, and signals between them cannot travel faster than the speed of light. The simplest Bell inequality is that of two measurement settings for each player with two outcomes each, proposed by Clauser, Horne, Shimony and Holt (CHSH) [76], and given by

$$|\langle A_0 B_0\rangle + \langle A_1 B_0\rangle + \langle A_0 B_1\rangle - \langle A_1 B_1\rangle| \leq 2, \tag{2.37}$$

where Alice measures either one of the observables A_0, A_1, and Bob either one of B_0, B_1, to

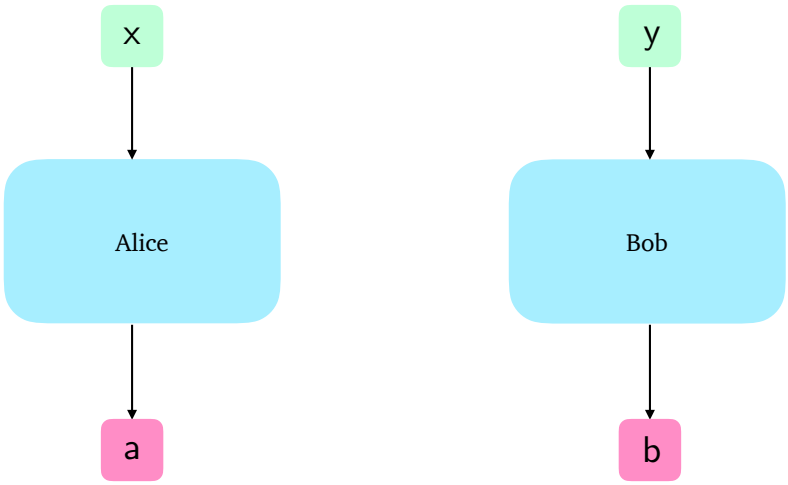


Figure 2.2: The nonlocality scenario. Alice measures in setting x to get outcome a, and Bob measures in setting y to get outcome b.

obtain outcomes that are ± 1. If this inequality is satisfied, it means that there could be a local hidden variable (LHV), or some shared classical information that determines the observed correlations. Such an LHV model is generally given by

$$p(\mathsf{a},\mathsf{b}|\mathsf{x},\mathsf{y}) = \int \mu(\lambda) p(\mathsf{a}|\mathsf{x},\lambda) p(\mathsf{b}|\mathsf{y},\lambda) d\lambda, \tag{2.38}$$

where λ is the hidden variable, $\mu(\lambda)$ is the probability distribution with respect to which λ is chosen, $p(\mathsf{a}|\mathsf{x},\lambda)$ is the probability that Alice measuring her particle in setting x gives an outcome a, $p(\mathsf{b}|\mathsf{y},\lambda)$ is the probability that Bob measuring his particle in setting y gives an outcome b, and $p(\mathsf{a},\mathsf{b}|\mathsf{x},\mathsf{y})$ is the joint probability of these events. Note that $p(\mathsf{a}|\mathsf{x},\lambda)$ does not depend on Bob's measurement or outcome, and similarly $p(\mathsf{b}|\mathsf{y},\lambda)$ does not depend on Alice's measurement or outcome; however, both probabilities depend on the hidden variable λ. (See Figure 2.2 for a depiction of the scenario.)

With the help of quantum mechanics, however, one can maximally violate the CHSH inequality at the Tsirelson bound of $2\sqrt{2}$ [77]; for example, if the players share the Bell state $|\Psi^-\rangle$, and measure the observables $A_0 = \sigma_Z, A_1 = \sigma_X, B_0 = \frac{-\sigma_Z - \sigma_X}{\sqrt{2}}$, and $B_1 = \frac{\sigma_Z - \sigma_X}{\sqrt{2}}$. This proves that there is no LHV theory that can explain the observed correlations.

The notion of *EPR-steering* in an entangled quantum system refers to the phenomenon that one player making local measurements can steer the qubit of the other player to a certain state. Although this was defined by Schrödinger [78] in response to the EPR paradox, it was only formalised in 2007 as a quantum information task by Wiseman, Jones and Doherty [79]. If one player (say Bob), can remotely steer the quantum state of the other player (say Alice), this rules out the existence of what is called a *local hidden state* (LHS) model, some pre-existing state on the side of Alice that is known to Bob. Such an LHS model is given by

$$\tau_{\mathsf{b}|\mathsf{y}} = \int \mu(\lambda)\rho_{\lambda}^{A} p(\mathsf{b}|\mathsf{y},\lambda)d\lambda, \tag{2.39}$$

where ρ_{λ}^{A} is the quantum state of Alice (which does not depend on Bob's measurement or outcome, but does depend on λ), and $\tau_{\mathsf{b}|\mathsf{y}}$ is the unnormalised state on Alice's side as a result of Bob measuring in setting y and getting an outcome b. The set of conditional states $\{\tau_{\mathsf{b}|\mathsf{y}}\}$ is known as an *assemblage*, of which each element is given by the probability $p(\mathsf{b}|\mathsf{y})$ multiplied by the resulting state on Alice's side, $\rho_{\mathsf{b}|\mathsf{y}}$, as $\tau_{\mathsf{b}|\mathsf{y}} = p(\mathsf{b}|\mathsf{y})\rho_{\mathsf{b}|\mathsf{y}}$.

Analogous to the Bell inequality case, we can express this capacity via inequalities that will be satisfied if there is an underlying LHS model. For example, one is said to observe steering if the following inequality [80] is violated:

$$|\langle A_0 B_0\rangle + \langle A_1 B_1\rangle| \leq \sqrt{2}. \tag{2.40}$$

A maximal violation of 2 can be demonstrated, for example, with the Bell state $|\Phi^+\rangle$ and the observables $A_0 = B_0 = \sigma_X, A_1 = B_1 = \sigma_Z$. Note that in addition to this two-measurement-setting steering inequality, we can demonstrate steering with more measurement settings.

The phenomena of Bell nonlocality and EPR-steering can be witnessed in all pure entangled states; however, as we move to mixed states, there is a hierarchy of quantum correlations (Figure 2.3). Not all entangled states are steerable or Bell nonlocal; not all steerable states exhibit Bell nonlocality. In 1989, Werner investigated this for a particular type of mixed en-

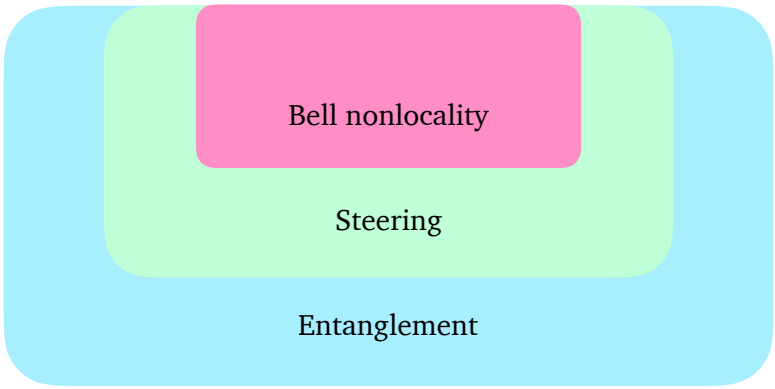


Figure 2.3: The hierarchy of quantum correlations. All states that exhibit Bell nonlocality exhibit steering and entanglement; all steerable states are entangled.

tangled state that we now call a Werner state [81], given by

$$\rho(v) = v \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + (1-v)\frac{\mathbb{1}}{4}, \tag{2.41}$$

where v is known as the visibility, and $|\Phi^+\rangle$ can alternatively be replaced by any Bell state.

Numerous experimental tests of both Bell nonlocality and steering have been carried out all over the world, and we will cover some of the highlights in Chapter 4. However, of particular importance when performing such a fundamental test of Nature is closing all possible loopholes that may lead to a false hypothesis. For example, the locality loophole [44] addresses the possibility that the players may communicate information about their choice of measurement setting or outcome. This is usually enforced in experiments by having a large separation between the two players. The freedom-of-choice loophole [82] is concerned with whether the measurement settings are chosen freely, or if they are somehow linked to the particles. Notably, the Big Bell Test collaboration [83] recently closed this loophole in multiple different experiments (sometimes concurrently with other loopholes) by using randomness generated by human participants. The detection loophole [84], caused by low detection efficiencies, is a common problem particularly in photonic experiments. Only a subset of the emitted pairs are usually measured in an experiment, and so often the fair-sampling assumption must be invoked, which takes the correlations from the detected pairs to be representative

of the full set.

2.4.2 Cryptographic applications

Let us now move on to the connection between nonlocality and cryptography. In Ekert's entanglement-based protocol for QKD [60], Alice and Bob check for a Bell inequality violation to detect eavesdroppers. This, in essence, is the idea behind device-independent quantum cryptography. If two players wish to test their shared entanglement, they can do so by violating a Bell inequality. In fact, it is even more powerful than this: the players need not even trust the devices with which they carry out their test. The only way to achieve a maximal Bell violation is by sharing a maximally entangled state and measuring the appropriate observables. This observation kick-started the field of device-independence, which promised to ensure the highest degree of security, satisfying even the most paranoid cryptographers. One no longer needed to overlook the possibility that an adversary may be hiding in their devices or cleverly manipulating them from a distance. QKD could be performed without worrying about security breaches resulting from the very devices it uses, such as those demonstrated in [85–88].

Some pioneering early works in device-independent quantum cryptography include that of Mayers and Yao, first in 1998 and further developed in 2004, where they proposed the idea of a 'self-testing' source of photons for QKD that could be tested even without trusting measurement devices [34, 89]. In 2005, Barrett, Hardy and Kent [90] formulated a protocol and security proof for distributing a shared secret bit in a device-independent way, resistant against any possible (non-signalling) attack by an eavesdropper. Since then, there has been a wealth of research on quantum cryptography with untrusted devices, notably the first fully device-independent security proof for QKD [91], self-testing of a multitude of states and measurements (which we discuss in more detail in Chapter 4), device-independent quantum random number generation [92, 93], and more recently, the use of quantum steering in one-sided device-independent (1sDI) protocols [94, 95].

How do the aforementioned loopholes come in to play here? As discussed by Pironio et

al. in [96], in a cryptographic setting the locality and freedom-of-choice loopholes are not important, as it is assumed that no information leaks out of each player's lab without their knowledge, and that the randomness used to choose the measurement settings is trusted. In fact, in the 1sDI scenario, one can even consider the player with trusted devices (in our case, Alice) to be the one who makes the random choice of measurement settings. The detection loophole, on the other hand, is another story. The fair-sampling assumption, when used in a cryptographic setting, could lead to cheating by the untrusted devices or source [97].

2.5 Semidefinite programming

Optimisation problems aim to find the maximum or minimum value of an *objective function* that satisfies some *constraints*. We now give some background on such problems for the purpose of entanglement certification.

To start, let us define a linear program, which is of the following form:

$$\begin{aligned} &\text{minimise} \quad \mathbf{c} \cdot \mathbf{x} \\ &\text{such that} \quad \mathbf{A}_i \cdot \mathbf{x} = b_i, \quad i = 1, ..., m \\ &\qquad\qquad \mathbf{x} \geq \mathbf{0}, \end{aligned} \tag{2.42}$$

where $\mathbf{c}$ is a row vector of length n, $\mathbf{A}_i$ is the i^{th} row of an $m \times n$ matrix A, and b_i gives the value of the constraint for each i. Solving this linear program gives the value of the vector $\mathbf{x} = (x_1, ..., x_n)^T$ that minimises the objective function, subject to the set of m linear constraints.

A semidefinite program (SDP) [98] then generalises this problem to matrices. It is a

convex optimisation problem of the following form:

$$\begin{aligned} &\text{minimise} \quad \text{Tr}(CX) \\ &\text{such that} \quad \text{Tr}(A_i X) = b_i, \quad i = 1, ..., m \\ &\qquad\qquad X \geq 0. \end{aligned} \tag{2.43}$$

Here, each A_i and C are symmetric matrices, and b_i again gives the corresponding value of the constraint. The solution of the SDP gives the $n \times n$ positive semidefinite matrix X that minimises the objective function, subject to the set of m constraints. (Note that an $n \times n$ matrix X is said to be positive semidefinite if, for all $v \in \mathbb{C}^n, v^\dagger X v \geq 0$.)

Techniques using SDPs have recently proved to be a powerful tool in quantum information. A notable early example was by Wehner [99], who applied them to derive Tsirelson's bound for the CHSH inequality. The development of the Navascués-Pironio-Acín (NPA) hierarchy [100, 101] paved the way for much work on device-independent entanglement certification using SDPs. The aim of the NPA hierarchy was to answer the question: given a probability distribution, does it correspond to statistics from local measurements on separate quantum systems? In other words, this provides an assessment of whether given correlations are nonlocal. For a set of operators $\mathcal{A} = \{A_1, ..., A_\nu\}$, the *moment matrix* Γ, of which each element is given by $\Gamma_{i,j} = \text{Tr}(A_i^\dagger A_j \rho)$, is positive semidefinite for all quantum states ρ. Each operator in the set $\mathcal{A}$ comprises of products of operators. As ν increases, this converges to the set of quantum correlations. One can then formulate an SDP in terms of Γ in order to test the quantum behaviour of untrusted systems. This can be used in both the 1sDI and DI settings; we will make use of this in Chapter 4.

2.6 Quantum networks

Throughout this thesis, we will deal with *players* in a network with varying levels of trust (Figure 1.1). When we are concerned with only two players, we will call them Alice and Bob as per convention. At the beginning of each Chapter, we will specify the network model, or

communication scenario, considered in the work that follows. In general, we may have the following options for our network:

- The players can be *honest* or *dishonest*. Honest players follow the protocol. Dishonest players might not follow the protocol, can work together and apply any operation on their part of the state.
- The quantum state they share is *untrusted*. The players obtain the state they require from an untrusted source, who may collaborate with the dishonest players.
- Their measurement devices can be *trusted* or *untrusted*. Trusted devices are free of adversarial intervention, but may be noisy. Untrusted devices might be corrupted by an adversary, and are modelled as black boxes.
- Honest players are only required to apply *local* operations, which can only affect their part of the state. Dishonest players can work together and apply operations on the part of the state that belongs to the whole dishonest set.

Our network is allowed the following classical resources:

- The players may share *classical channels*. They can use these to send classical information such that it cannot be tampered with (*authenticated channel*) and cannot be overheard (*secure channel*).
- The players may have access to a *classical broadcast channel*. This allows the broadcast of classical information by one player to all players in the network.

2.7 Security analysis

When discussing protocols in the context of quantum cryptography, a key question is how to assess their security. Broadly speaking, security refers to protection against adversaries. In the types of networks we consider, the adversarial components can be the source of the state, the players, or even their devices. To check the honesty of these adversarial components,

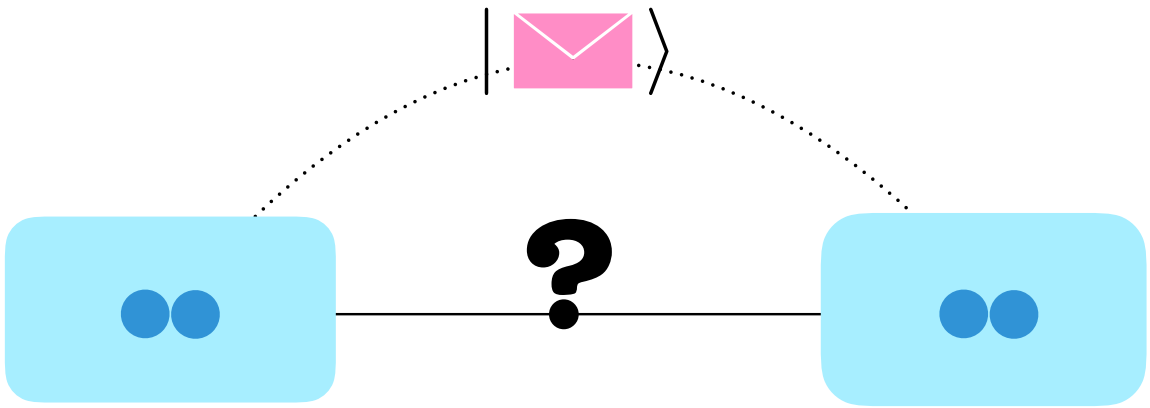
we subject them to some sort of test, and we are often interested in deriving the following security bounds:

- *Completeness*: This is the probability that the protocol works correctly if all the components behave honestly. For example, if only the source was untrusted, the completeness bound would give the probability of passing the test with an ideal state. This condition is sometimes referred to as correctness.

- *Soundness*: This represents the maximum probability of failure of the protocol if there are adversarial components. The soundness bound corresponds to the likelihood of the adversary tricking the protocol into passing the test; for example, an untrusted source providing a wrong state that passes.

Chapter 3

Authenticated teleportation in a noisy network



3.1 Introduction

In the cryptographic task of *authentication*, two players, who share a private classical key, wish to exchange a message, with the guarantee that it has not been tampered with by an adversary who controls their communication channel. This message may be classical or quantum; we are, of course, interested in the authentication of quantum messages, first formalised by Barnum et al. in [38]. Let us start, however, by explaining how authentication works in the classical case.

For classical information, the general way in which the identity of the sender and the integrity of a message are authenticated is as follows. To start with, we assume that our players, Alice and Bob, share a secret key. Alice then inputs a message, along with the secret key, to a particular message authentication code (MAC) algorithm, to produce an output. This output is then sent to Bob, along with the message itself. Bob inputs the received message and the secret key to the MAC algorithm, and checks if it matches the output that Alice sent. If so, the message is accepted. In this way, it is authenticated as being the message Alice herself has sent.

An example of an information-theoretically secure scheme for classical message authentication is that of Wegman and Carter [102]. They make use of a universal family of hash functions (proven to be secure without any computational hardness assumptions) to encode the message into a string of fixed length, and a one-time pad to encrypt it. The drawback here is that such classical methods only allow the key to be reused a small number of times.

The interplay between classical and quantum approaches to authentication started with work by Bennett et al. in 1982 (and published only thirty-two years later in [103]), with the idea of using quantum methods to authenticate classical messages that overrides the above problem. They employed quantum error-detecting codes to encode the encrypted classical message. A similar approach was suggested by Damgård et al. [104], and while they provided a rigorous security analysis, their scheme was even further from being practical. Other work on authentication of classical messages by quantum means include that of Curty and Santos [105], and Fehr and Salvail [106].

In the quantum scenario, Alice and Bob may share an insecure or imperfect quantum channel which they would like to use to send messages in the form of quantum states. If they had in their possession a perfect shared Bell state, Alice could send a quantum state to Bob using the quantum teleportation procedure (Protocol 2.1). The Bell state then forms a quantum channel between only Alice and Bob; it follows that only Alice could have sent the message that Bob receives, and an adversary cannot tamper with it during the transmission. However, the only thing we wish to assume is that our players share a private classical key. A quantum authentication scheme must then provide a way to distribute and test Bell states before using them as a quantum channel through which quantum messages can be sent.

The work by Barnum et al. [38] not only defines the quantum authentication framework that we will use in this Chapter, but additionally proposes the first scheme for authentication of quantum messages, based on error-correcting codes. Their starting point is to establish high quality Bell pairs between the players by means of an entanglement purification procedure, and to then use them for teleportation. They then give a few variants of the protocol, with the end result being a quantum authentication scheme that needs no interaction between the players, and the only requirement being that they share a random classical key.

In their scheme, Alice first encrypts her m-qubit quantum message ρ according to a classical key b. For example, if $m = 1$, a classical key comprised of two bits $b = \{b_0, b_1\}$ is used to encrypt the state as $\rho' = \sigma_Z^{b_0}\sigma_X^{b_1}\rho\sigma_X^{b_1}\sigma_Z^{b_0}$. (Similarly, encrypting an m-qubit message requires $2m$ classical key bits.) Such a so-called quantum one-time pad corresponds to teleportation. She then encodes ρ' in a randomly chosen, $(m + S)$-qubit stabiliser error-correcting code, where S is a security parameter. She sends the encoded version of ρ' to Bob, along with the choice of code and the classical key b. After checking for errors in the code and aborting if any occur, Bob decodes according to the error-correcting code, and decrypts according to b, to recover the message. To make this protocol non-interactive, they replace the classical communication by shared random strings. In this way, the maximum probability of failure of their authentication procedure, which is an assessment of its security, scales as 2^{-S}.

Further work on authentication of quantum messages has built upon this, focusing on

aspects such as proving the composability of the above protocol [107], allowing the key to be recycled if the message is accepted [107, 108], and even in the case where there is some tampering by the adversary [108]. While the exponential security scaling of such protocols is highly desirable, it comes at the cost of requiring levels of entanglement that increase with the security parameter. In practice, this becomes infeasible.

Our approach, on the other hand, is a simple yet practical way of achieving authenticated quantum communication. We consider an untrusted source who claims to be creating Bell states that the players wish to use for teleportation. The players then merely need to test many separate copies of the Bell state before using one for the teleportation procedure. This is an *authenticated teleportation*, whereby the quantum channel is authenticated before transmitting a message. While such a straightforward approach adversely affects the level of security one can expect, our focus is on methods that are not experimentally demanding; in fact, our scheme can be easily implemented with current linear optical setups.

As we are interested in practical quantum networks, we consider the influence of noise on our authentication procedure. We demonstrate the tradeoff between how well our authentication protocol works and its likelihood of failure in a noisy setting. Our protocol and analysis, being formulated in terms of measuring stabilisers, can then easily be extended for verifying graph states in a realistic, noisy scenario. This Chapter thus paves the way for introducing the main topics of this thesis.

3.2 Framework for quantum authentication

We start by outlining the authentication framework of Barnum et al. [38], which we use to discuss and define security. A quantum authentication scheme is comprised of a shared classical key, κ, known only to Alice and Bob and chosen uniformly from the set of keys $\mathcal{K}$, and corresponding operators A_κ, B_κ. Alice sends a message $|\phi\rangle$ to Bob by encoding with her operator A_κ. The output of Bob, after decoding with his operator B_κ, is the resulting quantum message, in addition to classical output indicating the decision to accept or reject the message encoded in orthogonal quantum states $|ACC\rangle, |REJ\rangle$. Based on the definitions in [38], we

introduce the following.

Definition 3.1. *We define the following security properties of a protocol for quantum authentication:*

- Completeness*: The protocol has* completeness c *if, when there is no adversarial intervention, the state accepted by Bob will be the same as that sent by Alice up to* c*; that is, for all* $\kappa \in \mathcal{K}$*,*

$$Tr\Big[\big(\,|\psi\rangle\langle\psi|\otimes|ACC\rangle\langle ACC|\,\big)\big(B_\kappa\big[A_\kappa(|\psi\rangle\langle\psi|)\big]\big)\Big] \geq c. \tag{3.1}$$

- Soundness*: If the adversary's intervention is characterised by* $\mathcal{O}$*, the resulting output state on Bob's side after the protocol is*

$$\rho_{out} = \frac{1}{|\mathcal{K}|}\sum_\kappa B_\kappa\Big[\mathcal{O}\big[A_\kappa(|\psi\rangle\langle\psi|)\big]\Big], \tag{3.2}$$

and the projector associated with failure is given by

$$P_{fail} = (\mathbb{1} - |\psi\rangle\langle\psi|)\otimes|ACC\rangle\langle ACC|\,, \tag{3.3}$$

then, the protocol has soundness ϵ *if*

$$Tr(P_{fail}\rho_{out}) \leq \epsilon. \tag{3.4}$$

In the notation of [38], a protocol is ϵ-secure if it has completeness 1 and soundness ϵ. The completeness condition is associated with an honest run of the protocol; in such an ideal case, the protocol should work perfectly. The soundness condition represents the failure of the protocol in the presence of an adversary, where by failure we mean that the accepted state lies in the orthogonal subspace to the ideal. It then tells us that, despite adversarial intervention, the maximum probability of failure of the protocol is ϵ. The smaller the ϵ, the more secure

the protocol. For example, in the authentication procedure of [38], ϵ decreases exponentially with an increase in the size of the encoding, scaling as 2^{-S}.

3.3 Network model

- *Players*: There are two players, Alice and Bob, both of whom are honest.
- *State*: The quantum state they share is untrusted. The players obtain the state they require from an untrusted source, who may produce a different state in each round. An honest source produces the Bell state, $|\Phi^+\rangle$.
- *Operations*: Their measurement devices are trusted, but may be noisy. The players are only required to perform local operations.
- *Classical channels*: The players share an authenticated classical channel, or a random secret key, which they can use to send classical information. (This ensures that our model lies in the authenticated communication setting.)

3.4 Protocol

Our protocol for authenticated teleportation is based on the work of Marin and Markham in [109], where they tackle quantum secret sharing over untrusted channels. We will start by adapting their protocol to the scenario of two players wishing to authenticate their quantum channel for teleportation, and then address noise in the network, finally extending our noise analysis to the certification of graph states.

We will formulate our protocol in terms of stabilisers, so that our analysis can be extended to other stabiliser states in a straightforward way. Here, our players, Alice and Bob, would like to certify that they share the Bell state

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{3.5}$$

so they can use it to teleport a quantum state $|\phi\rangle$. For the Bell state $|\Phi^+\rangle$, the stabiliser group is given by $\{\mathbb{1}\otimes\mathbb{1}, \sigma_X\otimes\sigma_X, -\sigma_Y\otimes\sigma_Y, \sigma_Z\otimes\sigma_Z\}$. Measuring any of these stabilisers on $|\Phi^+\rangle$ will always give a $+1$ outcome, and further, it is the only state for which this holds.

Based on this, we define an authenticated teleportation scheme given in Protocol 3.1. This protocol protects the players against an untrusted source who creates a state that is not $|\Phi^+\rangle$ and attempts to trick the players into using it for teleportation. The idea behind the protocol is simply that by asking the source for multiple copies of the state, and randomly choosing whether to test or use it, the source is forced to behave honestly in order to avoid being caught.

This corresponds to a quantum authentication scheme as in Definition 3.1, where the shared random classical key κ comprises of random strings that specify r and the choice of stabiliser to measure in each round $i \neq r$. Then, depending on this key κ, the players apply their corresponding operations. We will demonstrate that our protocol fulfils the conditions of completeness and soundness.

As mentioned previously, we are interested in analysing the performance of the protocol in a realistic, noisy network. We first consider how noise in Alice and Bob's measurement devices affects the security of the protocol, and further investigate the operation of the protocol when the source provides noisy states. Along the way, we will adapt the protocol to suit our purposes.

3.5 Security analysis

We first derive security bounds for Protocol 3.1, where the source can supply any state in the hope of cheating. We start by assuming Alice and Bob can do perfect measurements, and then extend this analysis to the case where their measurement devices are noisy.

3.5.1 Perfect measurements

For the case of perfect measurements, we first go through the security proof from [109], since we will be expanding on this in later sections. Let Π be the projector onto $|\Phi^+\rangle$, given by

Protocol 3.1 AUTHENTICATED TELEPORTATION

Input: Security parameter S.
Goal: Alice teleports state $|\phi\rangle$ to Bob through an authenticated channel.

1: An untrusted source generates S copies of the Bell state, and sends the shares of each to Alice and Bob.

2: Alice chooses a random $r \in \{1, ..., S\}$ and sends r to Bob.

3: For all copies $i \neq r$, Alice randomly chooses to measure either $\sigma_X, \sigma_Y, \sigma_Z$ on her part of the state. She tells Bob which operator she measured, and her measurement outcome.

4: For all copies $i \neq r$, Bob measures the same operator as Alice. For each copy, if the product of their measurement outcomes is $+1$ (or -1 when measuring σ_Y), they pass the test, otherwise they fail.

5: If *all* tests on copies $i \neq r$ were passed, the players ACCEPT. Otherwise, they REJECT.

6: The players run Protocol 2.1, using copy r as the entangled state, to teleport $|\phi\rangle$ to Bob.

$\Pi = |\Phi^+\rangle\langle\Phi^+|$. This can be written in terms of the stabilisers as

$$\Pi = \frac{1}{4}[\mathbb{1} \otimes \mathbb{1} + \sigma_X \otimes \sigma_X + \sigma_Z \otimes \sigma_Z + \sigma_Z\sigma_X \otimes \sigma_Z\sigma_X], \tag{3.6}$$

where from now onwards we will write $-\sigma_Y \otimes \sigma_Y$ as $\sigma_Z\sigma_X \otimes \sigma_Z\sigma_X$. The projector onto the $+1$ eigenspace of the stabiliser $\sigma_X \otimes \sigma_X$ (passing the test) is given by $\frac{\mathbb{1}\otimes\mathbb{1}+\sigma_X\otimes\sigma_X}{2}$, and similarly for the others. Thus, the POVM element for passing a test is

$$\begin{aligned} M_{pass} &= \frac{1}{3}\Big[\frac{\mathbb{1} \otimes \mathbb{1} + \sigma_X \otimes \sigma_X}{2} + \frac{\mathbb{1} \otimes \mathbb{1} + \sigma_Z \otimes \sigma_Z}{2} + \frac{\mathbb{1} \otimes \mathbb{1} + \sigma_Z\sigma_X \otimes \sigma_Z\sigma_X}{2}\Big] \\ &= \frac{\mathbb{1} \otimes \mathbb{1} + 2\Pi}{3}. \end{aligned} \tag{3.7}$$

Let us define M^r_{ACC} as the POVM element that corresponds to accepting. In Protocol 3.1, we see that all tests on copies $i \neq r$ must pass in order to do so. This gives

$$M^r_{ACC} = \bigotimes_{i \neq r} M_{pass_i}. \tag{3.8}$$

Theorem 3.1 ([109]). *In the case of perfect measurements, Protocol 3.1 has completeness 1 and soundness* $\frac{1}{S}$.

Proof. First, in the case that the source supplies all ideal Bell states, we show that the protocol works perfectly. We write S copies of the ideal state as $\underset{S}{\otimes}\Pi$. We can then calculate the probability of successful authenticated teleportation using copy r, when the source supplies all ideal states, as

$$\mathrm{Tr}\Big[\Pi_r \otimes M^r_{ACC} \underset{S}{\otimes} \Pi\Big] = \mathrm{Tr}\Big[\Pi_r \underset{i\neq r}{\otimes} \Big(\frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}\Big)_i \Pi_i\Big] = \mathrm{Tr}\Big[\Pi_r \underset{i\neq r}{\otimes} \Pi_i\Big] = 1. \tag{3.9}$$

As we see, in the ideal case we will always pass the verification test, and using the perfect Bell state for teleportation results in a teleportation fidelity of 1. Thus, if the source supplies ideal states, the players can perform authenticated teleportation of a quantum message perfectly.

We now consider the soundness bound. Let ρ_B be the output of the protocol, which is the teleported qubit on Bob's side along with the classical register that indicates whether to accept or reject the output. It is known that the fidelity of the teleportation is at least as high as the fidelity of the entangled state with the ideal Bell state [110].

Let P_{fail} be the projector onto the orthogonal subspace of the qubit $|\phi\rangle$ that Alice wants to teleport, given that the teleportation is accepted. If Bob's state ρ_B at the end of the protocol belongs to this subspace, the protocol has failed. We have

$$\begin{aligned}\mathrm{Tr}(P_{fail}\rho_B) &= \mathrm{Tr}\Big[(\mathbb{1}-|\phi\rangle\langle\phi|)\otimes|ACC\rangle\langle ACC|\,\rho_B\Big] \\ &\leq \mathrm{Tr}\Big[(\mathbb{1}\otimes\mathbb{1}-\Pi)_r\otimes|ACC\rangle\langle ACC|\,\rho^r_{AB}\Big],\end{aligned} \tag{3.10}$$

where the total output state after the verification steps, ρ^r_{AB}, is given by

$$\rho^r_{AB} = \frac{1}{S}\sum_{r=1}^{S}\Big[p_{acc}\rho^r_{acc}\otimes|ACC\rangle\langle ACC| + p_{rej}\rho^r_{rej}\otimes|REJ\rangle\langle REJ|\Big], \tag{3.11}$$

with p_{acc}, p_{rej} denoting the probability of accepting or rejecting, and $\rho^r_{acc}, \rho^r_{rej}$ denoting the output states conditioned on accepting or rejecting, respectively. Then, the joint probability

of accepting and the protocol failing is given by

$$\text{Tr}(P_{fail}\rho_B) \leq \text{Tr}\left[\frac{1}{S}\sum_{r=1}^{S}(\mathbb{1}\otimes\mathbb{1}-\Pi)_r p_{acc}\rho_{acc}^r\right]. \tag{3.12}$$

We will now denote the total state shared over all S copies between Alice and Bob as $\rho_{1\ldots S}$. Then, the entangled state used to teleport, which is the post-measurement state conditioned on accepting, is given by

$$\rho_{acc}^r = \frac{1}{\text{Tr}\left[M_{ACC}^r\rho_{1\ldots S}\right]}\underset{i\neq r}{\text{Tr}}\left[M_{ACC}^r\rho_{1\ldots S}\right] = \frac{1}{p_{acc}}\underset{i\neq r}{\text{Tr}}\left[M_{ACC}^r\rho_{1\ldots S}\right]. \tag{3.13}$$

This gives

$$\text{Tr}(P_{fail}\rho_B) \leq \text{Tr}\left[\frac{1}{S}\sum_{r=1}^{S}(\mathbb{1}\otimes\mathbb{1}-\Pi)_r\otimes M_{ACC}^r\rho_{1\ldots S}\right]. \tag{3.14}$$

Denoting

$$Q = \frac{1}{S}\sum_{r=1}^{S}(\mathbb{1}\otimes\mathbb{1}-\Pi)_r\otimes M_{ACC}^r, \tag{3.15}$$

we have

$$\text{Tr}(P_{fail}\rho_B) \leq \text{Tr}(Q\rho_{1\ldots S}). \tag{3.16}$$

We can determine an upper bound on this expression, no matter what state $\rho_{1\ldots S}$ the source supplies, by computing the maximum eigenvalue of Q. In Protocol 3.1, we accept if all tests on copies $i \neq r$ pass, and so in this case Q is given by

$$Q = \frac{1}{S}\sum_{r=1}^{S}(\mathbb{1}\otimes\mathbb{1}-\Pi)_r\bigotimes_{i\neq r}\left(\frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}\right)_i. \tag{3.17}$$

We know Π is an eigenprojector of $\frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}$. Let $\Pi^\perp$ be the projector $(\mathbb{1}\otimes\mathbb{1}-\Pi)$. Then, the

complete set of eigenprojectors for Q is given by

$$\{ \bigotimes_{\substack{k,\\ l\neq m}} \Pi_l^{\perp} \bigotimes_{\substack{S-k,\\ m\neq l}} \Pi_m \}, \tag{3.18}$$

where $k \in \{0, ..., S\}$ is the number of $\Pi^{\perp}$'s in the eigenprojector. We must then determine an expression for the eigenvalues of Q as a function of k, S, which we will denote as $g(k, S)$, from the eigenvalue equation

$$Q\Big[\bigotimes_{\substack{k,\\ l\neq m}} \Pi_l^{\perp} \bigotimes_{\substack{S-k,\\ m\neq l}} \Pi_m \Big] = g(k,S)\Big[\bigotimes_{\substack{k,\\ l\neq m}} \Pi_l^{\perp} \bigotimes_{\substack{S-k,\\ m\neq l}} \Pi_m \Big]. \tag{3.19}$$

We will make use of the following:

$$\begin{aligned} (\mathbb{1}\otimes\mathbb{1} - \Pi)\Pi = 0,\ \ (\mathbb{1}\otimes\mathbb{1} - \Pi)\Pi^{\perp} = \Pi^{\perp}, \\ \Big(\frac{\mathbb{1}\otimes\mathbb{1} + 2\Pi}{3}\Big)\Pi = \Pi,\ \ \Big(\frac{\mathbb{1}\otimes\mathbb{1} + 2\Pi}{3}\Big)\Pi^{\perp} = \frac{1}{3}\Pi^{\perp}. \end{aligned} \tag{3.20}$$

By examining the action of Q on an eigenprojector with $(S-k)$ Π's and k $\Pi^{\perp}$'s, we see that the corresponding eigenvalue is given by

$$g(k,S) = \frac{k}{S}(1)^{S-k}\Big(\frac{1}{3}\Big)^{k-1} = \frac{k}{S}\frac{1}{3^{k-1}}. \tag{3.21}$$

Here, $\frac{k}{S}$ is the probability of a randomly chosen eigenprojector r belonging to the set of k $\Pi^{\perp}$ terms (note that if r belongs to the set of Π terms, then this does not contribute to the eigenvalue), while the remaining terms come from the action of M^r_{ACC} on $\Pi, \Pi^{\perp}$. To determine the soundness bound, we then find the maximum value of $g(k, S)$ over all k, which occurs for $k = 1$, giving

$$\text{Tr}(P_{fail}\rho_B) \leq \max_k\ \frac{k}{3^{k-1}S} = \frac{1}{S}. \tag{3.22}$$

□

This shows that the optimal cheating strategy for a dishonest source is to provide all copies

but one as ideal Bell states. The probability of the non-ideal copy being used for teleportation is then $\frac{1}{S}$, representing the maximum probability of failure of our protocol.

Let us now consider the teleportation step, given that the players have accepted the transmission of the qubit as valid. We can derive an expression for the fidelity of the teleported qubit, $f = \text{Tr}(|\phi\rangle\langle\phi| \rho_{acc}^B)$, in terms of this soundness bound and the probability of acceptance:

$$\begin{aligned}\text{Tr}(P_{fail}\rho_B) &= \text{Tr}\Big[(\mathbb{1} - |\phi\rangle\langle\phi|) \otimes |ACC\rangle\langle ACC| \rho_B\Big] \\ &= \text{Tr}\Big[(\mathbb{1} - |\phi\rangle\langle\phi|)p_{acc}\rho_{acc}^B\Big] \\ &= p_{acc}(1-f). \end{aligned} \tag{3.23}$$

Thus, using our calculated expression for soundness in Equation (3.22), we obtain the following expression for the fidelity of the teleported qubit in Protocol 3.1:

$$f = 1 - \frac{\text{Tr}(P_{fail}\rho_B)}{p_{acc}} \geq 1 - \frac{1}{Sp_{acc}}. \tag{3.24}$$

3.5.2 Noisy measurements

We now extend this to the case where we have imperfect, or noisy, measurements, and model the scenario by introducing a noise parameter $p \in [0,1]$. Let us denote the POVM element for passing the test when we do the noisy $\sigma_X \otimes \sigma_X$ measurement as

$$p\frac{\mathbb{1}\otimes\mathbb{1} + \sigma_X \otimes \sigma_X}{2} + (1-p)\frac{\mathbb{1}\otimes\mathbb{1}}{2}, \tag{3.25}$$

and similarly for the other Pauli measurements $\sigma_Z\otimes\sigma_Z, \sigma_Z\sigma_X\otimes\sigma_Z\sigma_X$. Thus, with probability p each measurement proceeds perfectly, and with probability $(1-p)$ the measurement randomly gives either a ± 1 outcome. The POVM element for passing a test is then

$$M_{pass} = \frac{(3-p)\mathbb{1}\otimes\mathbb{1} + 4p\Pi}{6}, \tag{3.26}$$

and the overall POVM element for accepting in Protocol 3.1 is given by

$$M^r_{ACC} = \bigotimes_{i\neq r} \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1} + 4p\Pi}{6}\Big)_i. \tag{3.27}$$

Theorem 3.2. *In the case of noisy measurements with noise parameter p, Protocol 3.1 has completeness $(\frac{1+p}{2})^{S-1}$ and soundness $\max_k \frac{k}{S}(\frac{1+p}{2})^{S-k}(\frac{3-p}{6})^{k-1}$, where $k \in \{0,...,S\}, p \in [0,1]$.*

Proof. We will use:

$$\begin{gathered}(\mathbb{1}\otimes\mathbb{1} - \Pi)\Pi = 0,\ \ (\mathbb{1}\otimes\mathbb{1} - \Pi)\Pi^\perp = \Pi^\perp, \\ \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1} + 4p\Pi}{6}\Big)\Pi = \Big(\frac{1+p}{2}\Big)\Pi,\ \ \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1} + 4p\Pi}{6}\Big)\Pi^\perp = \Big(\frac{3-p}{6}\Big)\Pi^\perp.\end{gathered} \tag{3.28}$$

The probability of successful authenticated teleportation when the source supplies ideal states is given by

$$\begin{aligned}\mathrm{Tr}\Big[\Pi_r \otimes M^r_{ACC} \bigotimes_S \Pi\Big] &= \mathrm{Tr}\Big[\Pi_r \bigotimes_{i\neq r} \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1} + 4p\Pi}{6}\Big)_i \Pi_i\Big] \\ &= \mathrm{Tr}\Big[\Pi_r \bigotimes_{i\neq r} \Big(\frac{1+p}{2}\Big)\Pi_i\Big] \\ &= \Big(\frac{1+p}{2}\Big)^{S-1}.\end{aligned} \tag{3.29}$$

To calculate soundness, we replace Q in the previous proof by substituting in Equation (3.15) our new expression for M^r_{ACC}, giving

$$Q = \frac{1}{S}\sum_{r=1}^{S} (\mathbb{1}\otimes\mathbb{1} - \Pi)_r \bigotimes_{i\neq r} \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1} + 4p\Pi}{6}\Big)_i. \tag{3.30}$$

Considering the action of Q on a general eigenprojector with $(S-k)$ Π's and k $\Pi^\perp$'s, we find the expression for the corresponding eigenvalue to be

$$g(k,S,p) = \frac{k}{S}\Big(\frac{1+p}{2}\Big)^{S-k}\Big(\frac{3-p}{6}\Big)^{k-1}. \tag{3.31}$$

Again, we must determine the maximum eigenvalue of Q in order to bound the soundness of

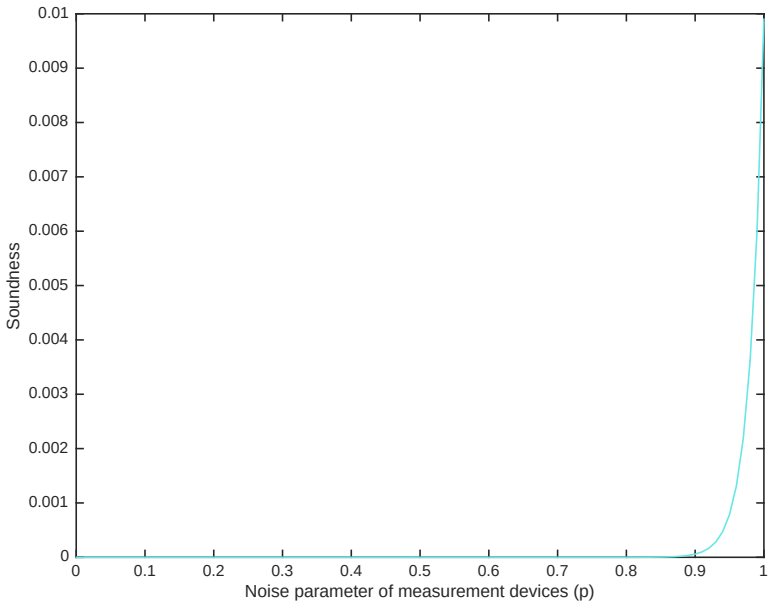


Figure 3.1: Variation in soundness with noise parameter of the measurements in Protocol 3.1. $S = 101$.

the protocol. This gives

$$\text{Tr}(P_{fail}\rho_B) \leq \max_k \frac{k}{S}\left(\frac{1+p}{2}\right)^{S-k}\left(\frac{3-p}{6}\right)^{k-1}. \tag{3.32}$$

□

We can compute this bound numerically. In Figure 3.1, we plot the maximum eigenvalue of Q for different values of p. This seems to show that the protocol can never fail in high noise. However, this is because our condition on the protocol accepting the state is that every copy must pass the test (Step 5). In high noise cases, we saw in our discussion of completeness that the probability of each state passing the test is low, and so it is very unlikely that noisy measurements will allow every test to pass. Thus, the protocol hardly ever accepts the state in high noise, and so it hardly ever fails.

From our analysis, it is clear that the protocol does not work well in the setting of noisy measurements. Therefore, we consider a modification of the protocol in the next section.

3.5.3 Noisy measurements with relaxed accept condition

We now consider no longer requiring each and every copy that is tested to pass, in order to accept the quantum message teleported using copy r. Let us denote the maximum number of tests that can fail as $\Delta \in \{0, ..., S-1\}$; this means that now, at least $S-1-\Delta$ tests must pass in order to accept. A modified version of the protocol incorporating such a failure threshold is given in Protocol 3.2.

In our analysis, we must consider all possible combinations of tests that are allowed to fail. The POVM element for passing a test remains $M_{pass} = \left(\frac{(3-p)\mathbb{1}\otimes\mathbb{1}+4p\Pi}{6}\right)$, while for failing a test it is $M_{fail} = \left(\frac{(3+p)\mathbb{1}\otimes\mathbb{1}-4p\Pi}{6}\right)$. We must then determine a new expression for M^r_{ACC}, which corresponds to accepting in Protocol 3.2. Let us take $\mathcal{D}$ to be the set of tests that are allowed to fail, such that $|\mathcal{D}| \leq \Delta$, and consider all possible choices for the copies that belong to this set. This gives

$$M^r_{ACC} = \sum_{\substack{\mathcal{D}, \\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D}, \\ i\neq r}} M_{pass_i} \bigotimes_{\substack{i\in\mathcal{D}, \\ i\neq r}} M_{fail_i}, \tag{3.33}$$

which for our case of noisy measurements gives

$$M^r_{ACC} = \sum_{\substack{\mathcal{D}, \\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D}, \\ i\neq r}} \left(\frac{(3-p)\mathbb{1}\otimes\mathbb{1}+4p\Pi}{6}\right)_i \bigotimes_{\substack{i\in\mathcal{D}, \\ i\neq r}} \left(\frac{(3+p)\mathbb{1}\otimes\mathbb{1}-4p\Pi}{6}\right)_i. \tag{3.34}$$

Theorem 3.3. *In the case of noisy measurements with noise parameter p, Protocol 3.2 has completeness*

$$\sum_{x=0}^{\Delta} {}^{S-1}C_x \left(\frac{1+p}{2}\right)^{S-1-x} \left(\frac{1-p}{2}\right)^x \tag{3.35}$$

and soundness

$$\max_k \frac{k}{S} \sum_{x=0}^{\Delta} \sum_{y=0}^{\Delta-x} {}^{S-k}C_x \, {}^{k-1}C_y \left(\frac{1+p}{2}\right)^{S-k-x} \left(\frac{1-p}{2}\right)^x \left(\frac{3-p}{6}\right)^{k-1-y} \left(\frac{3+p}{6}\right)^y. \tag{3.36}$$

Protocol 3.2 AUTHENTICATED TELEPORTATION WITH FAILURE THRESHOLD

Input: Security parameter S.
Goal: Alice teleports state $|\phi\rangle$ to Bob through an authenticated channel.

1: An untrusted source generates S copies of the Bell state, and sends the shares of each to Alice and Bob.

2: Alice chooses a random $r \in \{1, ..., S\}$ and a failure threshold $\Delta \in \{0, ..., S-1\}$, and sends r, Δ to Bob.

3: For all copies $i \neq r$, Alice randomly chooses to measure either $\sigma_X, \sigma_Y, \sigma_Z$ on her part of the state. She tells Bob which operator she measured, and her measurement outcome.

4: For all copies $i \neq r$, Bob measures the same operator as Alice. For each copy, if the product of their measurement outcomes is $+1$ (or -1 when measuring σ_Y), they pass the test, otherwise they fail.

5: If *at least* $S - 1 - \Delta$ tests on copies $i \neq r$ were passed, the players ACCEPT. Otherwise, they REJECT.

6: The players run Protocol 2.1, using copy r as the entangled state, to teleport $|\phi\rangle$ to Bob.

Proof. We will need the following:

$$
\begin{aligned}
&(\mathbb{1}\otimes\mathbb{1}-\Pi)\Pi = 0,\ \ (\mathbb{1}\otimes\mathbb{1}-\Pi)\Pi^{\perp} = \Pi^{\perp},\\
&\Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1}+4p\Pi}{6}\Big)\Pi = \Big(\frac{1+p}{2}\Big)\Pi,\ \ \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1}+4p\Pi}{6}\Big)\Pi^{\perp} = \Big(\frac{3-p}{6}\Big)\Pi^{\perp},\\
&\Big(\frac{(3+p)\mathbb{1}\otimes\mathbb{1}-4p\Pi}{6}\Big)\Pi = \Big(\frac{1-p}{2}\Big)\Pi,\ \ \Big(\frac{(3+p)\mathbb{1}\otimes\mathbb{1}-4p\Pi}{6}\Big)\Pi^{\perp} = \Big(\frac{3+p}{6}\Big)\Pi^{\perp}.
\end{aligned}
\tag{3.37}
$$

The completeness bound is given by

$$
\begin{aligned}
\mathrm{Tr}\Big[\Pi_r \otimes M^r_{ACC} \bigotimes_S \Pi\Big] &= \mathrm{Tr}\Bigg[\sum_{\substack{\mathcal{D},\\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D},\\ i\neq r}} \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1}+4p\Pi}{6}\Big)_i \Pi_i \bigotimes_{\substack{i\in\mathcal{D},\\ i\neq r}} \Big(\frac{(3+p)\mathbb{1}\otimes\mathbb{1}-4p\Pi}{6}\Big)_i \Pi_i\Bigg]\\
&= \sum_{x=0}^{\Delta} {}^{S-1}C_x \Big(\frac{1+p}{2}\Big)^{S-1-x}\Big(\frac{1-p}{2}\Big)^{x}.
\end{aligned}
\tag{3.38}
$$

To calculate the soundness bound, our expression for Q from Equation (3.15) is given by

$$Q = \frac{1}{S}\sum_{r=1}^{S}(\mathbb{1}\otimes\mathbb{1}-\Pi)_r \sum_{\substack{\mathcal{D},\\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D},\\ i\neq r}} \Big(\frac{(3-p)\mathbb{1}\otimes\mathbb{1}+4p\Pi}{6}\Big)_i \bigotimes_{\substack{i\in\mathcal{D},\\ i\neq r}} \Big(\frac{(3+p)\mathbb{1}\otimes\mathbb{1}-4p\Pi}{6}\Big)_i. \quad (3.39)$$

The eigenprojectors of Q are again given by $\{ \bigotimes_{\substack{k,\\ l\neq m}} \Pi_l^{\perp} \bigotimes_{\substack{S-k,\\ m\neq l}} \Pi_m\}$.

From the action of Q on an eigenprojector with $(S-k)$ Π terms and k $\Pi^{\perp}$ terms, using Equation (3.37), we determine the corresponding eigenvalue expression to be

$$g(k,S,p,\Delta) = \frac{k}{S}\sum_{x=0}^{\Delta}\sum_{y=0}^{\Delta-x} {}^{S-k}C_x\, {}^{k-1}C_y \Big(\frac{1+p}{2}\Big)^{S-k-x}\Big(\frac{1-p}{2}\Big)^{x}\Big(\frac{3-p}{6}\Big)^{k-1-y}\Big(\frac{3+p}{6}\Big)^{y}, \quad (3.40)$$

which leads to the soundness being the maximum of this expression over all possible values of k. (Note that if the players run Protocol 3.2 with perfect measurement devices, the corresponding security bounds can be determined by substituting $p=1$ in the above expressions.)

□

The maximum eigenvalue of Q for a certain Δ can be determined numerically for various values of the noise parameter p. We plot this, along with the completeness bound, for different failure thresholds in Figure 3.2. We see that allowing a large proportion of tests to fail of course gives a better completeness bound, but it comes at a cost of the protocol being more susceptible to cheating by a dishonest source. Our results demonstrate the robustness of our protocol, by providing a quantitative assessment of the tradeoff between how well the protocol works, and how likely it is to fail. This is particularly useful for an experimental implementation: for example, if the noise parameter of the measurement devices is known, we can use Theorem 3.3 to determine the appropriate failure threshold required to achieve our desired tradeoff.

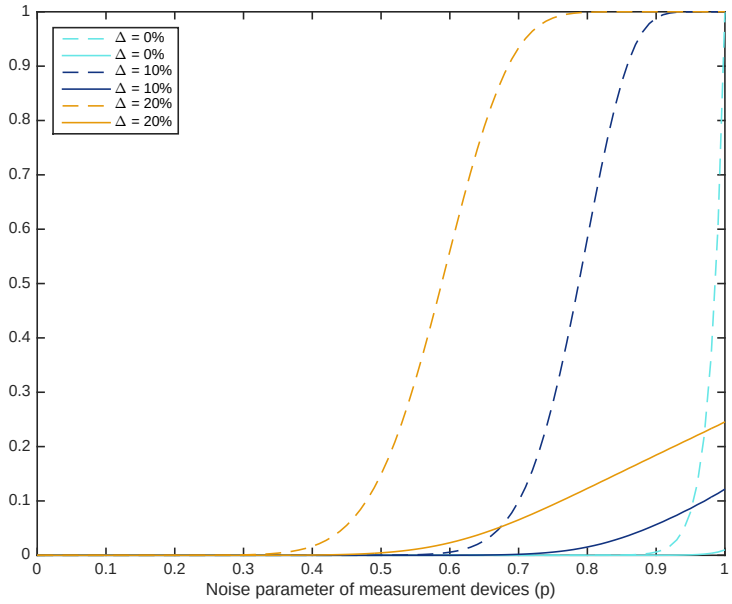


Figure 3.2: Comparison of completeness (dashed line) and soundness (solid line) bounds for different failure thresholds Δ in Protocol 3.2. $S = 101$.

3.6 Analysis for noisy states

Let us now consider the scenario where, due to imperfections of realistic networks, the states prepared by the source are noisy versions of the Bell state. In such a setting, we are interested in analysing how noise affects the working of the protocol: how likely it is that the final state will be accepted, and the statements we can make about the fidelity of teleportation in this case. We model the scenario using states of the form

$$\rho = v\Big[(1-\eta)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \eta\left|\Phi^-\right\rangle\left\langle\Phi^-\right|\Big] + (1-v)\frac{\mathbb{1}\otimes\mathbb{1}}{4}, \tag{3.41}$$

where v is a noise parameter and η is the dephasing noise. Such states take into account realistic noise that may be present when performing our protocols, and can easily be created in the lab when performing experiments [111]. Note that when $\eta = 0$, ρ takes the form of the Werner state [81] given in Equation (2.41), with visibility v.

Let us assume the measurements work perfectly for simplicity. As we saw earlier, in this

case, $M_{pass} = \frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}$. Then, the probability of passing a test with such a noisy state is

$$\text{Tr}(M_{pass}\rho) = \frac{3+3v-4v\eta}{6}. \tag{3.42}$$

Let us first see how Protocol 3.1 works in this scenario, where recall that $M^r_{ACC} = \bigotimes_{i\neq r} M_{pass_i}$. The probability of accepting (passing all $S-1$ tests) when the source produces noisy states is

$$\text{Tr}(M^r_{ACC} \bigotimes_S \rho) = \text{Tr}\Big[\rho_r \bigotimes_{i\neq r} \Big(\frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}\Big)_i \rho_i\Big] = \Big(\frac{3+3v-4v\eta}{6}\Big)^{S-1}. \tag{3.43}$$

We now examine the probability of acceptance with noisy states in Protocol 3.2. In the case of perfect measurements, we have $M_{fail} = \frac{2\mathbb{1}\otimes\mathbb{1}-2\Pi}{3}$. The modified M^r_{ACC} is then

$$M^r_{ACC} = \sum_{\substack{\mathcal{D},\\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D},\\ i\neq r}} M_{pass_i} \bigotimes_{\substack{i\in\mathcal{D},\\ i\neq r}} M_{fail_i} = \sum_{\substack{\mathcal{D},\\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D},\\ i\neq r}} \Big(\frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}\Big)_i \bigotimes_{\substack{i\in\mathcal{D},\\ i\neq r}} \Big(\frac{2\mathbb{1}\otimes\mathbb{1}-2\Pi}{3}\Big)_i. \tag{3.44}$$

We will also require the probability of failing a test with the noisy state:

$$\text{Tr}(M_{fail}\rho) = \frac{3-3v+4v\eta}{6}. \tag{3.45}$$

Then, the acceptance probability in Protocol 3.2 is given by

$$\begin{aligned}\text{Tr}(M^r_{ACC} \bigotimes_S \rho) &= \text{Tr}\left[\rho_r \sum_{\substack{\mathcal{D},\\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D},\\ i\neq r}} \Big(\frac{\mathbb{1}\otimes\mathbb{1}+2\Pi}{3}\Big)_i \rho_i \bigotimes_{\substack{i\in\mathcal{D},\\ i\neq r}} \Big(\frac{2\mathbb{1}\otimes\mathbb{1}-2\Pi}{3}\Big)_i \rho_i\right] \\ &= \sum_{x=0}^{\Delta} {}^{S-1}C_x \Big(\frac{3+3v-4v\eta}{6}\Big)^{S-1-x} \Big(\frac{3-3v+4v\eta}{6}\Big)^{x}. \end{aligned} \tag{3.46}$$

Note that for Werner states ($\eta = 0$), the above expression reduces to the completeness bound with noisy measurement devices. A plot of the probability of acceptance in a realistic experimental implementation is given in Figure 3.3, as a function of the failure threshold and visibility. If the source creates states of higher visibility, it is of course more likely to lead to

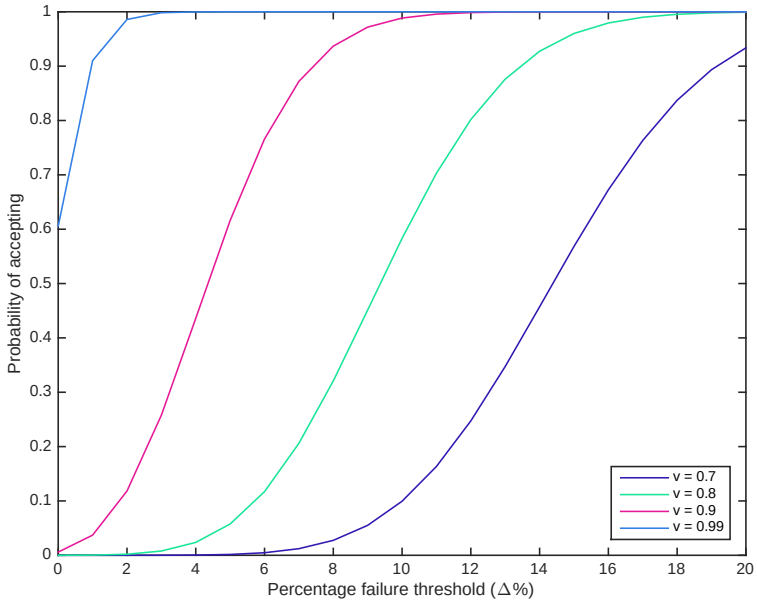


Figure 3.3: Comparison of the variation of acceptance probability in Protocol 3.2 with failure threshold Δ, for Werner states of different visibilities v. $S = 101$.

the teleported qubit being accepted; further, we can see how increasing the failure threshold helps this.

Knowing the probability of acceptance when the source provides Werner states, we can determine a lower bound on the fidelity of teleportation in Step 6 of Protocol 3.2. For this, we require the soundness bound in the case of perfect measurements (Equation (3.36) with $p = 1$), as well as Equation (3.23) for relating the soundness and probability of acceptance to the fidelity of teleportation. This gives

$$f \geq 1 - \frac{\max\limits_{k} \frac{k}{S} \sum\limits_{x=0}^{\Delta} \sum\limits_{y=0}^{\Delta-x} {}^{S-k}C_x \, {}^{k-1}C_y (1)^{S-k-x} (0)^x \left(\frac{1}{3}\right)^{k-1-y} \left(\frac{2}{3}\right)^y}{\sum\limits_{x=0}^{\Delta} {}^{S-1}C_x \left(\frac{1+v}{2}\right)^{S-1-x} \left(\frac{1-v}{2}\right)^x}. \tag{3.47}$$

We plot this in Figure 3.4 for different failure thresholds and Werner state visibilities. For a source creating Werner states of visibility v and allowing up to Δ failures, our results tell us the fidelity we can certify of an accepted transmission of a quantum message using Protocol 3.2. Further, by increasing the number of copies, the probability of acceptance increases while the soundness bound decreases, leading to a higher certified fidelity, and approaching

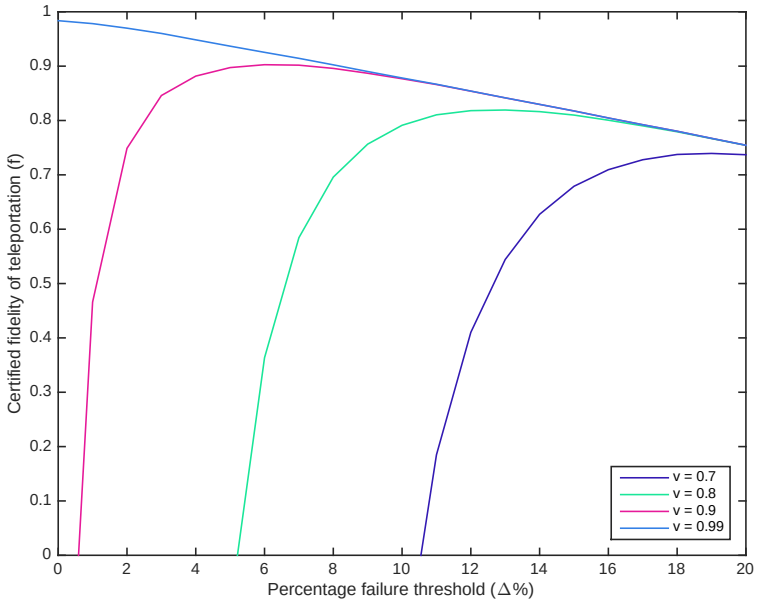


Figure 3.4: Comparison of the variation of fidelity of teleportation certified using Protocol 3.2 with failure threshold Δ, for Werner states of different visibilities v. $S = 101$.

the actual fidelity of teleportation with the Werner state.

3.7 Extension to graph state verification

As demonstrated by Markham and Krause in [112], the technique of stabiliser-based verification can be naturally extended to graph states. In Protocol 3.3, we give a modified version of their protocol that incorporates a failure threshold. We will now see how a similar noise analysis affects the security bounds in this case.

Consider an n-qubit graph state $|\mathcal{G}\rangle$ shared between n players. Its full stabiliser group is given by $\mathcal{S} = \{\mathcal{S}_j\}$, where $j = \{1, ..., 2^n\}$. Using the stabilisers for the graph state $|\mathcal{G}\rangle$, we can write the projector onto the graph state as a combination of these,

$$\Pi = |\mathcal{G}\rangle \langle \mathcal{G}| = \frac{1}{2^n} \sum_{j=1}^{2^n} \mathcal{S}_j. \tag{3.48}$$

The projector onto the $+1$ eigenspace of the stabiliser $\mathcal{S}_j$ (passing the test) is given by $\frac{\mathbb{1}+\mathcal{S}_j}{2}$. (Note that the identity matrix here is of size 2^n.) Let us model the noisy $\mathcal{S}_j$ measurement,

Protocol 3.3 VERIFICATION OF GRAPH STATES WITH FAILURE THRESHOLD (adapted from [112])

Input: Security parameter S.
Goal: The players verify that they share the n-qubit graph state $|\mathcal{G}\rangle$.

1: An untrusted source generates S copies of the graph state, and sends the shares of each to the players.

2: Player 1 chooses a random $r \in \{1, ..., S\}$ and a failure threshold $\Delta \in \{0, ..., S-1\}$, and sends r, Δ to the other players.

3: For all copies $i \neq r$, player 1 randomly chooses a stabiliser $\mathcal{S}_j$ to measure. She tells the other players which stabiliser she chose, and her measurement outcome.

4: For all copies $i \neq r$, the other players perform their corresponding stabiliser measurements. For each copy, if the product of all of the players' measurement outcomes is $+1$, they pass the test, otherwise they fail.

5: If *at least* $S - 1 - \Delta$ tests on copies $i \neq r$ were passed, the players ACCEPT. Otherwise, they REJECT.

6: The players use copy r for their desired application.

using POVMs as before, as

$$p\frac{\mathbb{1} + \mathcal{S}_j}{2} + (1-p)\frac{\mathbb{1}}{2}. \tag{3.49}$$

Then, the POVM element for passing a test is

$$\begin{aligned} M_{pass} &= \frac{1}{2^n}\sum_{j=1}^{2^n}\Big[p\Big(\frac{\mathbb{1} + \mathcal{S}_j}{2}\Big) + (1-p)\frac{\mathbb{1}}{2}\Big] \\ &= \frac{1}{2^n}\sum_{j=1}^{2^n} p\frac{\mathbb{1}}{2} + \frac{1}{2^n}\sum_{j=1}^{2^n} p\frac{\mathcal{S}_j}{2} + \frac{1}{2^n}\sum_{j=1}^{2^n}(1-p)\frac{\mathbb{1}}{2} \\ &= \frac{1}{2^n}p\frac{2^n\mathbb{1}}{2} + \frac{p}{2}\frac{1}{2^n}\sum_{j=1}^{2^n}\mathcal{S}_j + \frac{1}{2^n}(1-p)\frac{2^n\mathbb{1}}{2} \\ &= \frac{\mathbb{1} + p\Pi}{2}, \end{aligned} \tag{3.50}$$

and the POVM element for failing a test is $M_{fail} = \frac{\mathbb{1} - p\Pi}{2}$. We now write M^r_{ACC}, the overall

POVM element for accepting in Protocol 3.3, as

$$M^r_{ACC} = \sum_{\substack{\mathcal{D}, \\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D}, \\ i\neq r}} M_{pass_i} \bigotimes_{\substack{i\in\mathcal{D}, \\ i\neq r}} M_{fail_i} = \sum_{\substack{\mathcal{D}, \\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D}, \\ i\neq r}} \Big(\frac{\mathbb{1}+p\Pi}{2}\Big)_i \bigotimes_{\substack{i\in\mathcal{D}, \\ i\neq r}} \Big(\frac{\mathbb{1}-p\Pi}{2}\Big)_i. \tag{3.51}$$

The analysis then proceeds similarly to before, with this new M^r_{ACC}. We give the most general result in the following Theorem, which can then be reduced to specific cases (eg. perfect measurements, no failure threshold) by substituting the relevant values of parameters.

Theorem 3.4. *In the case of noisy measurements with noise parameter p, Protocol 3.3 has completeness*

$$\sum_{x=0}^{\Delta} {}^{S-1}C_x \Big(\frac{1+p}{2}\Big)^{S-1-x} \Big(\frac{1-p}{2}\Big)^{x} \tag{3.52}$$

and soundness

$$\max_k \frac{k}{2^{k-1}S} \sum_{x=0}^{\Delta} \sum_{y=0}^{\Delta-x} {}^{S-k}C_x \, {}^{k-1}C_y \Big(\frac{1+p}{2}\Big)^{S-k-x} \Big(\frac{1-p}{2}\Big)^{x}. \tag{3.53}$$

Proof. We now have

$$\begin{gathered}
(\mathbb{1}-\Pi)\Pi = 0, \;\; (\mathbb{1}-\Pi)\Pi^\perp = \Pi^\perp, \\
\Big(\frac{\mathbb{1}+p\Pi}{2}\Big)\Pi = \Big(\frac{1+p}{2}\Big)\Pi, \;\; \Big(\frac{\mathbb{1}+p\Pi}{2}\Big)\Pi^\perp = \frac{1}{2}\Pi^\perp, \\
\Big(\frac{\mathbb{1}-p\Pi}{2}\Big)\Pi = \Big(\frac{1-p}{2}\Big)\Pi, \;\; \Big(\frac{\mathbb{1}-p\Pi}{2}\Big)\Pi^\perp = \frac{1}{2}\Pi^\perp.
\end{gathered} \tag{3.54}$$

The completeness bound is given by

$$\mathrm{Tr}\left[\Pi_r \sum_{\substack{\mathcal{D}, \\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D}, \\ i\neq r}} \Big(\frac{\mathbb{1}+p\Pi}{2}\Big)_i \bigotimes_{\substack{i\in\mathcal{D}, \\ i\neq r}} \Big(\frac{\mathbb{1}-p\Pi}{2}\Big)_i \bigotimes_S \Pi\right] = \sum_{x=0}^{\Delta} {}^{S-1}C_x \Big(\frac{1+p}{2}\Big)^{S-1-x} \Big(\frac{1-p}{2}\Big)^{x}. \tag{3.55}$$

To calculate the soundness bound, from Equation (3.15) our Q is now given by

$$Q = \frac{1}{S}\sum_{r=1}^{S}(\mathbb{1}-\Pi)_r \sum_{\substack{\mathcal{D},\\ |\mathcal{D}|\leq\Delta}} \bigotimes_{\substack{i\notin\mathcal{D},\\ i\neq r}} \left(\frac{\mathbb{1}+p\Pi}{2}\right)_i \bigotimes_{\substack{i\in\mathcal{D},\\ i\neq r}} \left(\frac{\mathbb{1}-p\Pi}{2}\right)_i. \tag{3.56}$$

In a similar way to the previous calculations, we determine a general expression for the eigenvalues of Q as

$$\begin{aligned} g(k,S,p,\Delta) &= \frac{k}{S}\sum_{x=0}^{\Delta}\sum_{y=0}^{\Delta-x} {}^{S-k}C_x\, {}^{k-1}C_y \left(\frac{1+p}{2}\right)^{S-k-x}\left(\frac{1-p}{2}\right)^{x}\left(\frac{1}{2}\right)^{k-1-y}\left(\frac{1}{2}\right)^{y} \\ &= \frac{k}{2^{k-1}S}\sum_{x=0}^{\Delta}\sum_{y=0}^{\Delta-x} {}^{S-k}C_x\, {}^{k-1}C_y \left(\frac{1+p}{2}\right)^{S-k-x}\left(\frac{1-p}{2}\right)^{x}. \end{aligned} \tag{3.57}$$

The soundness bound is then given by the maximum of this expression over all k.

□

3.8 Discussion

In this Chapter, we have analysed a simple approach to authenticated teleportation of a quantum message in a noisy network. We conclude by discussing the merits and drawbacks of our work, and future perspectives.

As in [38, 109], the interaction required in our protocol can be reduced by the players sharing private random classical keys that encode the stabiliser they measure in each round, the copy r that is used for the teleportation, and the allowed failure threshold Δ. Further, as mentioned previously, teleportation of the quantum state can be viewed as Alice sending a quantum message encrypted with the outcomes of her Bell state measurement.

Comparing with previous authentication schemes for quantum messages [38, 107, 108], our protocol, which consists of performing stabiliser measurements on many separate copies of the state, allows for a much easier experimental implementation. The existing schemes, on the other hand, use stabiliser error-correcting codes, with the number of qubits of the encoded state increasing with the desired security level. However, the tradeoff comes in

terms of security, where both types of schemes are ϵ-secure with $\epsilon = \frac{1}{S}$ for our protocol and scaling as 2^{-S} for protocols based on [38].

We will briefly comment on the difference between entanglement purification, used in [38], and our method of authenticating the quantum channel in teleportation. In entanglement purification, one starts out with many copies of a state and applies operations to transform it to a (fewer) number of copies of a maximally entangled state. In the cryptographic setting we consider, an untrusted source is creating copies that we do not assume anything about (notably, they may be different in each round). This facilitates the application of our scheme to other scenarios where an adversarial source creates untrusted entanglement.

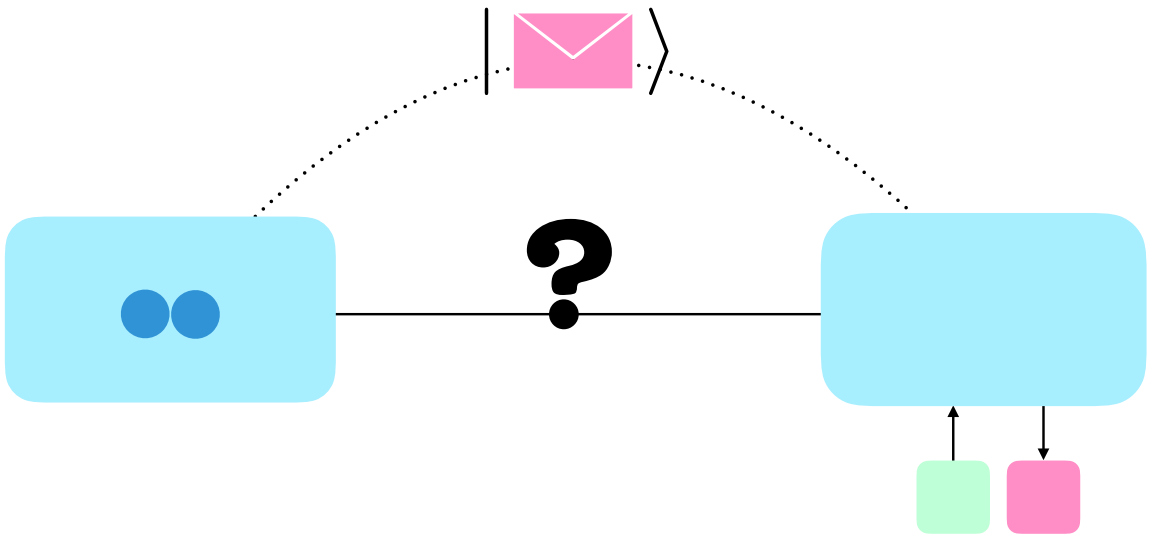
To demonstrate our protocol experimentally, one simply needs to generate many copies of a state, which is perfectly feasible with existing experimental setups. The noise tolerance of our protocol has been illustrated in terms of the tradeoff between the security bounds. Note that we have only considered noise in the authentication part of our scheme; we have assumed that the players can perform the teleportation perfectly once an authenticated quantum channel has been established. Future work could also incorporate noise in the teleportation procedure itself.

Finally, we showed that our analysis for noisy measurement devices can be extended to verification of graph states shared between a network of players. This has potential applications in the multitude of ways graph states are used across quantum information, be it for secret sharing [52], metrology [49], or blind quantum computation [37].

The work in this Chapter can be viewed as a starting point for the rest of this thesis. From now on, the amount of trust we place in our network will decrease. Chapter 4 goes a step further to look at authenticated teleportation with untrusted measurement devices. In Chapter 5, we apply verification techniques in the presence of dishonest players to build an anonymous quantum communication protocol. Finally, in Chapter 6, we take our network of players sharing graph states even further by allowing any number of them to be dishonest.

Chapter 4

Authenticated teleportation with one-sided trust



4.1 Introduction

Quantum teleportation is well-established as a cornerstone of the field of quantum information, allowing the transfer of a qubit from one player to another using an entangled pair and a classical communication channel [45]. While interesting in its own right, it is also a key ingredient in many protocols, such as secret sharing [48,68], anonymous transmission [73] and multiparty computation [70], and is an important tool across quantum information. From a cryptographic point of view, it is then vital to study the security of teleportation.

Continuing our work in the previous Chapter, here we consider *authenticated teleportation*, where the players wish to verify that the teleportation has succeeded even when they do not trust the entangled pair being used. This authenticates its application as a quantum channel between the two players. The capacity to certify or authenticate a successful teleportation will be significant for its use across quantum networks, computers and simulators.

As mentioned earlier, previous schemes for authentication of a quantum channel, such as [38], rely on generating large entangled states or performing entangling measurements. Guaranteeing high security of such protocols would need levels of entanglement that are, in practice, infeasible. In Chapter 3, we presented and investigated a protocol to achieve the same goal, but with much lower entanglement requirements. In this Chapter, we go one step further in solving this problem: allowing Alice and Bob to authenticate their quantum channel even without trusting their devices.

Device-independence has emerged as a highly desirable feature of quantum communication and computation protocols, from its early applications to quantum key distribution [90, 91, 113] and quantum random number generation [92, 114]. This approach addresses the situation where the untrusted components may have been obtained from, or be in the control of, an adversary. If not treated in this way, untrusted devices may lead to security loopholes such as, for example, susceptibility to physical attacks on the devices. Thus, device-independence represents the pinnacle of possible security.

In a two-player network, one can consider two trust settings: one-sided device-independent (1sDI), where Alice trusts her device but Bob does not (or vice versa), and fully device-

independent (DI), where neither player trusts their devices. One-sided trust should allow for a much simpler experimental implementation, as in [94, 95, 115]. This setting is particularly relevant when one player is naturally trusted; for example, a scenario with a trusted client but untrusted server, or simply if the channel and local measurement device are untrusted when one may wish to receive a resource (such as a magic state for computation, or a particular entangled state for metrology).

In this Chapter, we introduce a 1sDI protocol for authenticated teleportation. To achieve this, we investigate how to test the entangled state which will be used for the teleportation in a 1sDI way. For this purpose, we will use EPR-steering correlations (Section 2.4.1). Along the way, we will also present some results for the fully DI setting. Finally, we will argue that our protocol can be implemented with today's experimental capabilities. Building and analysing such a protocol will require ingredients from various subfields of verification, and so we will discuss the relevant previous work separately for each of these.

4.2 Network model

- *Players*: There are two players, Alice and Bob, both of whom are honest.
- *State*: The quantum state they share is untrusted. The players obtain the state they require from an untrusted source. An honest source produces the Bell state, $|\Phi^+\rangle$.
- *Operations*: Alice's measurement devices are trusted; Bob's measurement devices are untrusted and may not be performing the correct operations. The players are only required to perform local operations.
- *Classical channels*: The players share an authenticated classical channel, or a random secret key, which they can use to send classical information. (This ensures that our model lies in the authenticated communication setting.)

We will consider two trust levels for the untrusted components: in the iid setting, the source and devices are assumed to behave in the same way in each round, while in the non-iid

setting, they are free to behave differently in every round.

4.3 Building blocks

Let us now discuss how to construct a protocol for 1sDI authenticated teleportation in such a network. This task will require a few key ingredients. We will start by reviewing previous work in each of these areas, and further outline our contributions.

4.3.1 Self-testing

Firstly, we use the technique of *self-testing*, by which untrusted states and measurements can be characterised, in a device-independent scenario, by the exhibited correlations alone. From its beginnings by Mayers and Yao [34], self-testing results now encompass a variety of different states [35, 116–120], measurements [121–123], and trust settings [124, 125]. (For a thorough review on self-testing, see [126].) For our application to teleportation, we will focus on certifying the fidelity of the Bell state and the Pauli measurements.

By self-testing the Bell state, one can establish the closeness of an untrusted state with the Bell state, up to local isometry, from correlations such as the amount of violation of the CHSH inequality. While many self-testing results exist for the Bell state [35, 124, 127], only recently do we have techniques which are robust enough to be used in practice [122, 128, 129].

Self-testing a measurement certifies that, despite the possible presence of additional ancillae, the operators act close to ideally on the Bell state, and trivially on the rest of the system. This has not been as extensively covered in the literature. Existing bounds for the Pauli measurements have very low robustness [35, 124, 125]. Recent advances are not given in terms of a fidelity measure for the whole setup, but rather in the form of an effective commutator for each player's observables [121], or considering complementarity of observables [122]. Bowles et al. self-test all three Pauli observables, which requires dealing with the invariance of quantum correlations under complex conjugation [123]. However, no work so far has obtained a practically robust self-testing bound for the measurements.

To address this, we start by expanding on the 'SWAP method' introduced in [122, 128],

to derive full self-testing bounds for the Bell state that incorporate both the state and Pauli σ_X, σ_Z measurements, in both the 1sDI and DI settings. In this way, we obtain new bounds that are practically robust.

4.3.2 Extending self-testing to verification protocols

The results we obtain from self-testing are not immediately adapted to our requirements for several reasons. Firstly, they are based on the common self-testing assumptions of an infinite number of independent runs, throughout which the untrusted components behave identically (iid). In a realistic, adversarial scenario, we cannot rely on such assumptions, and so by adapting the methods of [124, 130], we remove these entirely.

In particular, in [124], Gheorghiu, Wallden and Kashefi take an analytical approach to self-testing in the 1sDI setting, using steering correlations. They derive bounds on the distance of the state from the ideal, as well as the finite number of copies required for verification in both the iid and non-iid scenarios, and apply this to the verification of quantum computing. However, their results are not robust enough to be implemented in practice, as they require at least 10^9 (10^{18}) copies of the state in the iid (non-iid) settings. In [130], Hajdušek, Pérez-Delgado and Fitzsimons consider self-testing with fourteen measurement settings, for the purpose of fully device-independent verifiable blind quantum computation, and purely in the non-iid scenario. In order to address our situation, we will use and adapt a combination of techniques from both of these works.

Secondly, as the security statements one achieves from self-testing refer to the states that have been measured, they cannot naively be used for ensuring the quality of the entangled pair used for teleportation. To address this, we incorporate a final, untested state in our analysis of the fidelity of teleportation, by adapting the techniques of [130]; the results in [124] are bounds on the tested states. Such an analysis marks a departure from the usual self-testing works, which certify a state already consumed in the testing process, as opposed to a state we wish to use. Recent work by Arnon-Friedman and Bancal [131] also considered this in their non-iid entanglement certification scheme; however, they focus on certifying

distillable entanglement, rather than quantifying the closeness of a state to the ideal.

4.3.3 Experiments on steering and nonlocality

To demonstrate the experimental feasibility of our protocol, we will give explicit values of the parameters we require to certify any fidelity of the teleportation; more specifically, both the number of states and the violation of the inequality required. We will argue that these results are within current experimental limitations [83, 111, 132–135]. Thus, before we begin, it is perhaps helpful to assess the state-of-the-art in nonlocality experiments. As we are interested in the 1sDI setting, we will focus more on steering. The steering inequality we will use has two measurement settings, and is given in Equation (2.40) by $|\langle A_0 B_0\rangle + \langle A_1 B_1\rangle| \leq \sqrt{2}$.

A photonic experiment by Saunders et al. [135] was the first to show steering in states which do not violate the Bell inequality (such states are said to be Bell-local), albeit without considering loopholes (Section 2.4). This was facilitated by their observation that using a steering inequality with a higher number of measurement settings improves the noise tolerance of steering. In addition, for the two-measurement steering inequality which has a maximum quantum violation of 2, they were able to observe a violation of around 1.68 using Werner states. Another demonstration of steering in Bell-local states without closing loopholes was performed by Orieux et al. [111]. Here, they demonstrated the steerability of a range of generalised Werner states of the form in Equation (3.41), using only two measurement settings, with the help of a steering inequality from [136]. By converting their experimental data to the form of the steering inequality in Equation (2.40), we found that the highest violation they managed to observe with a Werner state (subject to some noise and dephasing) was again around 1.68.

In terms of experiments that aim to close loopholes, we mention that of Wittmann et al. [137]. They violated the three-measurement-setting steering inequality while managing to close all three loopholes. They enforced space-like separation of the two players and used a fast quantum random number generator to close the locality and freedom-of-choice loopholes. To close the detection loophole, they modified the steering inequality to account for the

cases where no photon was detected. In this way, they observed a violation of 1.049 (the maximum quantum violation is 3). Smith et al. [138] took a similar approach to the no-detection events; however, by using highly efficient detectors, they observed a two-measurement-setting steering inequality violation of 1.14, and 1.74 for the three-measurement-setting case, in a detection-loophole-free manner. Bennet et al. [139] used from three to sixteen measurement settings, calculated a new bound on the relevant steering inequalities to depend on the heralding efficiency (in other words, the probability of detecting a photon), and experimentally showed its detection-loophole-free violation.

There has been a relative abundance of work on demonstrating violations of the CHSH inequality, perhaps most prominently in 2015 with the breakthrough loophole-free Bell tests [140–142]. Experiments in the Big Bell Test collaboration [83], notably that of Ringbauer and White, also reported high violations of up to 2.79 while closing the freedom-of-choice loophole. Other examples can be found, for example, in the works of [132, 133].

4.4 Self-testing by semidefinite programming

Let us now turn to our first goal: to derive full, robust self-testing bounds for the Bell pair $|\Phi^+\rangle$ and Pauli measurements σ_X, σ_Z, thus adding to the work of [125] in the 1sDI setting, and [122] in the DI setting. In order to do so, we will use the same framework as defined there.

In a device-independent scenario, one can only certify the state and measurements up to local isometry. Any local unitary transformation, or the presence of additional systems upon which the measurements act trivially, would result in the same correlations and so would not be detected. The dimension of the Hilbert space of the untrusted side is unrestricted; thus, we can take the state to be pure and the measurements to be projective, without loss of generality. Let us start by considering the 1sDI setting, and giving the definition of self-testing that we wish to make.

Definition 4.1. *Let $|\overline{\psi}\rangle$ denote the ideal Bell state $|\Phi^+\rangle$, and $\overline{M}_A, \overline{N}_B \in \{\sigma_X, \sigma_Z\}$ be the ideal Pauli measurements of Alice and Bob respectively. Let $|\psi\rangle$ denote the untrusted shared state, and $N_B \in \{X_B, Z_B\}$ be Bob's untrusted measurements. Given that the players observe a near-maximal violation $2-\epsilon$ of the steering inequality in Equation (2.40), we have achieved robust self-testing if there exists some isometry $\Phi : \mathcal{H}_B \to \mathcal{H}_B \otimes \mathcal{H}_{B'}$ such that*

$$F\big(\mathrm{Tr}_B\big[\Phi(|\psi\rangle\langle\psi|)\big], |\overline{\psi}\rangle\big) \geq 1 - f(\epsilon), \tag{4.1}$$

$$F\big(\mathrm{Tr}_B\big[\Phi(|\psi'\rangle\langle\psi'|)\big], \overline{M}_A \otimes \overline{N}_B |\overline{\psi}\rangle\big) \geq 1 - f'(\epsilon), \tag{4.2}$$

where $|\psi'\rangle = \overline{M}_A \otimes N_B |\psi\rangle$ and $f(\epsilon)$, $f'(\epsilon)$ are known simple functions of ϵ.

As is typical for self-testing statements, this bound effectively assumes an infinite number of iid copies of the state and measurements in order to approximate the violation and map it to the fidelity, and it is a statement on the state of the measured copies. We can define a similar statement for the DI setting, where now Alice's measurement M_A is also untrusted, using the CHSH inequality in Equation (2.37).

Our first aim is to determine forms of the functions $f(\epsilon), f'(\epsilon)$, for both the 1sDI and DI settings, that are practically robust, *i.e.* give a non-trivial fidelity for experimentally observable violations of the inequality. For Equation (4.1), such bounds for the state are already computed in [122, 125], by semidefinite programming (SDP) and the SWAP isometry. We will use their methods to derive new bounds which, for the measurements, are significantly more robust than previous analytical results [35, 124, 125]. Our results are given in Theorem 4.1.

Theorem 4.1. *(a) In the 1sDI setting, if the players observe a $2-\epsilon$ violation of the steering inequality in Equation (2.40), then $f(\epsilon) = 1.26\epsilon$, $f'(\epsilon) = 3.10\epsilon$.*

(b) In the DI setting, if the players observe a $2\sqrt{2}-\epsilon$ violation of the CHSH inequality in Equation (2.37), then $f(\epsilon) = 1.19\epsilon$, $f'(\epsilon) = 3.70\epsilon$.

Proof. Let us first give an outline of our proof. It is based on adapting the techniques of [122, 125], where by applying the SWAP isometry, we determine expressions for the fidelity measures in Equations (4.1) and (4.2). We write our fidelity measures and inequality

violations in terms of assemblage elements for the 1sDI setting, and expectation values of combinations of Alice and Bob's operators for the DI setting. Next, we introduce a positive semidefinite variable Γ, which is the moment matrix from the NPA hierarchy [100, 101], constructed such that now, the fidelity and inequality expressions can be written as a function of Γ. Since we wish to obtain a lower bound on the fidelity measures, we then use an SDP to find the minimum value of our expressions for Equations (4.1) and (4.2) which are compatible with the amount of violation of the inequality. As we shift from self-testing the state to the measurements, the size of Γ and the difficulty of the problem increases, particularly in constraining the structure of Γ. We solve this issue by automating the constraint generation step. Our full proof is given in the following subsections.

1. Fidelity expressions for 1sDI

Let us first look at how to get an expression for the fidelity of the self-testing. Here, we follow and extend the method of [125], using the SWAP isometry, which will later be fed into the SDP optimisation. We model Bob's untrusted device as a black box with measurement settings $\mathsf{y} \in \{0, 1\}$ and outcomes $\mathsf{b} \in \{0, 1\}$. Let us denote by $E_{\mathsf{b}|\mathsf{y}}$ the projector associated with Bob measuring in setting y and getting outcome b. Then, Alice's resulting conditional state is represented by the assemblage given by $\tau_{\mathsf{b}|\mathsf{y}} = \mathrm{Tr}_B(\mathbb{1}_A \otimes E_{\mathsf{b}|\mathsf{y}} |\psi\rangle \langle\psi|)$, which is equal to the resulting state times its probability. The untrusted measurements made by Bob are then written in terms of the projectors $E_{\mathsf{b}|\mathsf{y}}$ as $X_B = 2E_{0|1} - \mathbb{1}, Z_B = 2E_{0|0} - \mathbb{1}$.

The SWAP isometry $\Phi = \mathbb{1}_A \otimes \Phi_B$ (Figure 4.1), the standard in self-testing literature, performs the SWAP operation if the untrusted devices are operating correctly. It is composed of adding a trusted ancilla in a known state ($|+\rangle$) to Bob's subsystem, and then applying a unitary transformation which swaps part of the untrusted state onto the ancilla, resulting in a two-qubit state. The unitary transformation is written in such a way that it incorporates Bob's untrusted operators that we wish to test. Denoting Bob's system as B and his ancilla system

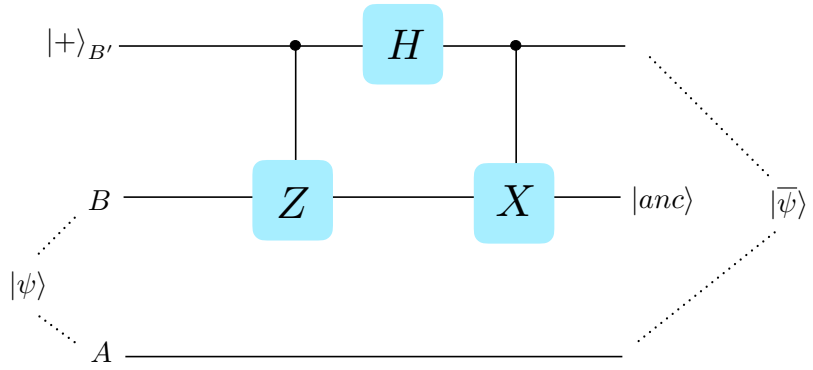


Figure 4.1: The SWAP isometry applied to Bob's system for self-testing the state $|\psi\rangle$.

as B', this transformation is given by VHU, where

$$V = |0\rangle\langle 0|_{B'} \otimes \mathbb{1}_B + |1\rangle\langle 1|_{B'} \otimes X_B, \tag{4.3}$$

$$H = |+\rangle\langle 0|_{B'} + |-\rangle\langle 1|_{B'}, \tag{4.4}$$

$$U = |0\rangle\langle 0|_{B'} \otimes \mathbb{1}_B + |1\rangle\langle 1|_{B'} \otimes Z_B. \tag{4.5}$$

The isometry then acts on the untrusted state as

$$\Phi(|\psi\rangle) = \mathbb{1}_A \otimes (VHU)_{B'B} |\psi\rangle_{AB} |+\rangle_{B'}. \tag{4.6}$$

To self-test the state, we will determine a bound on the fidelity $F(\mathrm{Tr}_B[\Phi(|\psi\rangle\langle\psi|)], |\overline{\psi}\rangle) = \langle\overline{\psi}| \mathrm{Tr}_B[\Phi(|\psi\rangle\langle\psi|)] |\overline{\psi}\rangle$. In addition, we wish to self-test the untrusted measurements N_B. To study this, we look at the action of the isometry given by

$$\Phi(\mathbb{1}_A \otimes N_B |\psi\rangle) = \mathbb{1}_A \otimes (VHU)_{B'B} \mathbb{1}_A \otimes N_B |\psi\rangle_{AB} |+\rangle_{B'}. \tag{4.7}$$

In the ideal case, we have $\mathbb{1}_A \otimes \overline{N}_B |\overline{\psi}\rangle$. We will determine the closeness between these two expressions, and denoting $|\psi'\rangle = \overline{M}_A \otimes N_B |\psi\rangle$, we will compute a bound on the fidelity $F(\mathrm{Tr}_B[\Phi(|\psi'\rangle\langle\psi'|)], \overline{M}_A \otimes \overline{N}_B |\overline{\psi}\rangle)$. Our fidelity expressions will be in terms of assemblages on Alice's side, given by $\tau_{b|y} = \mathrm{Tr}_B(\mathbb{1}_A \otimes E_{b|y} |\psi\rangle\langle\psi|)$. The full forms of the expressions we obtain in this way are given in Table 4.1. (Note that, for example,

To test	*Fidelity expression*
State	$\frac{1}{2}\Big[\langle 0_A\vert\,\tau_{0\vert 0}\,\vert 0_A\rangle + \langle 0_A\vert\,(2\tau_{0\vert 1,0\vert 0} - 2\tau_{0\vert 0,0\vert 1,0\vert 0})\,\vert 1_A\rangle$ $+ \langle 1_A\vert\,(2\tau_{0\vert 0,0\vert 1} - 2\tau_{0\vert 0,0\vert 1,0\vert 0})\,\vert 0_A\rangle + \langle 1_A\vert\,(\rho_A - \tau_{0\vert 0})\,\vert 1_A\rangle\Big]$
Z_B	$\frac{1}{2}\Big[\langle 0_A\vert\,\tau_{0\vert 0}\,\vert 0_A\rangle + \langle 0_A\vert\,(2\tau_{0\vert 1,0\vert 0} - 2\tau_{0\vert 0,0\vert 1,0\vert 0})\,\vert 1_A\rangle$ $+ \langle 1_A\vert\,(2\tau_{0\vert 0,0\vert 1} - 2\tau_{0\vert 0,0\vert 1,0\vert 0})\,\vert 0_A\rangle + \langle 1_A\vert\,(\rho_A - \tau_{0\vert 0})\,\vert 1_A\rangle\Big]$
X_B	$\frac{1}{2}\Big[\langle 0_A\vert\,(\rho_A - \tau_{0\vert 0} - 4\tau_{0\vert 1,0\vert 0,0\vert 1} + 2\tau_{0\vert 0,0\vert 1} + 2\tau_{0\vert 1,0\vert 0})\,\vert 0_A\rangle$ $+ \langle 0_A\vert\,(-2\tau_{0\vert 0,0\vert 1} + 4\tau_{0\vert 0,0\vert 1,0\vert 0,0\vert 1} + 4\tau_{0\vert 1,0\vert 0,0\vert 1,0\vert 0} + 4\tau_{0\vert 1,0\vert 0,0\vert 1}$ $- 2\tau_{0\vert 0,0\vert 1,0\vert 0} - 8\tau_{0\vert 1,0\vert 0,0\vert 1,0\vert 0,0\vert 1})\,\vert 1_A\rangle$ $+ \langle 1_A\vert\,(-2\tau_{0\vert 1,0\vert 0} + 4\tau_{0\vert 0,0\vert 1,0\vert 0,0\vert 1} + 4\tau_{0\vert 1,0\vert 0,0\vert 1,0\vert 0} + 4\tau_{0\vert 1,0\vert 0,0\vert 1}$ $- 2\tau_{0\vert 0,0\vert 1,0\vert 0} - 8\tau_{0\vert 1,0\vert 0,0\vert 1,0\vert 0,0\vert 1})\,\vert 0_A\rangle$ $+ \langle 1_A\vert\,(4\tau_{0\vert 1,0\vert 0,0\vert 1} - 2\tau_{0\vert 0,0\vert 1} - 2\tau_{0\vert 1,0\vert 0} + \tau_{0\vert 0})\,\vert 1_A\rangle\Big]$

Table 4.1: Fidelity expressions for the 1sDI setting.

$\tau_{0|0,0|1,0|0} = \mathrm{Tr}_B(E_{0|0}E_{0|1}E_{0|0}\,|\psi\rangle\,\langle\psi|)$, and similarly for other such terms).

2. Fidelity expressions for DI

We use a similar framework for self-testing in the DI setting, following [122]. Since both Alice and Bob's devices are now untrusted, we apply the SWAP isometry to both players' systems to extract a Bell pair. In the DI case, we must now also consider Alice's projector $D_{\mathsf{a}|\mathsf{x}}$, such that the probability distribution is given by $p(\mathsf{a},\mathsf{b}|\mathsf{x},\mathsf{y}) = \mathrm{Tr}_{AB}(D_{\mathsf{a}|\mathsf{x}} \otimes E_{\mathsf{b}|\mathsf{y}}\,|\psi\rangle\,\langle\psi|)$. For ease of calculations, we now take the ideal state to be

$$|\overline{\psi}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) \\ \sin\left(\frac{\pi}{8}\right) \\ \sin\left(\frac{\pi}{8}\right) \\ -\cos\left(\frac{\pi}{8}\right) \end{bmatrix}, \tag{4.8}$$

which is equivalent to the Bell state up to local unitaries. This state maximally violates the CHSH inequality if Alice and Bob measure the σ_Z, σ_X operators, which simplifies our analysis. The isometry $\Phi = \Phi_A \otimes \Phi_B$ performs the same SWAP operation here, but we write it slightly differently to follow [122]. The ancilla on both players' systems A', B' is initialised in state $|0\rangle$, and the unitary transformation is now written as VRV, where V is defined as before and R is given by

$$R = \mathbb{1}_{A'} \otimes \left(\frac{\mathbb{1}_A + Z_A}{2}\right) + \sigma_{X_{A'}} \otimes \left(\frac{\mathbb{1}_A - Z_A}{2}\right) \tag{4.9}$$

on Alice's side, for example. For self-testing the state, we then have

$$\Phi(|\psi\rangle) = (VRV)_{A'A} \otimes (VRV)_{B'B} |\psi\rangle_{AB} \otimes |00\rangle_{A'B'} . \tag{4.10}$$

The fidelity is given by $F(\mathrm{Tr}_{AB}[\Phi(|\psi\rangle\langle\psi|)], |\overline{\psi}\rangle) = \langle\overline{\psi}| \mathrm{Tr}_{AB}\left[\Phi(|\psi\rangle\langle\psi|)\right] |\overline{\psi}\rangle$. For self-testing the measurements, we now denote Alice's untrusted measurement operator as M_A and $|\psi'\rangle = M_A \otimes N_B |\psi\rangle$. After applying the isometry, we have

$$\Phi(M_A \otimes N_B |\psi\rangle) = (VRV)_{A'A} \otimes (VRV)_{B'B} M_A \otimes N_B |\psi\rangle_{AB} |00\rangle_{A'B'} . \tag{4.11}$$

The action of the ideal operators on the ideal state gives $|\overline{\psi'}\rangle = \overline{M}_A \otimes \overline{N}_B |\overline{\psi}\rangle$. The fidelity is then given by $F(\mathrm{Tr}_{AB}[\Phi(|\psi'\rangle\langle\psi'|)], \overline{M}_A \otimes \overline{N}_B |\overline{\psi}\rangle) = \langle\overline{\psi'}| \mathrm{Tr}_{AB}[\Phi(|\psi'\rangle\langle\psi'|)] |\overline{\psi'}\rangle$. The full forms of the fidelity expressions we obtain in this way are given in Table 4.2.

3. Constraints

Our next aim is to determine a bound on the fidelity measures in Tables 4.1 and 4.2, given an ϵ-near-maximal violation of the steering or CHSH inequalities. In the 1sDI setting, these inequalities can be written in the form of Alice's trusted operators σ_X, σ_Z acting on assemblages that result from Bob measuring his untrusted operators X, Z. The CHSH inequality may also be used in the 1sDI setting to witness steering. We can write these inequalities in terms of

assemblages on Alice's side as

$$\text{Tr}[\sigma_Z(2\tau_{0|0} - \rho_A) + \sigma_X(2\tau_{0|1} - \rho_A)] = 2 - \epsilon, \tag{4.12}$$

$$\text{Tr}[\sqrt{2}\sigma_Z(2\tau_{0|0} - \rho_A) + \sqrt{2}\sigma_X(2\tau_{0|1} - \rho_A)] = 2\sqrt{2} - \epsilon, \tag{4.13}$$

for steering and CHSH, respectively. In the DI case, where both players' devices are untrusted, they must demonstrate nonlocality by violating the CHSH inequality.

4. Finding a bound via SDP

We then use an SDP to find the minimum value of our fidelity expression consistent with the amount of violation of the inequality. It is formulated as follows:

$$\begin{aligned} &\text{minimise} && \text{Tr}(P\Gamma) \\ &\text{such that} && \text{Tr}(Q\Gamma) = w \\ & && \Gamma \geq 0. \end{aligned} \tag{4.14}$$

Here, Γ is the moment matrix from the NPA hierarchy for characterising quantum correlations [100, 101]. In the 1sDI setting, the rows of Γ are given by a set of operators that are some product of Bob's projectors $E_{\mathsf{b}|\mathsf{y}}$ written as $\{\mathcal{E}_1, ..., \mathcal{E}_\nu\}$, the columns by the adjoints, and each element by $\Gamma_{k,l} = \text{Tr}_B(\mathcal{E}_l^\dagger \mathcal{E}_k \left|\psi\right\rangle \left\langle\psi\right|)$. Thus, Γ is a $\nu \times \nu$ matrix composed of assemblage elements. In the DI setting, the rows of Γ are given by a set of operators that are some combination of both Alice and Bob's operators A_k, B_k, which results in its elements being expectation values. It has been proven in [122, 125] that Γ is positive semidefinite.

Our constraint is then given by the amount of violation w of a suitable inequality. Formulating our problem in terms of an SDP essentially amounts to finding a suitable form of Γ that contains all the elements in our fidelity and inequality expressions, writing these expressions in terms of symmetric matrices P, Q acting on Γ, and constraining the structure of Γ.

For self-testing the measurements, this final step is the most time-consuming. For example, in the case of self-testing the $X \otimes X$ measurement in the DI scenario, to solve the SDP we

To test	*Fidelity expression*
State	$\frac{1}{2}\Big[\frac{1}{2}+\frac{1}{2\sqrt{2}}\langle Z_AZ_B\rangle+\frac{1}{4\sqrt{2}}\langle Z_AX_B\rangle+\frac{1}{4\sqrt{2}}\langle X_AZ_B\rangle-\frac{1}{8\sqrt{2}}\langle X_AX_B\rangle-\frac{1}{8}\langle Z_AX_AZ_BX_B\rangle$ $-\frac{1}{8}\langle X_AZ_AX_BZ_B\rangle+\frac{1}{8}\langle X_AZ_AZ_BX_B\rangle+\frac{1}{8}\langle Z_AX_AX_BZ_B\rangle+\frac{1}{8\sqrt{2}}\langle Z_AX_AZ_AX_B\rangle$ $+\frac{1}{8\sqrt{2}}\langle X_AZ_BX_BZ_B\rangle-\frac{1}{4\sqrt{2}}\langle Z_AX_AZ_AZ_B\rangle-\frac{1}{4\sqrt{2}}\langle Z_AZ_BX_BZ_B\rangle$ $-\frac{1}{8\sqrt{2}}\langle Z_AX_AZ_AZ_BX_BZ_B\rangle\Big]$
$Z_A\otimes Z_B$	$\frac{1}{2}\Big[\frac{1}{2}+\frac{1}{2\sqrt{2}}\langle Z_AZ_B\rangle+\frac{1}{4\sqrt{2}}\langle Z_AX_B\rangle+\frac{1}{4\sqrt{2}}\langle X_AZ_B\rangle-\frac{1}{8\sqrt{2}}\langle X_AX_B\rangle-\frac{1}{8}\langle Z_AX_AZ_BX_B\rangle$ $-\frac{1}{8}\langle X_AZ_AX_BZ_B\rangle+\frac{1}{8}\langle X_AZ_AZ_BX_B\rangle+\frac{1}{8}\langle Z_AX_AX_BZ_B\rangle+\frac{1}{8\sqrt{2}}\langle Z_AX_AZ_AX_B\rangle$ $+\frac{1}{8\sqrt{2}}\langle X_AZ_BX_BZ_B\rangle-\frac{1}{4\sqrt{2}}\langle Z_AX_AZ_AZ_B\rangle-\frac{1}{4\sqrt{2}}\langle Z_AZ_BX_BZ_B\rangle$ $-\frac{1}{8\sqrt{2}}\langle Z_AX_AZ_AZ_BX_BZ_B\rangle\Big]$
$X_A\otimes X_B$	$\frac{1}{2}\Big[\frac{1}{2}-\frac{1}{8\sqrt{2}}\langle X_AX_B\rangle-\frac{1}{4\sqrt{2}}\langle X_AZ_AX_AX_B\rangle-\frac{1}{4\sqrt{2}}\langle X_AX_BZ_BX_B\rangle-\frac{1}{8}\langle Z_AX_AZ_BX_B\rangle$ $-\frac{1}{8}\langle X_AZ_AX_BZ_B\rangle+\frac{1}{8}\langle X_AZ_AZ_BX_B\rangle+\frac{1}{8}\langle Z_AX_AX_BZ_B\rangle+\frac{1}{2\sqrt{2}}\langle X_AZ_AX_AX_BZ_BX_B\rangle$ $+\frac{1}{8\sqrt{2}}\langle X_AZ_AX_AZ_AX_AX_B\rangle+\frac{1}{8\sqrt{2}}\langle X_AX_BZ_BX_BZ_BX_B\rangle$ $+\frac{1}{4\sqrt{2}}\langle X_AZ_AX_AZ_AX_AX_BZ_BX_B\rangle+\frac{1}{4\sqrt{2}}\langle X_AZ_AX_AX_BZ_BX_BZ_BX_B\rangle$ $-\frac{1}{8\sqrt{2}}\langle X_AZ_AX_AZ_AX_AX_BZ_BX_BZ_BX_B\rangle\Big]$
$Z_A\otimes X_B$	$\frac{1}{2}\Big[\frac{1}{2}+\frac{1}{4\sqrt{2}}\langle Z_AX_B\rangle-\frac{1}{8\sqrt{2}}\langle X_AX_B\rangle+\frac{1}{8\sqrt{2}}\langle Z_AX_AZ_AX_B\rangle-\frac{1}{2\sqrt{2}}\langle Z_AX_BZ_BX_B\rangle$ $-\frac{1}{4\sqrt{2}}\langle X_AX_BZ_BX_B\rangle-\frac{1}{8}\langle Z_AX_AZ_BX_B\rangle-\frac{1}{8}\langle X_AZ_AX_BZ_B\rangle+\frac{1}{8}\langle X_AZ_AZ_BX_B\rangle$ $+\frac{1}{8}\langle Z_AX_AX_BZ_B\rangle+\frac{1}{4\sqrt{2}}\langle Z_AX_AZ_AX_BZ_BX_B\rangle-\frac{1}{4\sqrt{2}}\langle Z_AX_BZ_BX_BZ_BX_B\rangle$ $+\frac{1}{8\sqrt{2}}\langle X_AX_BZ_BX_BZ_BX_B\rangle-\frac{1}{8\sqrt{2}}\langle Z_AX_AZ_AX_BZ_BX_BZ_BX_B\rangle\Big]$

Table 4.2: Fidelity expressions for the DI setting.

require a Γ of size 81×81, which has over $22,000$ constraints. To work around this problem, we have automated the process of generating Γ and its constraints, using a combination of C++ and Python scripts. Our code takes as input the rows and columns of Γ. It then generates all elements of Γ, determines which elements are equal to one another, and after

	Method	*Trust*	*Inequality*	*State bound*	*State + meas. bound*
Reichardt et al. [127]	analytical	DI	CHSH	$320\sqrt{\epsilon}$	
McKague et al. [35]	analytical	DI	CHSH	$10.9\epsilon^{1/4} + 3.6\sqrt{\epsilon}$	$10.9\epsilon^{1/4} + 13.1\sqrt{\epsilon}$
Kaniewski [129]	analytical	DI	CHSH	$1.18\sqrt{\epsilon}$	
Bancal et al. [122]	numerical	DI	CHSH	$1.48\sqrt{\epsilon}$	
Gheorghiu et al. [124]	analytical	1sDI	steering	$2.8\sqrt{\epsilon} + 0.5\epsilon$	$10.8\sqrt{\epsilon} + 0.5\epsilon$
Šupić et al. [125]	numerical	1sDI	CHSH	$1.34\sqrt{\epsilon}$	
This work	numerical	1sDI	steering	$1.59\sqrt{\epsilon}$	$2.49\sqrt{\epsilon}$
		1sDI	CHSH	$1.34\sqrt{\epsilon}$	$2.10\sqrt{\epsilon}$
		DI	CHSH	$1.54\sqrt{\epsilon}$	$2.72\sqrt{\epsilon}$

Table 4.3: New and existing bounds on trace distance, given an ϵ-near-maximal violation of the inequality. The state bound gives an upper bound on $\left\|\Phi(|\psi\rangle) - |\overline{\psi}\rangle \otimes |anc\rangle\right\| \leq \sqrt{2f(\epsilon)}$, while the state and measurements bound gives an upper bound on $\left\|\Phi(M_A \otimes N_B\,|\psi\rangle) - (\overline{M}_A \otimes \overline{N}_B\,|\overline{\psi}\rangle) \otimes |anc\rangle\right\| \leq \sqrt{2f'(\epsilon)}$, where the relation between the bounds is calculated from Equation (39) of [122]. In the 1sDI case, $M_A = \overline{M}_A$, since we trust Alice's measurement devices.

some processing, outputs a list of all the unique constraints, in a format that can be directly entered into our SDP.

Once our SDP is set up, we solve it via CVX [143, 144], giving the bounds in Theorem 4.1. (For more details of the SDP calculations, see Appendix 4.A.1.)

□

An alternative form of our bounds is given in Table 4.3, for comparison with the literature. Let us now denote the constant term by α, such that the bounds in Theorem 4.1 can be written as $f(\epsilon)$, $f'(\epsilon) = \alpha\epsilon$, where α depends on the trust setting, inequality, and whether we wish to use the self-testing bound for the state, or both state and measurements.

4.5 Protocol

We are now ready to build our protocol for authenticated teleportation with untrusted devices. As mentioned, we cannot directly apply our results from Theorem 4.1, as they are valid under the assumptions of an infinite number of iid rounds (appearing in the use of expectation values in the SDP). In any experiment, by doing a finite number of runs we can only get an estimation of the expectation values required for our inequality. Thus, if we want to use Theorem 4.1 to propose a realistic verification protocol, we must also determine the number of runs required to approximate the expectation values to our desired precision. We start by considering the case of the iid assumption, and then remove this altogether for the fully adversarial setting. In this way, we define a scheme for 1sDI authenticated teleportation in Protocol 4.1.

The main idea of Protocol 4.1 is as follows. The source is asked for many copies of the Bell pair. One copy is randomly chosen that will be used, and the rest are tested for steering using the inequality in Equation (2.40). If it passes, the remaining pair is used to teleport. If the source and devices behave as they should, the tests will always pass, and the teleported state is perfect. On the other hand, if the source is dishonest, it cannot know which pair will be used and which pairs will be tested, and so if it supplies non-ideal states, it will sometimes fail the test. Further, the self-testing statements for the test mean that Bob's security holds even with untrusted devices on Bob's side.

There is some flexibility in the protocol which would not affect our results. For example, we have written it such that Alice chooses the copy r, and essentially runs the protocol, but this can be easily changed to Bob, or a third party. Furthermore, as in [38, 109], it is possible to make the protocol less interactive by replacing the communication between Alice and Bob with shared random strings, indicating which copy to use for the teleportation, and which measurement setting to test each copy with.

Protocol 4.1 ONE-SIDED DEVICE-INDEPENDENT AUTHENTICATED TELEPORTATION

Input: Parameters ϵ, q, x are agreed, depending on the experimental limitations, and the fidelity of teleportation that the players wish to certify.

Goal: Alice teleports $|\phi\rangle$ to Bob through an authenticated channel without trusting Bob's devices.

1: The source is instructed to prepare

- $S = \lceil \frac{4q^2x}{\epsilon^2} \ln \frac{1}{\epsilon} + 1 \rceil$ Bell pairs in the iid setting, or
- $S = \lceil \frac{16q^2x}{\epsilon^2} \ln \frac{1}{\epsilon} + 1 \rceil$ Bell pairs in the non-iid setting,

and send the shares to Alice and Bob.

2: Alice randomly chooses a copy r to be used for the teleportation, and sends the value r to Bob.

3: Alice randomly divides the set of remaining copies into two subsets, $\mathbb{Q}_0$ and $\mathbb{Q}_1$, each of size $\frac{S-1}{2}$.

4: For each copy $i \in \mathbb{Q}_t$:

(a) Alice measures observable A_t and gets outcome a_i.

(b) She tells Bob to measure observable B_t and he gets outcome b_i.

(c) Alice and Bob calculate their correlation for round i as $\hat{C}_i = a_i b_i$.

5: Alice and Bob calculate their average correlation over all rounds.

6: If their average correlation has deviation ϵ from maximal violation of the steering inequality in Equation (2.40), Alice uses copy r to teleport $|\phi\rangle$ to Bob using Protocol 2.1.

4.6 Security analysis

Theorem 4.2 then characterises the final untested state that is used as the quantum resource for teleportation in Step 6 of Protocol 4.1, for both the case where we assume an iid source and the non-iid setting. Our proof for the non-iid case is based on techniques from [124] to certify the fidelity of the state of a randomly chosen copy r, as opposed to at least one state as in [122].

Theorem 4.2. *(a) In the iid setting, the fidelity of the copy r used for teleportation in Protocol 4.1 is bounded (up to local isometry) with probability at least $(1-\epsilon^x)$ by*

$$F \geq 1 - \alpha\Big[\frac{2\epsilon}{q} + \epsilon\Big], \tag{4.15}$$

where $\alpha = 1.26$.

(b) In the non-iid setting, the fidelity of the averaged state of copy r used for teleportation in Protocol 4.1 is bounded (up to local isometry) with probability at least $(1-\epsilon^x)$ by

$$F \geq 1 - \alpha\Big[\frac{2\epsilon}{q} + \frac{\epsilon}{2} + \frac{4q^2 x\epsilon \ln\frac{1}{\epsilon} + 2\epsilon^2}{8q^2 x \ln\frac{1}{\epsilon} + \epsilon^2}\Big], \tag{4.16}$$

where $\alpha = 1.26$.

Proof. Let us start by giving a proof outline. In Protocol 4.1, the final copy is accepted in Step 6 if, for all previous tested copies, the measured average correlation was ϵ-close to the correlation for an ideal copy. Our aim is to use this information to bound the fidelity of the final untested state that we wish to use for teleportation. First, following the method of [124], we determine the closeness between the true correlation (*i.e.* the expectation value) and the ideal correlation, using this measured correlation. In the iid case, we do this by taking the measurement outcomes to be independent random variables, and then using the Chernoff-Hoeffding bound [145, 146]. In the non-iid case, we instead use the martingale approach of Pironio et al. [114] and apply the Azuma-Hoeffding inequality [146, 147]. In our analysis, we also take into account the untested state r, which is straightforward if we assume an iid source. For the non-iid case, we do this by considering the maximum hypothetical deviation from the ideal correlation as in [130]. At this stage, we have an expression for the amount of violation of our steering inequality from the measured average correlations. Then, we apply our result from Theorem 4.1 to bound the fidelity of the average state over all copies, including state r which is used for teleportation. In the iid setting, this is a bound on any state prepared by the source. Further, we introduce the parameters q, x in order to tailor our protocol to possible experimental implementations, depending on the relative ease of

generating many states or observing a high violation of the inequality.

We will now give the full proof. Let us assume Alice and Bob share S copies, which are partitioned into m copies used for testing, and one copy used for teleportation. For each copy, Alice and Bob measure either $X \otimes X$ or $Z \otimes Z$. Note that although we use an untested copy for teleportation, we will include this in our analysis as a 'hypothetical measurement'. Since half of the copies are measured in $X \otimes X$ and the other half in $Z \otimes Z$ in each test round, we have the number of tested copies measured in either basis as $m_{XX} = m_{ZZ} = \frac{m}{2}$. For now, we will assume that a copy measured in $X \otimes X$ is used for teleportation and the others for testing, and the copies measured in $Z \otimes Z$ are only used for testing. (We will see later that this assumption does not affect the results.) We also partition S into S_{XX} and S_{ZZ}, which are the total number of copies measured in each respective basis. Then, we have

$$S_{XX} = m_{XX} + 1 = \frac{m+2}{2}, \quad S_{ZZ} = m_{ZZ} = \frac{m}{2}. \tag{4.17}$$

The *ideal correlation* for a copy measured in the basis $X \otimes X$ is given by $\mu_{XX} = \langle\overline{\psi}|\sigma_X \otimes \sigma_X|\overline{\psi}\rangle$, and similarly for $Z \otimes Z$. Note that $\mu_{XX} + \mu_{ZZ} = 2$. The *measured correlation* in round i is denoted by $\hat{C}_i = a_i b_i$, where $a_i, b_i \in \{+1, -1\}$ are Alice and Bob's measurement outcomes. The average measured correlation can be written in terms of the deviation from the ideal correlation, denoted by $\epsilon_{XX}, \epsilon_{ZZ}$ for the tested copies, and ϵ'_{XX} for the copy r used for teleportation, as

$$\begin{aligned}
\frac{1}{S_{XX}} \sum_{i=1}^{S_{XX}} \hat{C}_i &= \frac{1}{S_{XX}} \Big[\sum_{i=1}^{m_{XX}} \hat{C}_i + \hat{C}_r \Big] \\
&= \frac{1}{S_{XX}} \Big[m_{XX}(\mu_{XX} - \epsilon_{XX}) + \mu_{XX} - \epsilon'_{XX} \Big], \qquad (4.18) \\
\frac{1}{S_{ZZ}} \sum_{i=1}^{S_{ZZ}} \hat{C}_i &= \frac{1}{S_{ZZ}} \Big[\sum_{i=1}^{m_{ZZ}} \hat{C}_i \Big] \\
&= \frac{1}{S_{ZZ}} \Big[m_{ZZ}(\mu_{ZZ} - \epsilon_{ZZ}) \Big]. \qquad (4.19)
\end{aligned}$$

Using our tested copies, the measured correlation showed a deviation ϵ from the ideal correla-

tion, giving $\epsilon = \epsilon_{XX} + \epsilon_{ZZ}$. Let us take $\epsilon_{XX} = \epsilon_{ZZ} = \frac{\epsilon}{2}$, noting however that any other choice does not have a significant effect on our results. We will discuss the hypothetical deviation separately for the iid and non-iid cases.

The *true correlation*, or expectation value, in a round i where $X \otimes X$ is measured is denoted by $C_i = \text{Tr}(X \otimes X \rho_i)$, and similarly for $Z \otimes Z$, where ρ_i is the shared state in that round. Given the ϵ-closeness between the ideal and measured correlation, we now compute the closeness between the ideal and true correlation over the copies measured in $X \otimes X$ and $Z \otimes Z$ separately. We can then apply our self-testing result from Theorem 4.1 to bound the fidelity of the state. At first, we will assume iid, and then remove this assumption for the most general scenario.

(a) iid setting

In the iid setting, the untrusted components are assumed to behave the same way in each round. This implies that the hypothetical correlation of the untested copy will be the same as a tested copy ($\epsilon'_{XX} = \epsilon_{XX}$). (Note that this would be the same if we had used a copy measured in $Z \otimes Z$ for the teleportation.) Substituting in Equations (4.18) and (4.19), we get

$$\frac{1}{S_{XX}} \sum_{i=1}^{S_{XX}} \hat{C}_i = \mu_{XX} - \frac{\epsilon}{2}, \quad \frac{1}{S_{ZZ}} \sum_{i=1}^{S_{ZZ}} \hat{C}_i = \mu_{ZZ} - \frac{\epsilon}{2}. \tag{4.20}$$

Now, let us consider the rounds where $X \otimes X$ is measured. We start by defining a variable

$$W_j = \sum_{i=1}^{j} (\hat{C}_i - C_i), \text{ where } j \in \{1, ..., S_{XX}\}. \tag{4.21}$$

We use the Chernoff-Hoeffding bound for approximating the expectation value of independent random variables [145, 146]. We have $g_i \leq \hat{C}_i \leq h_i$, where $g_i = -1, h_i = 1$. This gives

$$\Pr(W_{S_{XX}} \geq \gamma) \leq \exp\left(-\frac{2\gamma^2}{\sum_{i=1}^{S_{XX}} (h_i - g_i)^2}\right) \leq \exp\left(-\frac{\gamma^2}{2S_{XX}}\right). \tag{4.22}$$

Since our focus is on developing a protocol that can be implemented in the lab, we will introduce parameters $q, x \geq 1$ that allow a tradeoff between the number of copies we can generate, and observing a high violation of the steering inequality. We choose $\gamma = S_{XX}\frac{\epsilon}{q}$, which gives

$$\begin{aligned}\Pr\Big(\frac{1}{S_{XX}}W_{S_{XX}} \geq \frac{\epsilon}{q}\Big) &= \Pr\Big(\frac{1}{S_{XX}}\big[\sum_{i=1}^{S_{XX}}\hat{C}_i - \sum_{i=1}^{S_{XX}}C_i\big] \geq \frac{\epsilon}{q}\Big) \\ &= \Pr\Big(\mu_{XX} - \frac{\epsilon}{2} - \frac{1}{S_{XX}}\sum_{i=1}^{S_{XX}}C_i \geq \frac{\epsilon}{q}\Big) \\ &\leq \exp\Big(-\frac{1}{2q^2}S_{XX}\epsilon^2\Big). \end{aligned} \tag{4.23}$$

Thus, we have

$$\Pr\Big(\frac{1}{S_{XX}}\sum_{i=1}^{S_{XX}}C_i - \mu_{XX} \geq -\frac{\epsilon}{q} - \frac{\epsilon}{2}\Big) \geq 1 - \exp\Big(-\frac{1}{2q^2}S_{XX}\epsilon^2\Big). \tag{4.24}$$

Similar calculations for the rounds where $Z \otimes Z$ is measured give us

$$\Pr\Big(\frac{1}{S_{ZZ}}\sum_{i=1}^{S_{ZZ}}C_i - \mu_{ZZ} \geq -\frac{\epsilon}{q} - \frac{\epsilon}{2}\Big) \geq 1 - \exp\Big(-\frac{1}{2q^2}S_{ZZ}\epsilon^2\Big). \tag{4.25}$$

Let $\rho_{avg} = \frac{1}{S}\sum_{i=1}^{S}\rho_i$ be the average state over all S copies, including the one used for teleportation. Since the states in each round are identical in the iid setting, we have $\rho_{avg} = \rho_i$. We define the following averaged true correlations:

$$C^{XX} = \frac{1}{S_{XX}}\sum_{i=1}^{S_{XX}}C_i, \quad C^{ZZ} = \frac{1}{S_{ZZ}}\sum_{i=1}^{S_{ZZ}}C_i. \tag{4.26}$$

We now rephrase Equations (4.24) and (4.25) as

$$\Pr\Big(C^{XX} - \mu_{XX} \geq -\frac{\epsilon}{q} - \frac{\epsilon}{2}\Big) \geq 1 - \exp\Big(-\frac{1}{4q^2}(m+2)\epsilon^2\Big), \tag{4.27}$$

$$\Pr\Big(C^{ZZ} - \mu_{ZZ} \geq -\frac{\epsilon}{q} - \frac{\epsilon}{2}\Big) \geq 1 - \exp\Big(-\frac{1}{4q^2}m\epsilon^2\Big). \tag{4.28}$$

The true correlation for the averaged state when measured in the $X \otimes X$ basis is given by $C^{XX} = \text{Tr}(X \otimes X \rho_{avg})$, and similarly for $Z \otimes Z$. Combining Equations (4.27) and (4.28),

$$\begin{aligned} C^{XX} + C^{ZZ} - (\mu_{XX} + \mu_{ZZ}) &\geq -\frac{2\epsilon}{q} - \frac{2\epsilon}{2} \\ C^{XX} + C^{ZZ} &\geq 2 - \left[\frac{2\epsilon}{q} + \epsilon\right] \\ &= 2 - \delta, \end{aligned} \tag{4.29}$$

with probability $\geq \left[1 - \exp\left(-\frac{1}{4q^2}(m+2)\epsilon^2\right)\right]\left[1 - \exp\left(-\frac{1}{4q^2}m\epsilon^2\right)\right]$, and where $\delta = \frac{2\epsilon}{q} + \epsilon$. If we set $m = \frac{4q^2x}{\epsilon^2}\ln\frac{1}{\epsilon}$, we get this probability to be $\gtrsim 1 - \epsilon^x$. Then, if $|\zeta\rangle$ is a purification of ρ_{avg},

$$\langle\zeta|X \otimes X|\zeta\rangle + \langle\zeta|Z \otimes Z|\zeta\rangle \geq 2 - \delta, \tag{4.30}$$

with probability $\geq 1 - \epsilon^x$. Our self-testing result in Theorem 4.1 tells us that given such a correlation in expectation values, we have for $\alpha = 1.26$,

$$F(\text{Tr}_B[\Phi(|\zeta\rangle\langle\zeta|)], |\overline{\psi}\rangle) \geq 1 - \alpha\delta, \tag{4.31}$$

with probability $\geq 1 - \epsilon^x$. It follows that

$$F(\text{Tr}_B[\Phi(\rho_{avg})], |\overline{\psi}\rangle) \geq 1 - \alpha\delta, \tag{4.32}$$

with probability $\geq 1 - \epsilon^x$. Recalling that $\rho_{avg} = \rho_i$ in the iid setting, we can rewrite this as the following bound on the fidelity of any copy, including that used for teleportation:

$$F(\text{Tr}_B[\Phi(\rho_i)], |\overline{\psi}\rangle) \geq 1 - \alpha\left[\frac{2\epsilon}{q} + \epsilon\right], \tag{4.33}$$

with probability $\geq 1 - \epsilon^x$. The total number of copies we need is then $S = \frac{4q^2x}{\epsilon^2}\ln\frac{1}{\epsilon} + 1$. Note that as $q, x \to \infty$, the expression for fidelity reduces to the self-testing result of $F \geq 1 - \alpha\epsilon$ with probability 1.

(b) Non-iid setting

Now, we no longer assume the same behaviour throughout the rounds. We first determine the hypothetical correlation of the untested copy, considering the worst case scenario, *i.e.* the maximum possible error. Since $\mu_{XX} = 1$, this then gives $\epsilon'_{XX} = 2$. (Note that we get this same value if we had used a copy measured in $Z \otimes Z$ for teleportation.) Substituting in Equations (4.18) and (4.19), we get

$$\frac{1}{S_{XX}} \sum_{i=1}^{S_{XX}} \hat{C}_i = \mu_{XX} - \left[\frac{8 + m\epsilon}{2m + 4}\right], \quad \frac{1}{S_{ZZ}} \sum_{i=1}^{S_{ZZ}} \hat{C}_i = \mu_{ZZ} - \frac{\epsilon}{2}. \tag{4.34}$$

Let us again start with $X \otimes X$. The true correlation C_i now depends on the history of the measurements made up to (but not including) round i, which we denote H_i, and so we can also write this as

$$C_i = \Pr(a_i = b_i | H_i) - \Pr(a_i \neq b_i | H_i). \tag{4.35}$$

We have $|W_{j+1} - W_j| \leq 2$, since $\hat{C}_i = \pm 1, -1 \leq C_i \leq 1$. The expectation value of W_j is finite, and the conditional expected value $E(W_{j+1}|H_{j+1}) = W_j$ for all $j \leq S_{XX}$. By fulfilling these conditions, our set of random variables $\{W_j\}$ is called a martingale. We can then use the Azuma-Hoeffding inequality [146, 147], which gives for $|W_{j+1} - W_j| \leq d_i$,

$$\Pr(W_{S_{XX}} \geq \gamma) \leq \exp\left(-\frac{\gamma^2}{2\sum_{i=1}^{S_{XX}} d_i^2}\right) \leq \exp\left(-\frac{\gamma^2}{8S_{XX}}\right). \tag{4.36}$$

We again choose $\gamma = S_{XX}\frac{\epsilon}{q}$, which gives

$$\Pr\left(\frac{1}{S_{XX}} \sum_{i=1}^{S_{XX}} C_i - \mu_{XX} \geq -\frac{\epsilon}{q} - \frac{8 + m\epsilon}{2m + 4}\right) \geq 1 - \exp\left(-\frac{1}{8q^2} S_{XX} \epsilon^2\right). \tag{4.37}$$

For $Z \otimes Z$, we get

$$\Pr\left(\frac{1}{S_{ZZ}} \sum_{i=1}^{S_{ZZ}} C_i - \mu_{ZZ} \geq -\frac{\epsilon}{q} - \frac{\epsilon}{2}\right) \geq 1 - \exp\left(-\frac{1}{8q^2} S_{ZZ} \epsilon^2\right). \tag{4.38}$$

We substitute for S_{XX}, S_{ZZ} and obtain $\langle\zeta|X\otimes X|\zeta\rangle + \langle\zeta|Z\otimes Z|\zeta\rangle \geq 2-\delta$ with probability $\geq \left[1-\exp\left(-\frac{1}{16q^2}(m+2)\epsilon^2\right)\right]\left[1-\exp\left(-\frac{1}{16q^2}m\epsilon^2\right)\right]$, and where $\delta = \frac{2\epsilon}{q}+\frac{\epsilon}{2}+\frac{8+m\epsilon}{2m+4}$. If we set $m = \frac{16q^2x}{\epsilon^2}\ln\frac{1}{\epsilon}$, we get this probability to be $\gtrsim 1-\epsilon^x$. Then, using our self-testing result from Theorem 4.1 with $\alpha = 1.26$, we get

$$F(\mathrm{Tr}_B[\Phi(\rho_{avg})], |\overline{\psi}\rangle) \geq 1-\alpha\delta, \tag{4.39}$$

with probability $\geq 1-\epsilon^x$. Here, ρ_{avg} is not equal to ρ_i, since we do not assume the source behaves the same way in each round. Thus, our statement certifying the fidelity holds for the average state, $\rho_{avg} = \frac{1}{S}\sum_{i=1}^{S}\rho_i$.

Writing δ in terms of ϵ, we have our final result that the state ρ_{avg} averaged over all copies, including the one used for teleportation, is such that

$$F(\mathrm{Tr}_B[\Phi(\rho_{avg})], |\overline{\psi}\rangle) \geq 1-\alpha\left[\frac{2\epsilon}{q}+\frac{\epsilon}{2}+\frac{4q^2x\epsilon\ln\frac{1}{\epsilon}+2\epsilon^2}{8q^2x\ln\frac{1}{\epsilon}+\epsilon^2}\right], \tag{4.40}$$

with probability $\geq 1-\epsilon^x$. The total number of copies required is then $S = \frac{16q^2x}{\epsilon^2}\ln\frac{1}{\epsilon}+1$.

□

The bound on the fidelity of teleportation follows from this, as given in Corollary 4.3.

Corollary 4.3. *The fidelity of teleportation (up to local isometry) in Protocol 4.1 is lower-bounded by Theorem 4.2.*

Proof. It is known that the fidelity of teleportation is at least as high as the fidelity of the entangled state used for teleportation [110]; thus, our bound on the entangled state also holds for the teleported state.

In the way that we propose our protocol above, a quantum memory is needed to store the copies until they are tested or used. To override this experimentally difficult requirement, the source can generate Bell pairs on-the-fly, and the players either test or use each pair depending on the chosen r. In this case, since we may not have checked for our desired inequality violation before the teleportation step (for example, if $r=1$ we immediately use

the state before any testing), we run the risk of teleporting through a bad quantum channel. However, once we know our inequality violation at the end of the protocol, we can compute a bound on the fidelity of the teleportation from Theorem 4.2.

Finally, we note that the CHSH inequality can also be used to witness steering. The analysis of Protocol 4.1 in this case, including the number of copies required, follows from the proof of Theorem 4.2 by applying the relevant self-testing result (see Appendix 4.A.2 for details).

4.7 Discussion and experimental feasibility

Bridging the gap between theoretical and experimental work in the field of device-independent quantum cryptography is a significant challenge in the progression of quantum technology [148]. This Chapter is an effort towards this, in the form of a practical protocol for 1sDI authenticated teleportation. We end by analysing our work in more detail.

First, we compare the security and resources required in our protocol alongside that of [38]. While the protocol in [38] has an exponential scaling with the security parameter, the size of the encoding, effectively the entanglement, increases with the desired security level. On the other hand, our protocol only uses multiple copies of the Bell pair. As we outline below, due to the ease of generating entangled pairs (compared to high entanglement), our protocol is practically feasible. Furthermore, our protocol is secure even in the case where devices are not trusted, which was not dealt with in [38].

Next, we discuss our self-testing results for the Pauli measurements, given as a fidelity measure. Using a steering inequality violation of at least 1.94 in the 1sDI case, or a CHSH violation of 2.78 in the DI case, one can certify a fidelity greater than 80%. As such high Bell violations have been observed, for example in [83, 134], our bounds are sufficiently robust to be experimentally useful.

To facilitate comparison with previous works, our bounds in Theorem 4.1 are given in the same form as the literature in Table 4.3. We see that we have improved upon all existing full self-testing bounds for the state and measurements in both the 1sDI and DI settings. Kaniewski's analytical approach [129] used a different isometry than SWAP and resulted in

a better bound for the state in the DI setting. Any improved self-testing bound can directly be used to bound the fidelity of teleportation in our protocol using Corollary 4.3 and the parameter α.

We will now assess the experimental feasibility of Protocol 4.1. Let us recall that our non-iid result is a bound on the fidelity of teleportation using an average, or typical, state, while the iid result is a bound on the fidelity of teleportation using any state. In order to improve upon teleportation by classical communication, we require the fidelity of teleportation to be greater than $\frac{2}{3}$ [149]. For example, 1sDI authenticated teleportation could be demonstrated by observing a steering inequality violation of 1.75 using 10^5 copies under the iid assumption, or 10^6 copies in a non-iid setting. If, instead, the CHSH inequality was used as the test, one would require a violation of 2.49 using with 10^6 (10^7) copies in the iid (non-iid) settings. (See Figure 4.2 in Appendix 4.A.2 for a plot of the full results.) The above results could be demonstrated using Werner states of visibility $v \geq 0.88$, which is well within experimental limitations. However, any implementation will also be subject to other imperfections and losses, such as in the photon detection efficiency. Using previous experimentally demonstrated violations of the steering inequality with two measurement settings [111, 135], one could certify a teleportation fidelity of at least 60%. The relative abundance of experimental work on the CHSH inequality shows that the number of copies and violation (even in the non-iid setting) required for our scheme could be demonstrated in existing laboratories, for example [83,132,133]. Additionally, the number of copies required by our finite analysis is sufficiently high so as to provide a good enough estimate of the quantum distribution, meaning that we do not need to employ regularisation methods as in [150]. Our scheme is thus the first authenticated teleportation protocol that is practical in its robustness, implementable with existing experimental setups, and further, tolerates untrusted devices.

Let us now comment on possible extensions of this work. Note that our protocol is a one-sided device-independent method of authenticating the quantum channel in teleportation. One can use our results to do a fully DI test of the Bell pair (the required parameters are in Appendix 4.A.2), but in order to build a fully device-independent teleportation scheme,

we must also consider self-testing of Alice's Bell state measurement. Recently, Renou et al. [151] and Bancal et al. [152] have focused on this particular problem, and considered an entanglement swapping-based approach to test the Bell state measurement. While [152] gives practically robust bounds, they assume iid and infinite runs, as is common in self-testing. Thus, we cannot directly apply these results to our protocol, and it remains as further work.

In this Chapter, we have implicitly assumed sufficiently high detection efficiencies so as not to worry about the detection loophole; an extension of our work that closes this loophole could take the no-detection events into account in the steering inequality, as was experimentally demonstrated in [137–139, 153]. These reported violations are not directly comparable with what we require, however, due to their use of this different steering inequality. Further, most experiments demonstrate steering with many more measurement settings than the two we have considered (some go up to even sixteen measurements), as this is simpler to do experimentally. In fact, investigating other steering inequalities, possibly with more measurement settings, could prove useful in further optimising our protocol for experimental implementation. We expect, however, that the development of 1sDI protocols will stimulate experimental efforts to achieve violations high enough for a loophole-free demonstration of our scheme in the near future. It is worth noting that for the CHSH inequality, it is already possible to achieve high violations while closing the detection loophole [133].

Finally, we emphasise that teleportation is not the only application of our work. Our results in Theorem 4.2 for the 1sDI setting, and in Appendix 4.A.2 for the DI setting, give a bound on the fidelity of the final untested state, which can then be used for a variety of other applications such as verified quantum computation. Our techniques can also be used in the certification of other states, in particular to extend self-testing results to the practical world.

4.A Appendix

4.A.1 Example SDPs for Theorem 4.1

We give some examples of our SDP method for self-testing the state and measurements, in the 1sDI setting with the steering inequality as a constraint. The SDP we solve is given by

$$\begin{aligned} &\text{minimise} \quad \text{Tr}(P\Gamma) \\ &\text{such that} \quad \text{Tr}(Q\Gamma) \geq 2-\epsilon \\ &\qquad\qquad \Gamma \geq 0, \end{aligned} \tag{4.41}$$

where:

State or Z operator

$$\Gamma = \begin{bmatrix} \rho_A & \tau_{0|0} & \tau_{0|1} & \tau_{0|0,0|1} \\ \tau_{0|0} & \tau_{0|0} & \tau_{0|1,0|0} & \tau_{0|0,0|1,0|0} \\ \tau_{0|1} & \tau_{0|0,0|1} & \tau_{0|1} & \tau_{0|0,0|1} \\ \tau_{0|1,0|0} & \tau_{0|0,0|1,0|0} & \tau_{0|1,0|0} & \tau_{0|0,0|1,0|0} \end{bmatrix},$$

$$Q = 2\begin{bmatrix} \frac{-\sigma_X-\sigma_Z}{2} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sigma_Z & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_X & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}, P = \frac{1}{2}\begin{bmatrix} W & \mathbf{0} & \mathbf{0} & V \\ \mathbf{0} & \sigma_Z & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ V^T & \mathbf{0} & \mathbf{0} & -2\sigma_X \end{bmatrix},$$

where $W = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, $V = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}$, $\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

X operator

$$\Gamma = \begin{bmatrix} \rho_A & \tau_{0|0} & \tau_{0|1} & \tau_{0|1,0|0} & \tau_{0|0,0|1} & \tau_{0|1,0|0,0|1} \\ \tau_{0|0} & \tau_{0|0} & \tau_{0|1,0|0} & \tau_{0|1,0|0} & \tau_{0|0,0|1,0|0} & \tau_{0|1,0|0,0|1,0|0} \\ \tau_{0|1} & \tau_{0|0,0|1} & \tau_{0|1} & \tau_{0|1,0|0,0|1} & \tau_{0|0,0|1} & \tau_{0|1,0|0,0|1} \\ \tau_{0|0,0|1} & \tau_{0|0,0|1} & \tau_{0|1,0|0,0|1} & \tau_{0|1,0|0,0|1} & \tau_{0|0,0|1,0|0,0|1} & \tau_{0|1,0|0,0|1,0|0,0|1} \\ \tau_{0|1,0|0} & \tau_{0|0,0|1,0|0} & \tau_{0|1,0|0} & \tau_{0|1,0|0,0|1,0|0} & \tau_{0|0,0|1,0|0} & \tau_{0|1,0|0,0|1,0|0} \\ \tau_{0|1,0|0,0|1} & \tau_{0|0,0|1,0|0,0|1} & \tau_{0|1,0|0,0|1} & \tau_{0|1,0|0,0|1,0|0,0|1} & \tau_{0|0,0|1,0|0,0|1} & \tau_{0|1,0|0,0|1,0|0,0|1} \end{bmatrix},$$

$$Q = 2 \begin{bmatrix} \frac{-\sigma_X - \sigma_Z}{2} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sigma_Z & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_X & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}, P = \frac{1}{2} \begin{bmatrix} A & \mathbf{0} & \mathbf{0} & D & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -\sigma_Z & \mathbf{0} & \mathbf{0} & \mathbf{0} & 4\sigma_X \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ D^T & \mathbf{0} & \mathbf{0} & P & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & -2\sigma_X & \mathbf{0} \\ \mathbf{0} & 4\sigma_X & \mathbf{0} & \mathbf{0} & \mathbf{0} & -8\sigma_X \end{bmatrix},$$

where $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $D = \begin{bmatrix} 2 & 0 \\ -2 & -2 \end{bmatrix}$, $P = \begin{bmatrix} -4 & 4 \\ 4 & 4 \end{bmatrix}$, $\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

In addition, we must enforce constraints on which elements of Γ are equal to each other in our SDP. To do this, we have written a combination of C++ and Python code. We then solve the SDP using the CVX package in Matlab [143, 144].

4.A.2 Results using the CHSH inequality

In the 1sDI setting of Protocol 4.1, the players can also use the CHSH inequality instead of the steering inequality. For such a case, we now state the analogous statement to Theorem 4.2 and Corollary 4.3, for which the proof follows by the same method as above.

Theorem 4.4. *Alice and Bob perform Protocol 4.1 but using the CHSH inequality. In the iid setting, if they share* $\frac{8q^2x}{\epsilon^2}\ln\frac{1}{\epsilon}+1$ *copies, then the fidelity of teleportation is bounded with probability at least* $(1-\epsilon^x)$ *by*

$$F \geq 1-\alpha\Big[\frac{4\epsilon}{q}+\epsilon\Big], \tag{4.42}$$

and in the non-iid setting, if they share $\frac{32q^2x}{\epsilon^2}\ln\frac{1}{\epsilon}+1$ *copies, then the fidelity of teleportation is bounded with probability at least* $(1-\epsilon^x)$ *by*

$$F \geq 1-\alpha\Big[\frac{4\epsilon}{q}+\frac{3\epsilon}{4}+\frac{4q^2x\epsilon\ln\frac{1}{\epsilon}+(2+\sqrt{2})\epsilon^2}{16q^2x\ln\frac{1}{\epsilon}+2\epsilon^2}\Big], \tag{4.43}$$

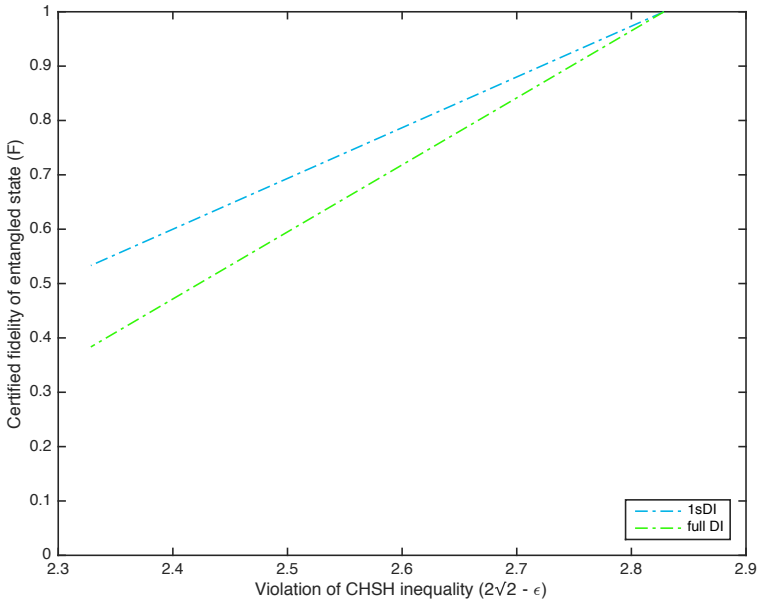
where $\alpha = 0.90$.

This value of α comes from the self-testing result we obtain from bounding the fidelity expression for the state in Table 4.1 with respect to the constraint in Equation (4.13).

Note that we do not use the fact that one player's devices may be trusted apart from when we apply the SDP result. Thus, in the DI setting, Theorem 4.4 holds, for the fidelity of the entangled state, with $\alpha = 1.19$, using the same number of copies as specified there. This can be used to do a fully device-independent test of the Bell pair, which would be useful for various applications.

In Figure 4.2, we compare the parameters required in the 1sDI and DI trust scenarios, under the iid and non-iid assumptions. In the 1sDI case, from Corollary 4.3, this fidelity bound holds for the fidelity of teleportation. In the DI case, one must also consider Alice's Bell state measurement in order to make such a statement; thus, this remains a bound on the entangled state.

(a)



(b)

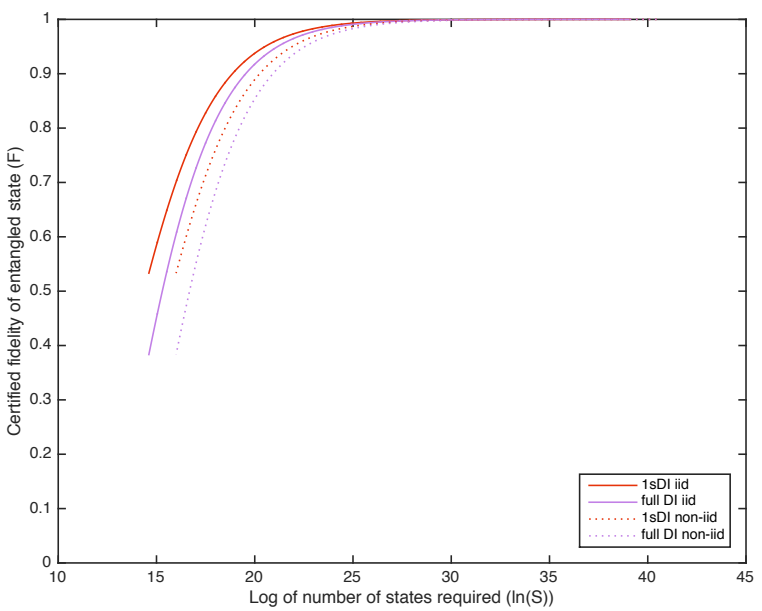
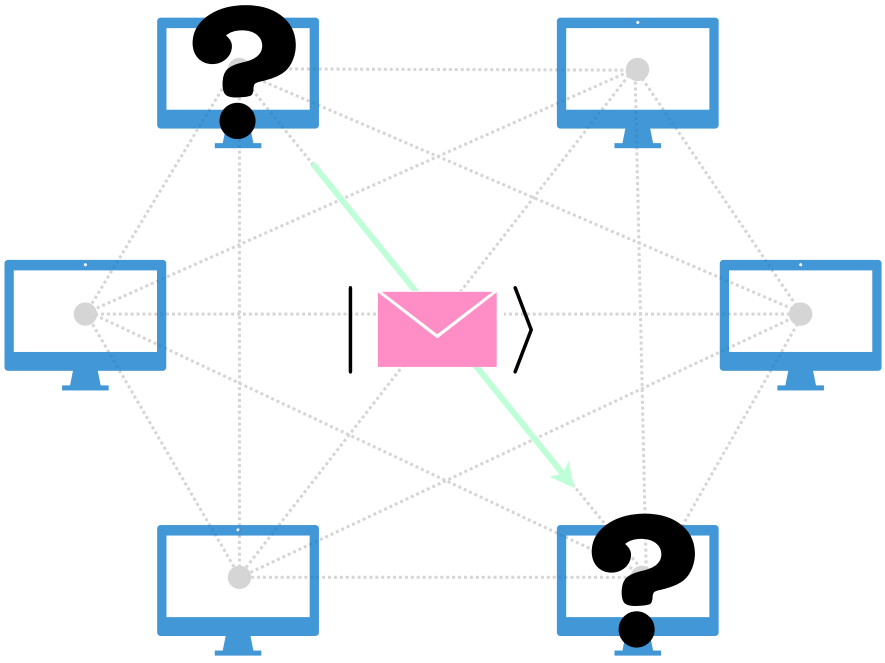


Figure 4.2: Certifying fidelities of the entangled state for 1sDI and DI authenticated teleportation, in the iid (solid line) and non-iid (dashed line) settings, requires (a) a CHSH inequality violation of $2\sqrt{2} - \epsilon$, and (b) at least S states.

Chapter 5

Anonymity for practical quantum networks



5.1 Introduction

The quantum internet, once thought to be a far-fetched dream, is now well on its way to fruition [23, 24]. With such a network, users will be able to securely exchange messages and perform computational tasks more efficiently, by harnessing the power of quantum information. Although the time it takes to create a fully functional quantum network will depend on experimental progress, it promises multiple benefits even in the early development phases. A few such examples are quantum key distribution [32], verifiable delegated quantum computation [37], and clock synchronisation [26].

While the move towards a quantum internet brings with itself many challenges, *anonymity* is inarguably an essential feature. Establishing private and secure channels of communication is becoming more and more vital in today's (perhaps too) connected world. Anonymity, or the secrecy of identity, is another basic necessity in our information age. The ability to not reveal who you are when communicating across a network opens up the possibilities of voting, anonymous email, academic peer-review, and numerous other applications.

In the classical world, anonymity has of course been the object of much study, with three main ways of tackling the problem. First, if we allow a trusted third party, anonymous communication can be carried out using a proxy server. This acts as an intermediary that forwards messages and thus hides the identity of the actual Sender [154]. Second, the computationally secure approach, which could be, for example, a chain of such servers that mix up the order of the messages so that they cannot be tracked [155]. Since in quantum cryptography we aim to address the security ramifications of migrating to quantum information, in this Chapter we are more interested in the third approach of information-theoretic, or unconditional, anonymity. This does not rely on computational assumptions or a trusted third party, and guarantees anonymity even in the age of quantum computers.

In such a setting, the first protocol for classical anonymous transmission was given by Chaum, in the form of the dining cryptographers problem [156]. A group of paranoid cryptographers, dining at a restaurant, want to figure out whether one of them has anonymously paid the bill, or an outside party. Chaum proposed a simple protocol to do this, whereby all

the cryptographers receive the value of a bit (which is equal to one if any of the group pays), without revealing which one of them has paid. The bit is essentially broadcast anonymously; this is classical anonymous transmission.

In fact, this is linked to secure multiparty computation [69, 157, 158], where a group of players wish to compute some function that depends on each of their inputs, while keeping their inputs private, and crucially, without trusting a third party. Classical anonymous transmission as presented in the dining cryptographers problem is itself an example of secure multiparty computation, namely computing the parity of the input string. Usually, secure multiparty computation involves the strong assumption that a majority of the players are honest [69, 158]. To avoid this restriction, Broadbent and Tapp [159] gave a set of protocols ensuring information-theoretic anonymity no matter the number of dishonest players, starting from a protocol for anonymously computing parity. We will later employ a selection of their other secure multiparty protocols.

As we move to quantum networks, we similarly want to be able to guarantee anonymity when we deal with quantum information. How can we send and receive qubits in an anonymous way across networks? Here, we are interested in the scenario of a Sender who wishes to transmit an arbitrary quantum state to a single Receiver anonymously. This differs from the previous case of anonymous broadcast of classical information; from the no-cloning theorem, we know that an unknown quantum state cannot be broadcast. Further, as the quantum version of secure multiparty computation involves a group of players who wish to compute a quantum circuit with each player holding an input state [70, 71], these are different problems.

Finally, we mention the difference between privacy and anonymity. If a transmission is private, the contents are hidden, while if it is anonymous, the Sender and the Receiver of the message are hidden. It is worth noting that protocols for anonymous transmission may not necessarily protect the privacy of the message. To guarantee anonymity, we must ensure that the dishonest players in the network cannot guess the Sender or the Receiver with more accuracy than a random guess. In fact, even the Receiver may be dishonest; even in this case, she must not be able to tell who is sending her the message.

5.2 Previous work

Having discussed the importance and meaning of anonymity, we are now ready to review progress in the realm of quantum anonymous transmission. The first work to consider this issue was that of Christandl and Wehner [73]. Their proposal is based on the key observation that a phase flip on any qubit alters an n-qubit GHZ state, *i.e.* $(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$, in a way that it is impossible to detect which qubit it was applied on. They suggested that each of the n players in the network hold one qubit of a GHZ state, and apply a series of local transformations and measurements on their qubit. In this way, a Sender can transmit a classical bit to all players anonymously. Further, they provided a protocol by which the anonymous transmission of a quantum bit can be achieved, again only using local operations and classical communication (LOCC). At the end of the protocol, the Sender and the Receiver share an anonymous entangled pair. This means no player but the Sender knows who shares this state. Then, the Sender can teleport a quantum state to the Receiver using Protocol 2.1, with the correction bits sent by classical anonymous transmission from the Sender to the Receiver. Once the Receiver applies this correction to her state, she will have received a quantum message sent by an anonymous player in the network.

Although their protocol is simple, requires only LOCC operations, and fulfils the much-needed requirement of quantum anonymity, in order for the protocol to be completely secure, the players may not wish to assume they share a GHZ state at the beginning. In fact, in an experimentally relevant scenario, their shared state may be imperfect. Can our network of players still have some notion of anonymity?

This question was considered in the work of Brassard et al. [39]; however, their proposal is rather complicated. It includes in the beginning a verification stage for ensuring that the shared state is at least symmetric with respect to the honest players, and so perfect anonymity is preserved. This test involves each player performing a CNOT between her initial qubit and $n-1$ ancilla qubits that she then sends to all other players. Each player then measures $n-1$ qubits in the subspace spanned by the all zeros and all ones strings. If the measurement accepts, the protocol continues with the remaining n-player GHZ state. While the authors

manage in this way to preserve perfect anonymity, their protocol cannot be easily implemented, since each player needs to perform a size-n quantum circuit and also to have access to quantum communication with all other players.

Recently, Lipinska, Murta and Wehner [74] considered a different approach to anonymous transmission: using trusted W states, *i.e.* $(|10...0\rangle + ... + |0...01\rangle)/\sqrt{n}$, instead of GHZ states. In this way, they manage to avoid the fragility of GHZ states, demonstrating that their protocol tolerates particle losses. Although their method improves the noise tolerance of quantum anonymous transmission, one of their classical subroutines requires the impractical resource of a simultaneous broadcast channel, and most importantly, their protocol creates anonymous entanglement only probabilistically, *i.e.* with a probability of $\frac{2}{n}$.

Despite progress in these different directions, the aforementioned gaps still need to be filled. When quantum networks are fully operational, we will require a protocol for quantum anonymous transmission that is noise-tolerant, secure and practical. That is the aim of this Chapter. Similarly to our previous work, we wish to use the least possible resources to achieve this goal. As protocols for the quantum internet are intended to supplement classical protocols, it is reasonable to assume that the players share private pairwise classical channels and a broadcast channel. In the quantum regime, the former can be substituted by public quantum channels and QKD protocols. Further, each player is only required to apply local transformations and measurements.

We will consider the GHZ state as our central resource, but we incorporate as our verification stage the GHZ verification protocol from Pappa et al. [160], that was further improved upon and experimentally demonstrated by McCutcheon et al. [31]. This is a practical, efficient and secure way of assessing the quality of the state, even if some of the players are dishonest. Our protocol alternates between verifying the state, and using the state for anonymous transmission, thus providing security against an untrusted source who will not know how each copy of the state will be used. In addition, we will use classical anonymous protocols from [159] that are known to be information-theoretically secure.

It is important to discuss the adversarial models considered in previous work. In both the

original Christandl-Wehner protocol and subsequent work by Lipinska et al., the adversary is said to be semi-active. This means that the shared quantum state is trusted, but the players are allowed to be dishonest. On the other hand, our model considers a fully active adversary, *i.e.* the untrusted source of GHZ states can collaborate with the dishonest players to try and break the anonymity of the transmission. This demonstrates the power of our protocol.

Further, all the quantum protocols we have seen assume perfect operations and achieve perfect anonymity. In practice, of course, no operation can be perfect, and thus perfect anonymity is unattainable. Nevertheless, it is still possible to define an appropriate notion of anonymity that is relevant for practical protocols. Our aim is to present such a protocol that allows some degree of imperfections, as is appropriate for realistic quantum networks.

5.3 Definitions

Let us now give the definitions of anonymity. We denote by n the total number of players, out of which k are honest. We will always assume the Sender is honest; however, the Receiver may be dishonest.

Definition 5.1 ([73]). *A protocol is said to be anonymous if it preserves the uncertainty about the identity of the Sender and the Receiver.*

In other words, the actions of the players during the protocol must not give away any new information regarding the identity of the Sender or the Receiver. Assuming that the Sender has not given away her identity before the protocol begins, anonymous message transmission has been achieved if, no matter what the dishonest players do, they cannot guess who has sent or received the message with probability higher than a random guess between the players they know to be honest, *i.e.* $\frac{1}{k}$.

Definition 5.2. *A protocol is said to be ϵ-anonymous if it preserves the uncertainty about the identity of the Sender and the Receiver up to ϵ.*

For a protocol to be ϵ-anonymous, it must be true that despite any number of dishonest players in the network, they can only guess who the Sender or the Receiver are with prob-

ability bounded by $\frac{1}{k} + \epsilon$. Such an approximate version of anonymity is crucial for realistic networks with imperfections. When ϵ is equal to 0, we achieve perfect anonymity. Note that these definitions must hold in spite of the Receiver as well being dishonest.

5.4 Network model

- *Players*: There are n players in total, out of which k are honest, and $n-k$ are dishonest. Honest players follow the protocol. Dishonest players might not follow the protocol, and can apply any cheating strategy on their systems. The aim of the dishonest players is to break the anonymity of the protocol.

- *State*: The quantum state they share is untrusted. The players obtain the state they require from an untrusted source, who may produce a different state in each round, and can collaborate with the dishonest players. An honest source produces the GHZ state, $|GHZ\rangle$.

- *Operations*: Their measurement devices are trusted. Honest players are only required to apply local operations. Dishonest players can apply operations on the part of the state that belongs to the whole dishonest set.

- *Classical channels*: Each pair of players shares a secure classical channel, which they can use to privately send classical information. (This is necessary to retain privacy of the honest players' measurement settings and outcomes, without which the dishonest players could cheat perfectly.)

- *Classical broadcast channel*: The players have access to a broadcast channel, allowing the broadcast of classical information by one player to all players in the network. We will use the term simultaneous broadcast when all players must broadcast their bit simultaneously, which is an impractical resource as it is hard to ensure in practice. Crucially, we only need a regular (or non-simultaneous) broadcast channel in our final protocol; all the subprotocols that we use remove the requirement of simultaneous broadcasting.

5.5 Building blocks

We will first discuss the building blocks of our protocols, which are a combination of new and existing subroutines, both classical and quantum. Throughout our protocols, we will use the same security parameter S for simplicity; however, this is not required. Let us start with our classical ingredients. These protocols are taken from or based on the information-theoretically secure functionalities of [159], where the privacy of each player's input is preserved. A dishonest player may cause the protocol to abort, but in any case they do not obtain any information about the other players' inputs.

First, we use PARITY, a classical protocol which computes the parity of the input string of n players (or equivalently, the XOR of their input bits), without revealing anything about the input of each player. It is defined in [159] and we outline it in Protocol 5.1. It is important to note that although this has the strong requirement of a simultaneous broadcast channel, we use only the modified version of this protocol (as given in the LOGICALOR protocol afterwards), which just requires a regular broadcast channel.

This protocol is then used to construct the LOGICALOR functionality from [159], by which a set of n players can privately determine the logical OR of their inputs. This is given in Protocol 5.2. A crucial step here is repeating PARITY with different orderings of the players each time; this allows the removal of the simultaneous broadcasting requirement. If the input of all players is 0, the protocol always outputs the correct answer (*i.e.* 0). If any player inputs 1, this protocol succeeds (*i.e.* outputs 1) with probability $1 - 2^{-S}$ after S rounds.

We use the LOGICALOR protocol in order to create the functionality RANDOMBIT, given in Protocol 5.3, which allows the Sender to anonymously choose a random bit according to some probability distribution. The correctness and privacy of RANDOMBIT follow directly from the properties of LOGICALOR; namely, the only thing the dishonest players learn is the bit chosen by the Sender, but not who the Sender is.

Protocol 5.1 PARITY [159]

Input: $\{x_i\}_{i=1}^n$.
Goal: Each player gets $y_i = \bigoplus_{i=1}^n x_i$.

1: Each of the n players wants to input their bit x_i. Every player i chooses random bits $\{r_i^j\}_{j=1}^n$ such that $\bigoplus_{j=1}^n r_i^j = x_i$.

2: Every player i sends their jth bit r_i^j to player j (j can equal i).

3: Every player j computes $z_j = \bigoplus_{i=1}^n r_i^j$ and reports the value in the simultaneous broadcast channel. (If the simultaneous broadcast fails, the players abort.)

4: The value $z = \bigoplus_{j=1}^n z_j$ is computed, which equals y_i.

Protocol 5.2 LOGICALOR [159]

Input: $\{x_i\}_{i=1}^n$, security parameter S.
Goal: Each player gets $y_i = \bigvee_{i=1}^n x_i$.

1: The players agree on n orderings, with each ordering having a different last player.

2: For each ordering:

(a) Each player i picks the value of p_i as follows: if $x_i = 0$, then $p_i = 0$; if $x_i = 1$, then $p_i = 1$ with probability $\frac{1}{2}$ and $p_i = 0$ with probability $\frac{1}{2}$.

(b) The players run PARITY with input $\{p_i\}_{i=1}^n$, with a regular broadcast channel rather than simultaneous broadcast, and with the players broadcasting according to the current ordering. If the result is 1, then $y_i = 1$.

(c) Repeat Steps 2(a) - (b) S times. If the result of the PARITY protocol is never 1, then $y_i = 0$.

We then extend the RANDOMBIT functionality to define a RANDOMPLAYER functionality, where the Sender can privately pick a random player from the n players by performing the RANDOMBIT protocol $\log_2 n$ times. Here, the probability distribution is the uniform random distribution. We will also need the NOTIFICATION functionality from [159], where the Sender can anonymously notify one player in the network as the Receiver. This is given in Protocol 5.4, modified to account for the fact that we do not consider multiple Senders or Receivers.

We now describe briefly the ANONYMOUS ENTANGLEMENT protocol from [73], given in

Protocol 5.3 RANDOMBIT

Input: All: parameter S. Sender: distribution D.
Goal: Sender chooses a bit according to D.

1: The players pick bits $\{x_i\}_{i=1}^n$ as follows: the Sender picks bit x_i to be 0 or 1 according to distribution D; all other players pick $x_i = 0$.

2: The players perform LOGICALOR with input $\{x_i\}_{i=1}^n$ and security parameter S, and output its outcome.

Protocol 5.4 NOTIFICATION [159]

Input: Security parameter S, Sender's choice of Receiver is player r.
Goal: Sender notifies Receiver.

1: For each player i:

(a) Each player $j \neq i$ picks p_j as follows: if $i = r$ and player j is the Sender, then $p_j = 1$ with probability $\frac{1}{2}$ and $p_j = 0$ with probability $\frac{1}{2}$. Otherwise, $p_j = 0$. Let $p_i = 0$.

(b) The players run PARITY with input $\{p_i\}_{i=1}^n$, with the following differences: player i does not broadcast her value, and they use a regular broadcast channel rather than simultaneous broadcast. If the result is 1, then $y_i = 1$. (If any player refuses to broadcast, the players abort.)

(c) Repeat Steps 1(a) - (b) S times. If the result of PARITY is never 1, then $y_i = 0$.

2: If player i obtained $y_i = 1$, then she is the Receiver.

Protocol 5.5. Here, it is assumed that the players share a GHZ state, and that the Sender and the Receiver know their respective identities. Assuming the initial state is a perfect GHZ state, the protocol creates a Bell state between the Sender and the Receiver perfectly anonymously. Note that this protocol is anonymous for up to $n - 2$ dishonest players; if all players but one were dishonest, they could easily cooperate to figure out the identity of the Sender by the process of elimination. However, in all other cases, the protocol protects the identity of the communicating players, no matter what the dishonest players do.

The last ingredient we use is the VERIFICATION protocol for GHZ states from the work of Pappa et al. [160], implemented for 3- and 4-qubit GHZ states by McCutcheon et al. [31]. There, one of the players, known as the Verifier, runs tests to assess how close the shared

Protocol 5.5 ANONYMOUS ENTANGLEMENT [73]

Input: GHZ state shared between n players.
Goal: Bell state $|\Phi^+\rangle$ created between Sender and Receiver anonymously.

1: Each player, apart from the Sender and Receiver, applies a Hadamard transform to their qubit. They measure in the computational basis and broadcast their outcome.

2: The Sender first picks a random bit b, broadcasts it, and applies a phase flip σ_z to her qubit only when $b = 1$.

3: The Receiver picks a random bit b', broadcasts it and applies a phase flip σ_z to her qubit only when the parity of everyone else's broadcasted bits is 1.

Protocol 5.6 VERIFICATION [160], [31]

Input: State $|\Psi\rangle$ shared between n players.
Goal: Players verify that $|\Psi\rangle$ is the n-qubit GHZ state.

1: The Verifier generates random angles $\theta_j \in [0, \pi)$ for all players including themselves ($j \in \{1, 2, ..., n\}$), such that $\sum_j \theta_j$ is a multiple of π. The angles are then sent out to all the players in the network.

2: Player j measures in the basis $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta_j}|1\rangle)\}$, and sends the outcome $Y_j = \{0, 1\}$ to the Verifier.

3: The state passes the verification test when the following condition is satisfied: if the sum of the randomly chosen angles is an even multiple of π, there must be an even number of 1 outcomes for Y_j, and if the sum is an odd multiple of π, there must be an odd number of 1 outcomes for Y_j. We can write this condition as $\bigoplus_j Y_j = \frac{1}{\pi}\sum_j \theta_j \pmod 2$.

state is to the ideal state; their scheme is given in Protocol 5.6. The test measurements, which are equivalent to a rotation around the $\hat{z}$-axis followed by a measurement in the σ_X basis, are chosen from a large set, in order to allow the protocol to tolerate losses, while minimising attacks that exploit this. We can see that the perfect state always passes the verification test, and more interestingly, a soundness statement can be proven, which we will explain and use in later sections. For our purposes, we will use a version of this verification protocol that is similar to the Symmetric Verification protocol from [160], while ensuring that anonymity is preserved.

5.6 Protocol

Now that we have our building blocks, we are ready to devise an efficient protocol for anonymous quantum message transmission. Before we present our protocol, let us explain two assumptions we have made for simplicity, and how to remove them. Firstly, we have assumed there is only one Sender. If there is the possibility of multiple Senders (this is known as a collision), the players can run a simple classical protocol, COLLISION DETECTION from [159], and only continue if there are no collisions. Secondly, our protocol will distribute one Bell pair between the Sender and the Receiver. Then, the Sender can anonymously teleport the quantum message to the Receiver, with the correction bits sent by classical anonymous transmission. This can be done, for example, by the FIXED ROLE ANONYMOUS MESSAGE TRANSMISSION functionality from [159], where, in the case the Sender and the Receiver know their identities, the Sender can transmit a classical message to the Receiver anonymously. Further, if we want to increase the fidelity of the transmitted quantum message, we can use the subroutines from Brassard et al. [39], which first create a number of non-perfect Bell states, then distill one pair, and finally perform the teleportation.

Our scheme is given in Protocol 5.7. Let us now analyse its working. First, note that if the state is a perfect GHZ state and the operations of the honest players are perfect, then the anonymity of the protocol is perfect. In Step 1, the players run the NOTIFICATION protocol which is perfectly anonymous. In Step 2, the GHZ state is shared between the players, which does not affect the anonymity. Note that the role of the source can be played by a player, as long as the choice of the player is independent of who the Sender is.

In Step 3(a), the players run the RANDOMBIT protocol which is also perfectly anonymous. The analysis of Step 3(b) follows from the analysis of the Symmetric Verification protocol in [160]. However, in contrast to their work, we do not need a trusted common random source (CRS), which was the major drawback of their verification protocol. They needed this resource to randomly choose whether the state is used for verification or computation, and to pick which player plays the role of the Verifier. In their case, they wanted to allow any player to be dishonest, and so no player could be trusted to pick the randomness. In

Protocol 5.7 ϵ-ANONYMOUS ENTANGLEMENT DISTRIBUTION

Input: Security parameter S.
Goal: Bell state $|\Phi^+\rangle$ created between Sender and Receiver with ϵ-anonymity.

1: **The Sender notifies the Receiver:**
The players run NOTIFICATION.

2: **GHZ state generation:**
The source generates a state $|\Psi\rangle$ and distributes it to the players.

3: **The Sender anonymously chooses Verification or Anonymous Entanglement:**

(a) The players perform RANDOMBIT, with the Sender choosing her input according to the following probability distribution: she flips S fair classical coins, and if all coins are heads, she inputs 0; else, she inputs 1. Let the outcome be x.

(b) If $x = 0$, the players run ANONYMOUS ENTANGLEMENT; else if $x = 1$:

(i) Run RANDOMPLAYER, where the Sender inputs a uniformly random $j \in \{1, 2, ..., n\}$, to get output j.

(ii) Player j runs VERIFICATION as the Verifier, and if she accepts the outcome of the test they return to Step 2, otherwise the protocol aborts.

If at any point in the protocol, the Sender realises someone does not follow the protocol, she stops behaving like the Sender and behaves as any player.

our protocol, whether each state is used for verification or anonymous transmission is determined by the output of RANDOMBIT, and the choice of which player becomes the Verifier by the output of RANDOMPLAYER. For both of these cases, it is the input of the Sender that completely determines the outcomes of these subroutines; the purpose of RANDOMBIT and RANDOMPLAYER is simply to distribute the Sender's choice anonymously to the other players. Since in our case, the Sender is always an honest player, she can immediately see if her choice does not correspond to the outcome of the subroutine. If it does not, she will realise that a player is misbehaving (which means inputting 1 instead of 0 as required to in RANDOMBIT) and she does not continue behaving like the Sender. In this way, we are able to remove the requirement of a CRS.

5.7 Analysis of security and anonymity

Our proof proceeds in two main stages. First, we will show that by running Protocol 5.7 enough times, the players can ensure that the probability that the protocol has not aborted and the state is 'far' from the GHZ state is small. Then, we will see that if the state is 'close' to the GHZ state, then anonymity is almost preserved, since the players started with almost the GHZ state. (We will clarify later what exactly is meant by 'close' and 'far'.)

Although our ideal state is the GHZ state, we will work in a different basis for ease of calculations such that the ideal state is now denoted by $|\Phi_0^n\rangle$ and expressed as

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle - \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle\Big], \tag{5.1}$$

where $\Delta(\bar{\mathbf{y}}) = \sum_i y_i$ denotes the Hamming weight of the classical n-bit string $\bar{\mathbf{y}}$. The state $|\Phi_0^n\rangle$ can be obtained from the GHZ state by local unitaries, namely a Hadamard and phase shift applied to every qubit. We will also define the orthogonal state $|\Phi_1^n\rangle$, given by

$$|\Phi_1^n\rangle = \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle - \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle\Big]. \tag{5.2}$$

In this basis, the Sender's transformation of σ_Z becomes $\sigma_X\sigma_Z$. The following Lemma 5.1, which we prove in Appendix 5.A.1, will be useful for our calculations.

Lemma 5.1. *The Sender's transformation $\sigma_X\sigma_Z$ applied to any qubit of the states $|\Phi_0^n\rangle, |\Phi_1^n\rangle$ gives $\sigma_X\sigma_Z |\Phi_0^n\rangle = |\Phi_1^n\rangle, \sigma_X\sigma_Z |\Phi_1^n\rangle = -|\Phi_0^n\rangle$.*

The security statements we wish to make are based on the state used for anonymous transmission. Let us now see what Protocol 5.6 tells us about this state. We will use a fidelity measure of the state $|\Psi\rangle$ shared between the n players given by

$$F'(|\Psi\rangle) \equiv \max_{U_D} F(U_D |\Psi\rangle, |\Phi_0^n\rangle). \tag{5.3}$$

The intuition behind this measure is that the honest players can never hope to control what

the dishonest players do to their part of the state. To take this into account, here we define U_D as some operation applied by the dishonest players on their qubits. Since we assume all purification power to the dishonest players, it is sufficient to consider U_D to be a unitary operation. This fidelity measure is equal to the fidelity between the reduced states of the honest players of the states $|\Psi\rangle$ and $|\Phi_0^n\rangle$ (for more details, see Appendix 5.A.2).

The proofs in [31, 160] assume that the dishonest players apply their optimal cheating strategy to guess the measurement outcomes of the honest players. Then, they show that the probability of passing the verification test with the state $|\Psi\rangle$, denoted by $P(|\Psi\rangle)$, is related to the fidelity of the state by $F'(|\Psi\rangle) \geq 4P(|\Psi\rangle) - 3$. This holds even if the shared state is mixed; however, as we will see, a clever dishonest source will always create pure states.

To discuss the security of Protocol 5.7, we wish to bound the probability that a state far from the ideal GHZ state is accepted for anonymous transmission. Since in our scheme, we alternate between verification and creation of anonymous entanglement, this corresponds to the scenario where the source manages to make the players accept the previously tested copies (and not trigger an abort of the protocol), yet the used copy is far from ideal.

Let us denote by C_ϵ the event that a state of fidelity $F'(|\Psi\rangle) \leq \sqrt{1-\epsilon^2}$ is used for anonymous transmission in Step 3(b). This means that the state supplied by the source is such that, no matter what operation the dishonest players apply to their qubits, the fidelity is at most $\sqrt{1-\epsilon^2}$. We will now bound the probability of the event C_ϵ in the following Theorem, illustrating the soundness of our protocol.

Theorem 5.2. *For all $\epsilon > 0$, the honest players have the guarantee that*

$$Pr[C_\epsilon] \leq 2^{-S} \frac{4n}{1-\sqrt{1-\epsilon^2}}. \tag{5.4}$$

Proof. Our aim is to bound the probability of the protocol failing, given that the dishonest players apply the best cheating strategy that would maximise this probability. Let us discuss what such an optimal cheating strategy would be, following [160]. Although we allow

the dishonest source to create any state in any round and even entangle the states between rounds, we will see that the optimal cheating strategy, which maximises the probability of the event C_ϵ, is to create in each round some pure state $|\Psi\rangle$ such that $F'(|\Psi\rangle) = \sqrt{1-\epsilon^2}$.

To start, a dishonest source providing all copies but one as ideal states, and one copy as a completely different state, will succeed with a very small probability. This is because the probability of this one copy being chosen for anonymous transmission is 2^{-S}, and so the probability of failure will be this at most. By providing a mixed state, the source does not gain any advantage, as a mixed state is a probabilistic mixture of pure states, and the overall cheating probability of this mixed strategy is just a weighted combination of the cheating probabilities of each of the pure states. Then, this mixed strategy is worse than the strategy that always sends the pure state that has the maximum cheating probability of all states in the mixture. Thus, we can continue the proof by only considering strategies with pure states.

Next, we see that an entangled strategy does not help, as it can be replaced by a strategy sending unentangled states as follows. Given some entangled state, for a given round, the probability of passing the test and the fidelity of the state depend only on the reduced state, conditioned on passing previous rounds. The exact same effect can be achieved by sending these mixed reduced states corresponding to each round, without any entanglement.

If the source sends any state with even smaller $F'(|\Psi\rangle)$, the probability of failing the test (and therefore, the protocol aborting) would just increase. Lastly, if in any round the source created a state with higher $F'(|\Psi\rangle)$, then this would not contribute to the event C_ϵ, and in fact, it may also cause the protocol to abort. Thus, to upper bound the probability of event C_ϵ with respect to the best attack a dishonest source can perform, we only need to consider the case where in each round the source creates some state $|\Psi\rangle$ such that $F'(|\Psi\rangle) = \sqrt{1-\epsilon^2}$.

Now that we have determined the optimal cheating strategy, we will bound the probability of the state used for anonymous transmission in Protocol 5.7 being such that the maximum fidelity is $\sqrt{1-\epsilon^2}$. First, we consider the probability that the state is used in a round l. For this to happen, the Sender must get the result of all S coin flips in Step 3(a) to be heads ($x = 0$), which happens with probability 2^{-S}. The Sender then calls RANDOMBIT with her input as 0.

The output of RANDOMBIT will be 0 with probability 1 when all players input 0 (note that the Sender can see if any player behaves dishonestly and inputs 1, as the output of RANDOMBIT can then be 1, and so the Sender will abort).

Second, we consider the probability that the state is tested in all $(l-1)$ previous rounds. Here, the Sender must input 1 to RANDOMBIT. The probability of the Sender not getting all S coin flips to be 0 is given by $1-2^{-S}$. Then, the probability that RANDOMBIT will give an output of 1 is given by $1-2^{-S}$ after S rounds. Dishonest players will not affect the output, since even if they input 1 to RANDOMBIT, the output will still be 1. Thus, the overall probability is given by $[(1-2^{-S})(1-2^{-S})]^{l-1}$.

Finally, we consider the probability that all the $(l-1)$ tests have passed. In our protocol, a randomly chosen player j runs VERIFICATION as the Verifier. If the Verifier is honest (which happens with probability $\frac{k}{n}$), the probability that the test is passed with a state $|\Psi\rangle$ is given by $P(|\Psi\rangle)$. If the Verifier is dishonest (with probability $\frac{n-k}{n}$), let the probability be 1 as the worst case scenario. Then, the probability that all $(l-1)$ tests have passed is $\left(\frac{n-k}{n}+\frac{k}{n}P(|\Psi\rangle)\right)^{l-1}$. As mentioned previously, from [31, 160], the probability that a state $|\Psi\rangle$ with fidelity $F'(|\Psi\rangle)$ will pass the test is given by $P(|\Psi\rangle) \leq \frac{3}{4}+\frac{F'}{4}$. In our case, recall that $F'(|\Psi\rangle) \leq \sqrt{1-\epsilon^2}$. Thus, the total probability of event C_ϵ at the l^{th} repetition of the protocol is

$$\Pr[C_\epsilon^l] \leq 2^{-S}\Big(1-2^{1-S}+2^{-2S}\Big)^{l-1}\Big(1-\big(\frac{k-F'k}{4n}\big)\Big)^{l-1}. \tag{5.5}$$

We then take the integral to upper bound this probability as follows:

$$\begin{aligned}
\Pr[C_\epsilon] &\leq \int_0^\infty 2^{-S}(1-2^{1-S}+2^{-2S})^l\Big(1-\big(\frac{k-F'k}{4n}\big)\Big)^l dl \\
&\leq 2^{-S}\int_0^\infty \Big(1-\big(\frac{k-F'k}{4n}\big)\Big)^l dl \\
&= -\frac{2^{-S}}{\ln\left(1-\left(\frac{k-F'k}{4n}\right)\right)} \\
&\leq 2^{-S}\frac{4n}{k(1-F')} \\
&\leq 2^{-S}\frac{4n}{k(1-\sqrt{1-\epsilon^2})}.
\end{aligned} \tag{5.6}$$

Since each honest player does not know which other players are honest or dishonest, we can further upper bound this in terms of a security statement for the honest players:

$$\Pr[C_\epsilon] \leq 2^{-S} \frac{4n}{1-\sqrt{1-\epsilon^2}}. \tag{5.7}$$

□

If the players take $S = \log_2(\frac{4n}{(1-\sqrt{1-\epsilon^2})\delta})$, they get $\Pr[C_\epsilon] \leq \delta$. The expected number of runs of the protocol is given by $2^S = \frac{4n}{(1-\sqrt{1-\epsilon^2})\delta}$. Thus, they can make this probability of failure negligible by doing a large number of runs.

Let us assume for simplicity that when the event C_ϵ is true, which happens with probability at most δ, the dishonest players can perfectly guess the identity of the Sender or the Receiver. We will now show that when the event C_ϵ is false, which happens with probability at least $1-\delta$, the dishonest players (even having in their possession the entire quantum state that corresponds to the protocol) cannot guess the Sender or the Receiver with probability much higher than a random guess. If C_ϵ is false, this means the state used for anonymous transmission has a fidelity of at least $\sqrt{1-\epsilon^2}$.

Given a state $|\Psi\rangle$ such that $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, we now want to see how well the dishonest players can guess the identity of the Sender, thus determining the anonymity of Protocol 5.7. Recall that the Sender's transformation is $\sigma_X \sigma_Z$; this action sets the Sender apart from the other players. Further, the Sender is known to be an honest player. The best cheating strategy a dishonest player could apply to guess the identity of the Sender is then to make some sort of measurement that distinguishes the state $|\Psi_i\rangle$, which is the resulting state after any honest player i applies the Sender's transformation, from $|\Psi_j\rangle$, which is the resulting state after any other honest player j applies the Sender's transformation.

In our calculations, we will assume an imperfect state, and further consider two cases: firstly, when all the players are honest (Lemma 5.3), and secondly, when we have dishonest players who could apply some operation on their part of the state (Lemma 5.4).

Lemma 5.3. *If all the players are honest, and they share a state $|\Psi\rangle$ such that $F(|\Psi\rangle, |\Phi_0^n\rangle) = \sqrt{1-\epsilon^2}$, then for all honest players i, j who could be the Sender, we have that $F(|\Psi_i\rangle, |\Psi_j\rangle) \geq 1-\epsilon^2$, where $|\Psi_i\rangle$ is the state after player i has applied the Sender's transformation.*

Proof. If we have $F(|\Psi\rangle, |\Phi_0^n\rangle) = |\langle\Psi|\Phi_0^n\rangle|^2 = \sqrt{1-\epsilon^2}$, then similarly to [160], we can write the state shared by all the players as

$$|\Psi\rangle = (1-\epsilon^2)^{1/4} |\Phi_0^n\rangle + \epsilon_1 |\Phi_1^n\rangle + \sum_{i=2}^{2^n-1} \epsilon_i |\Phi_i^n\rangle, \tag{5.8}$$

where $\sum_{i=1}^{2^n-1} \epsilon_i^2 = 1 - \sqrt{1-\epsilon^2}$ to preserve normalisation. If player i is the Sender, then she applies $\sigma_X \sigma_Z$, and using Lemma 5.1, the state becomes

$$|\Psi_i\rangle = (1-\epsilon^2)^{1/4} |\Phi_1^n\rangle - \epsilon_1 |\Phi_0^n\rangle + \sum_{i=2}^{2^n-1} \epsilon_i' |\Phi_i^n\rangle. \tag{5.9}$$

Instead, if player j is the Sender and she applies $\sigma_X \sigma_Z$, the state becomes

$$|\Psi_j\rangle = (1-\epsilon^2)^{1/4} |\Phi_1^n\rangle - \epsilon_1 |\Phi_0^n\rangle + \sum_{i=2}^{2^n-1} \epsilon_i'' |\Phi_i^n\rangle. \tag{5.10}$$

The fidelity is then given by

$$F(|\Psi_i\rangle, |\Psi_j\rangle) = |\langle\Psi_i|\Psi_j\rangle|^2 = \left| \sqrt{1-\epsilon^2} + \epsilon_1^2 + \sum_{i=2}^{2^n-1} \epsilon_i' \epsilon_i'' \right|^2 \geq 1-\epsilon^2. \tag{5.11}$$

□

Lemma 5.4. *If some of the players are dishonest, and they share a state $|\Psi\rangle$ such that $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, then for all honest players i, j who could be the Sender, we have that $F(|\Psi_i\rangle, |\Psi_j\rangle) \geq 1-\epsilon^2$, where $|\Psi_i\rangle$ is the state after player i has applied the Sender's transformation.*

Proof. Recall that our fidelity measure is given by $F'(|\Psi\rangle) \equiv \max_{U_D} F(U_D |\Psi\rangle, |\Phi_0^n\rangle)$. Let us now denote by $|\Psi'\rangle$ the state after the operation U_D which maximises this fidelity has been

applied. Decomposing the state into honest and dishonest parts as in [160], we have

$$\left|\Psi'\right\rangle = \left|\Phi_0^k\right\rangle |\psi_0\rangle + \left|\Phi_1^k\right\rangle |\psi_1\rangle + |\chi\rangle \,. \tag{5.12}$$

Here, $|\chi\rangle$ contains both honest and dishonest parts, of which the honest part is orthogonal to both $\left|\Phi_0^k\right\rangle$ and $\left|\Phi_1^k\right\rangle$, and we consider the dishonest parts of the state to be unnormalised. We now want to find the closeness of the states $|\Psi_i\rangle, |\Psi_j\rangle$, which are the states after the $\sigma_X\sigma_Z$ operation is applied to $|\Psi'\rangle$ by either player i or j who is the Sender, and given by

$$|\Psi_i\rangle = \left|\Phi_1^k\right\rangle |\psi_0\rangle - \left|\Phi_0^k\right\rangle |\psi_1\rangle + \left|\chi'\right\rangle, \quad |\Psi_j\rangle = \left|\Phi_1^k\right\rangle |\psi_0\rangle - \left|\Phi_0^k\right\rangle |\psi_1\rangle + \left|\chi''\right\rangle. \tag{5.13}$$

The fidelity is then given by

$$F(|\Psi_i\rangle, |\Psi_j\rangle) = |\langle\Psi_i|\Psi_j\rangle|^2 = \left|\langle\psi_0|\psi_0\rangle + \langle\psi_1|\psi_1\rangle + \left\langle\chi'\middle|\chi''\right\rangle\right|^2. \tag{5.14}$$

However, although the overall state $|\Psi'\rangle$ is normalised, the dishonest players' part of the state is not. Thus, we need to determine a bound on $\langle\psi_0|\psi_0\rangle$ and $\langle\psi_1|\psi_1\rangle$. We have $F(|\Psi'\rangle, |\Phi_0^n\rangle) = |\langle\Phi_0^n|\Psi'\rangle|^2 \geq \sqrt{1-\epsilon^2}$. It was shown in [160] that we can write $|\Phi_0^n\rangle$ for any k, n as

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2}}\Big[\left|\Phi_0^k\right\rangle\left|\Phi_0^{n-k}\right\rangle - \left|\Phi_1^k\right\rangle\left|\Phi_1^{n-k}\right\rangle\Big], \tag{5.15}$$

and using this, we get

$$\frac{1}{2}\left|\left\langle\Phi_0^{n-k}\middle|\psi_0\right\rangle^2 + \left\langle\Phi_1^{n-k}\middle|\psi_1\right\rangle^2 - 2\left\langle\Phi_0^{n-k}\middle|\psi_0\right\rangle\left\langle\Phi_1^{n-k}\middle|\psi_1\right\rangle\right| \geq \sqrt{1-\epsilon^2}. \tag{5.16}$$

To simplify our calculation, let us add a term $2\left\langle\Phi_0^{n-k}\middle|\psi_0\right\rangle\left\langle\Phi_1^{n-k}\middle|\psi_1\right\rangle$ to the left hand side, which does not affect the inequality. Using the triangle inequality $|x| + |y| \geq |x+y|$, we have

$$\frac{1}{2}\Big[\left|\left\langle\Phi_0^{n-k}\middle|\psi_0\right\rangle\right|^2 + \left|\left\langle\Phi_1^{n-k}\middle|\psi_1\right\rangle\right|^2\Big] \geq \sqrt{1-\epsilon^2}. \tag{5.17}$$

Using the Cauchy-Schwarz inequality, $|\langle v|w\rangle|^2 \leq \langle v|v\rangle\langle w|w\rangle$, and recalling that the ideal parts

of the state are normalised, we have

$$\langle\psi_0|\psi_0\rangle + \langle\psi_1|\psi_1\rangle \geq \left|\left\langle \Phi_0^{n-k}\middle|\psi_0\right\rangle\right|^2 + \left|\left\langle \Phi_1^{n-k}\middle|\psi_1\right\rangle\right|^2 \geq \sqrt{1-\epsilon^2}. \tag{5.18}$$

Since the overall state $|\Psi'\rangle$ is normalised, we must then have $\langle\chi'|\chi''\rangle \leq 1 - \sqrt{1-\epsilon^2}$. Thus, we get our expression for fidelity from Equation (5.14) as $F(|\Psi_i\rangle, |\Psi_j\rangle) \geq 1 - \epsilon^2$. □

We are now ready to prove the anonymity of our protocol in Theorem 5.5.

Theorem 5.5. *If the players share a state $|\Psi\rangle$ such that $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, then the probability that the dishonest players can guess the identity of the Sender is given by*

$$Pr[guess] \leq \frac{1}{k} + \epsilon. \tag{5.19}$$

Proof. We will now show that if the players share close to the GHZ state, then the Sender is ϵ-anonymous. From Theorem 5.2, we saw that the probability that the state used for anonymous transmission satisfies $F'(|\Psi\rangle) \leq \sqrt{1-\epsilon^2}$ is given by $\Pr[C_\epsilon] \leq \delta$ for the honest players, where δ depends on the number of runs of the verification protocol. Thus, by doing enough runs, we can make this very small, and so we have that the state used for anonymous transmission will be close to the GHZ state, as given by $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$.

From the previous proof, we see that if $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, the distance between the states if player i or j was the Sender is $D(|\Psi_i\rangle, |\Psi_j\rangle) \leq \epsilon$. A dishonest player who wishes to guess the identity of the Sender would make some sort of measurement to do so. Then, we must find the maximum success probability of a measurement that could distinguish between the k states resulting from the Sender (who can only be an honest player) applying the $\sigma_X\sigma_Z$ transformation. We are purely interested in determining the highest success probability of such a strategy; this will allow us to make an assessment of the anonymity of our protocol.

From Equation (2.31), we know that the success probability of discriminating between k

states $\{\rho_i\}$ occurring with probabilities $\{p_i\}$ is given by

$$\Pr[\text{success}] = \sum_{i=1}^{k} p_i \text{Tr}(\pi_i \rho_i), \tag{5.20}$$

where $\{\pi_i\}$ is the set of corresponding POVM elements. As we have just shown, the distance between any two states after the Sender's transformation is upper bounded by ϵ. Then, if we take $|\alpha\rangle = |\Psi_j\rangle$, we know that any of these k states is of a maximum distance ϵ away from this same state $|\alpha\rangle$. From Equation (2.27), we see that for any POVM element P, we can write the trace distance between two states ρ, σ as $\text{Tr}\big[P(\rho - \sigma)\big] \leq D(\rho, \sigma)$. Thus, we have for each POVM element π_i and states $|\Psi_i\rangle, |\alpha\rangle$,

$$\text{Tr}\big(\pi_i |\Psi_i\rangle \langle\Psi_i|\big) - \text{Tr}\big(\pi_i |\alpha\rangle \langle\alpha|\big) \leq \epsilon. \tag{5.21}$$

Assuming that each honest player has an equiprobable chance of becoming the Sender, the probability that the dishonest players can guess the identity of the Sender is given by

$$\begin{aligned}
\Pr[\text{guess}] &= \sum_{i=1}^{k} \frac{1}{k} \text{Tr}\big(\pi_i |\Psi_i\rangle \langle\Psi_i|\big) \\
&\leq \frac{1}{k} \sum_{i=1}^{k} \Big[\text{Tr}\big(\pi_i |\alpha\rangle \langle\alpha|\big) + \epsilon\Big] \\
&= \frac{1}{k} \text{Tr}\Big[\sum_{i=1}^{k} \pi_i |\alpha\rangle \langle\alpha|\Big] + \frac{1}{k} k\epsilon \\
&= \frac{1}{k} \text{Tr}\big(|\alpha\rangle \langle\alpha|\big) + \epsilon \\
&= \frac{1}{k} + \epsilon.
\end{aligned} \tag{5.22}$$

From Definition 5.2, this shows that Protocol 5.7 is an ϵ-anonymous protocol for quantum message transmission. □

5.8 Discussion

In this Chapter, we have proposed a practical protocol for anonymous communication of quantum messages in the presence of dishonest players and an untrusted resource state, thus demonstrating its security in the fully adversarial scenario. Our protocol achieves ϵ-anonymity, where the parameter ϵ incorporates imperfections in the network. The verification step is carried out using a protocol that has been experimentally demonstrated [31], and is tolerant to losses and noise by design. In fact, such a setup for generating GHZ states could already allow a proof-of-principle demonstration of our protocol, and existing setups for the creation of GHZ states with more qubits, such as [161, 162], could further be used to show anonymous quantum communication across a large network.

If all players are honest and have followed the protocol, an entangled state will be created anonymously between the Sender and the Receiver. Of course, a dishonest player can always block all anonymous transmission by measuring her qubit in the computational basis. However, as we have shown, the goal of anonymous transmission, which is to hide the identity of the communicating players, will be achieved no matter what the dishonest players do. Although we have not considered a specific noise model, our analysis incorporates imperfections in $|\Psi\rangle$, the state shared by all the players at the beginning of the protocol. We can carry this forward to the anonymously transmitted message, under the assumption that all players are honest. The fidelity of the final entangled state with the Bell state will be at least as high as the fidelity of $|\Psi\rangle$ with the GHZ state. As mentioned previously, after the entangled state has been constructed, the Sender and the Receiver can perform anonymous teleportation of the quantum message (using Protocol 2.1), with the Sender anonymously sending a classical message with the correction bits required to complete the teleportation. The fidelity of teleportation will then be at least as high as the fidelity of the entangled state, as we saw in previous Chapters.

One could make the protocol even more practical by optimising the analysis so as to not require a high fidelity GHZ state, which poses experimental challenges. There may also possibly be other states that could be used as a resource for anonymous transmission, although

as far as we know, there is none so naturally suited as the GHZ state, and other options may only work probabilistically. Nevertheless, there may be a tradeoff between this and other advantages that these states could offer. In fact, in [74], they considered particular noise models such as dephasing and depolarising noise, demonstrating that the W state protocol has higher noise tolerance than the GHZ state version. On the experimental side, our protocol can be used for the first implementation of anonymous quantum communication.

We end by suggesting some applications of our work. The anonymous entangled channel created by our scheme could be used to perform anonymous QKD, if two players in a network wish to establish a secret key without the others knowing. Another important application is quantum electronic voting [163, 164]. Many existing protocols that achieve this functionality have since been shown to be vulnerable to possible attacks [165]. An anonymous channel, on the other hand, could allow each voter to send their vote anonymously. In any case, we expect that these types of applications will be very important for future quantum networks, and thus an essential building block of the near-future communication infrastructure.

5.A Appendix

5.A.1 Proof of Lemma 5.1

Lemma 5.1. *The Sender's transformation $\sigma_X\sigma_Z$ applied to any qubit of the states $|\Phi_0^n\rangle, |\Phi_1^n\rangle$ gives $\sigma_X\sigma_Z |\Phi_0^n\rangle = |\Phi_1^n\rangle, \sigma_X\sigma_Z |\Phi_1^n\rangle = -|\Phi_0^n\rangle$.*

Proof. Note that we have $\sigma_X\sigma_Z |0\rangle = |1\rangle$, $\sigma_X\sigma_Z |1\rangle = -|0\rangle$. Recall our states are defined as

$$
\begin{aligned}
|\Phi_0^n\rangle &= \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle - \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle\Big], \\
|\Phi_1^n\rangle &= \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle - \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle\Big].
\end{aligned} \tag{5.23}
$$

Let the Sender be player $i \in \{1, ..., n\}$, and let y_i denote the i^{th} qubit of the string $\bar{\mathbf{y}}$. We can express the terms in the above states as

$$
\begin{aligned}
\sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle &= \sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0} + \sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1}, \\
\sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle &= \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0} + \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1}, \\
\sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle &= \sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0} + \sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1}, \\
\sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle &= \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0} + \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1}.
\end{aligned} \tag{5.24}
$$

Applying the Sender's transformation $\sigma_X\sigma_Z$ to y_i will then have the following effect:

$$\begin{aligned}
&\sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\,,\\
&\sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\,,\\
&\sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\,,\\
&\sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\,.
\end{aligned} \tag{5.25}$$

Substituting in Equation (5.23),

$$\begin{aligned}
|\Phi_0^n\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \frac{1}{\sqrt{2^{n-1}}}\Big[&\Big(\sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\Big)\\
&- \Big(\sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\Big)\Big].\\
|\Phi_1^n\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \frac{1}{\sqrt{2^{n-1}}}\Big[&\Big(\sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\Big)\\
&- \Big(\sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=1} - \sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle_{y_i=0}\Big)\Big].
\end{aligned} \tag{5.26}$$

Using Equation (5.24),

$$\begin{aligned}
|\Phi_0^n\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(\bar{\mathbf{y}})=1 \pmod 4} |\bar{\mathbf{y}}\rangle - \sum_{\Delta(\bar{\mathbf{y}})=3 \pmod 4} |\bar{\mathbf{y}}\rangle\Big] &= |\Phi_1^n\rangle\,,\\
|\Phi_1^n\rangle \xrightarrow{(\sigma_X\sigma_Z)_i} \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(\bar{\mathbf{y}})=2 \pmod 4} |\bar{\mathbf{y}}\rangle - \sum_{\Delta(\bar{\mathbf{y}})=0 \pmod 4} |\bar{\mathbf{y}}\rangle\Big] &= -|\Phi_0^n\rangle\,.
\end{aligned} \tag{5.27}$$

This proves that the Sender's transformation $\sigma_X\sigma_Z$ applied to any qubit of the state $|\Phi_0^n\rangle$ converts it to $|\Phi_1^n\rangle$, and applied to any qubit of the state $|\Phi_1^n\rangle$ converts it to $-|\Phi_0^n\rangle$.

□

5.A.2 Fidelity measure

In a network with dishonest players, we will work with the fidelity measure $F'(|\Psi\rangle)$. Since the dishonest players collaborate with the source of $|\Psi\rangle$, the honest players can only know the fidelity of the state up to local operations on the dishonest part, rather than the fidelity of the actual state created by the source.

Lemma 5.6. *The fidelity measure between the state $|\Psi\rangle$ and the ideal state $|\Phi\rangle$, shared between the set of honest players, H, and the set of dishonest players, D, is given by*

$$F'(|\Psi\rangle) \equiv \max_{U_D} F(U_D |\Psi\rangle, |\Phi\rangle) = F(\rho_H^{|\Psi\rangle}, \rho_H^{|\Phi\rangle}), \tag{5.28}$$

where U_D is a unitary acting on the dishonest part of the state, $\rho_H^{|\Psi\rangle}$ is the reduced state of the honest players of the state $|\Psi\rangle$, and $\rho_H^{|\Phi\rangle}$ is the reduced state of the honest players of the state $|\Phi\rangle$.

Proof. By Uhlmann's Theorem [166], the fidelity between the reduced states is equal to the maximum fidelity over all purifications:

$$F(\rho_H^{|\Psi\rangle}, \rho_H^{|\Phi\rangle}) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle|^2, \tag{5.29}$$

where $\rho_H^{|\Psi\rangle} = \mathrm{tr}_D(|\psi\rangle\langle\psi|)$, and $\rho_H^{|\Phi\rangle} = \mathrm{tr}_D(|\phi\rangle\langle\phi|)$. Let us take one purification of $\rho_H^{|\Psi\rangle}$ to be $|\Psi\rangle$, and one purification of $\rho_H^{|\Phi\rangle}$ to be $|\Phi\rangle$. We assume the dishonest players hold the purification of $\rho_H^{|\Psi\rangle}, \rho_H^{|\Phi\rangle}$. Since all purifications of a state are unitarily equivalent, we have

$$F(\rho_H^{|\Psi\rangle}, \rho_H^{|\Phi\rangle}) = \max_{V_D,W_D} |\langle\Psi| (\mathbb{1}_H \otimes V_D)(\mathbb{1}_H \otimes W_D^\dagger) |\Phi\rangle|^2. \tag{5.30}$$

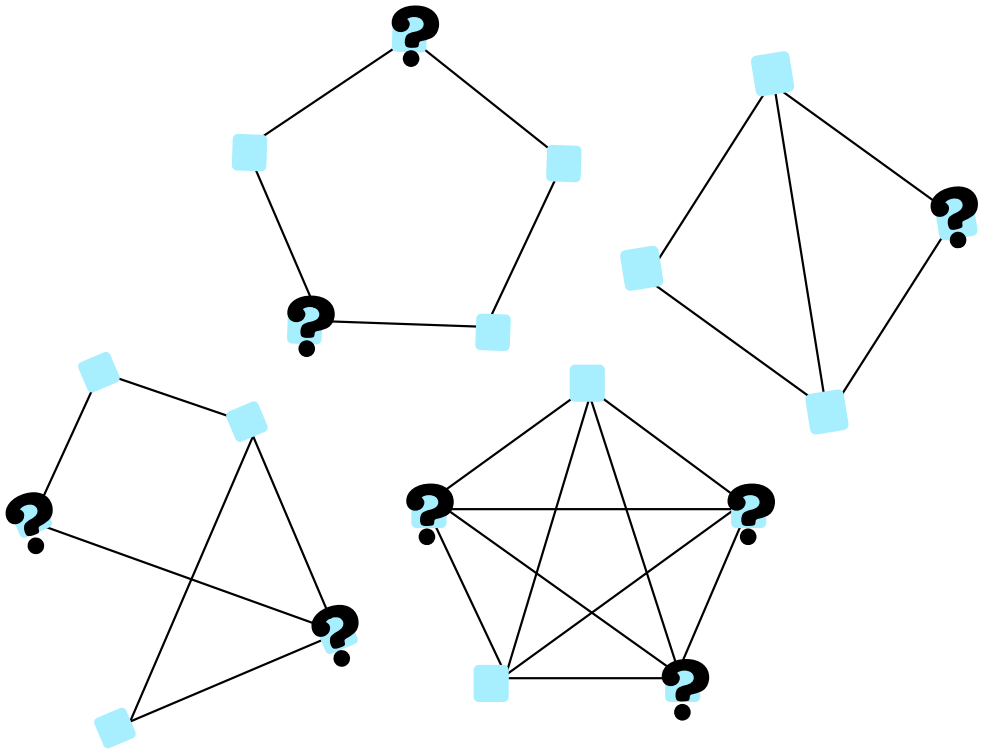
Now, let us write $U_D^\dagger = V_D W_D^\dagger$. Then, we have

$$F(\rho_H^{|\Psi\rangle}, \rho_H^{|\Phi\rangle}) = \max_{U_D} |\langle\Psi| \mathbb{1}_H \otimes U_D^\dagger |\Phi\rangle|^2 = \max_{U_D} F(U_D |\Psi\rangle, |\Phi\rangle) \equiv F'(|\Psi\rangle). \tag{5.31}$$

□

Chapter 6

Verification of graph states in an untrusted network



6.1 Introduction

The power of graph states extends across the field of quantum information, with their inherent multipartite entanglement leading them to be promising candidates for a variety of tasks. As quantum states that correspond to mathematical graphs, with entanglement links between each pair of vertices connected by an edge, graph states may possess varying degrees of entanglement that render them ideal for applications ranging from quantum computation [36,50,167] and error-correction [29,168] to metrology [49,169] and much more [170,171].

The need for verification of graph states stemmed from their role as the central resource in measurement-based quantum computation (MBQC). In this paradigm, a computation is carried out by performing projective (hence irreversible) measurements on qubits entangled in a graph state. This is known as a one-way quantum computer [50,51,172]. The question of how to verify a quantum computation in this picture can then be broken down into verifying the creation of the graph state, and verifying the measurements.

One may also visualise a different type of scenario, where a graph state is distributed over a network of players each holding a share of the state. The verification of graph states over such networks could find uses in some fundamental cryptographic tasks. For example, in *secret sharing*, a player known as the Dealer wishes to distribute a secret to a group of players, in such a way that only certain authorised sets of players can access it by working together, while the unauthorised set cannot. Quantum secret sharing may refer to the sharing of a secret quantum state, or a classical secret by quantum means [48, 68]. It was shown by Markham and Sanders [52] that graph states are perfectly suited to this task, where the Dealer can encode the secret on a graph state and distribute it among the players. A further example is the previously mentioned task of *secure multiparty quantum computation*, where a set of (possibly dishonest) players wish to compute some function that depends on each of their input states, while keeping these inputs private [70, 71].

In this Chapter, we investigate how players in a network can verify that they share a graph state, even if some among them are dishonest. We assume each player holds one qubit of the graph state; this corresponds to each vertex of the graph. Such an analysis could be used

to verify quantum computation in the MBQC picture in the presence of untrusted players, or for verification of entanglement for distributed communication or computational tasks. We discuss and define the types of security statements one can make in such a scenario, where there is no guarantee that the dishonest players follow the protocol. In fact, as in the previous Chapter, we will assume the strongest adversarial model, where they may do anything to the qubits they hold, and may even cooperate with each other and the source of graph states to disrupt the protocol.

In keeping with the central theme of this thesis, we aim to bring such verification methods closer to experimental implementation; however, in the case of general graph states with any player allowed to be dishonest, we will see that an impractically large number of copies of the graph state are required. On the other hand, our protocol only requires many separate copies, rather than more complicated procedures such as encoding in error-correcting codes. Further, we provide the most general recipe; when verifying a particular graph state, the players will have more information about its structure that they can use to modify the resources required for the protocol. In addition, any information known about the dishonest players can be used to dramatically reduce the requirements; for example, if some specific players are suspected to be dishonest, or if it is known that they are in the neighbourhood of each other. By making use of such information, our protocol can be made very practical, and we give explicit examples of this in later sections for cluster states, complete and cycle graphs.

6.2 Previous work

A natural starting point would be the verification protocol of Pappa et al. [160], along with the loss-tolerant and experimentally demonstrated version [31], that we discussed in the previous Chapter. While these protocols were specific for GHZ states, we will consider the same powerful adversarial model as in their work, and thus aim to obtain similar statements for graph states. Due to the symmetry of GHZ states (which are equivalent to complete graphs), we would expect their scenario to be much simpler than for arbitrary graph states, and as a consequence the results to be much better. However, since complete graphs form a

special case of the verification of general graph states, we will do a comparison of the two approaches at the end.

The application of graph state verification to verifiable quantum computing in the MBQC picture has prompted much of the work in this area. However, such approaches consider the client-server setting, where an honest client wants to test a possibly dishonest server that claims to be making a specific graph state. Here, the client receives the entire graph state, and makes measurements to test it. This can be thought of as a network comprising of all honest players. For example, Markham and Krause [112] proposed a protocol for graph state verification in such a setting. As we saw in Chapter 3, the untrusted source of graph states is asked to produce many copies of the state and distribute it amongst the players. In each round, a stabiliser is randomly chosen to be measured from the entire stabiliser set. Each player performs their part of the stabiliser measurement on their qubit. In this way, they achieve a soundness bound inversely proportional to the total number of copies. Similar approaches were used in the works by Hayashi and Morimae [173], and Takeuchi and Morimae [174].

Another recent result by Takeuchi et al. [175], which our approach is based on, provides a resource-efficient way of verifying graph states for quantum computation. This again fits into the client-server setting. Although this protocol is similar to previous works, their analysis uses the Serfling bound [176], a probability inequality from classical statistics. While such an approach places more constraints on the protocol parameters, for a given fidelity (with a fixed relationship to success probability), it can be more efficient in terms of the number of copies needed. Further, it has a natural way of incorporating the capacity to fail for a certain number of test runs, as we do in Chapter 3. We will discuss and extend their work more in further sections.

Finally, we discuss the work of McKague [177] on self-testing graph states. In the setting considered here, the players wish to certify a graph state without trusting the operations of their devices. McKague derives bounds on the closeness of the actual and ideal shared states, given some measurement statistics, using the SWAP isometry tool (similarly to our approach in Chapter 4). While this works well in the ideal case, the robust bound on the trace distance

for self-testing an n-qubit graph state, given ϵ-close correlations, scales as $O(n^3\sqrt{\epsilon})$. Further, this scenario enforces the requirement of no communication between the players. Since we wish to assume a powerful adversarial model where the dishonest players can work together, but without the need for device-independence, our approach is rather different.

6.3 Network model

- *Players*: There are n players in total. The set of honest players is H; the set of dishonest players is D. Honest players follow the protocol. Dishonest players might not follow the protocol, and can apply any cheating strategy on their systems.

- *State*: The quantum state they share is untrusted. The players obtain the state they require from an untrusted source, who may produce a different state in each round, and can collaborate with the dishonest players. An honest source produces the desired graph state, $|\mathcal{G}\rangle$.

- *Operations*: Their measurement devices are trusted. Honest players are only required to apply local operations. Dishonest players can apply operations on the part of the state that belongs to the whole dishonest set.

- *Classical channels*: Each pair of players shares a secure classical channel, which they can use to privately send classical information. (This is is necessary to retain privacy of the honest players' measurement settings and outcomes, without which the dishonest players could cheat perfectly.)

6.4 Protocol

Throughout this Chapter, we will use and adapt the verification protocol from Takeuchi et al. [175], where they employ the Serfling bound to assess the fidelity of a graph state generated by an untrusted source. As mentioned, in their work, an untrusted server generates graph states and sends them to an honest client, who wishes to verify that the graph state is the one

she asked for. In Protocol 6.1, we adapt their protocol to our scenario, where an untrusted source distributes an arbitrary graph state amongst a network of (possibly dishonest) players. Note that here we assume an honest player plays the role of the Verifier.

As we saw in previous Chapters, the intuition behind such a protocol is that only the ideal state will pass all stabiliser tests, and so by randomly choosing which stabiliser to measure, the players can force a dishonest source to provide ideal states to avoid being caught. Additionally, in our case we would like to account for any number of dishonest players, who may work together and coordinate with a dishonest source. While the original protocol [175] only requires measuring the stabiliser generators of the graph state the players wish to verify, in order to extend this to any graph state with any number of dishonest players, we will see that the players must measure the full set of stabilisers. This is due to the power of our adversarial model; we will show in later sections how to reduce this requirement if we have more information about the dishonest players, or for specific graphs.

While the idea behind Protocol 6.1 is the same as previous graph state verification schemes as in Protocol 3.3 and [112], the analysis is rather different as a consequence of the Serfling bound. This is a probability inequality relating correlations observed from a subset of data to the expected correlations in the remaining data. This allows us to make a statement about the untested states, given the measurement outcomes from the stabiliser tests.

6.5 Security analysis

In our scenario, an untrusted source claims to be generating the n-qubit graph state $|\mathcal{G}\rangle$. The players perform Protocol 6.1, measuring the full set of 2^n stabilisers, to test whether the state they receive in each round, $|\Psi\rangle$, is the ideal graph state $|\mathcal{G}\rangle$, even in the presence of dishonest players. Recall that in a network with dishonest players who may collaborate with the source of the state, we may take the state $|\Psi\rangle$ to be pure, as the dishonest players can purify it by adding a reference system. Further, in such a network, we can only make statements on the fidelity up to local operations on the dishonest part. As we showed in Appendix 5.A.2, this is equal to the fidelity of the reduced states of the honest players.

Protocol 6.1 VERIFICATION OF GRAPH STATE (adapted from [175])

Input: The players choose values of N_{test}, N_{total}.
Goal: The players verify that they share the n-qubit graph state $|\mathcal{G}\rangle$.

1: An untrusted source generates N_{total} copies of the graph state, and sends the shares to the players.

2: The players repeat the following for $j = 1, ..., 2^n$:

   (a) The Verifier chooses N_{test} copies from the remaining $N_{total} - (j-1)N_{test}$ copies independently and uniformly at random.

   (b) For each copy, the Verifier instructs each player to perform the measurement corresponding to their part of the stabiliser $\mathcal{S}_j$.

   (c) For each copy, the players send their measurement outcome to the Verifier, who calculates the total measurement outcome. The copy passes the test if the total measurement outcome is $+1$. Let $N_{pass,j}$ be the number of copies that pass the stabiliser test for $\mathcal{S}_j$.

3: The Verifier uniformly randomly chooses a single copy from the remaining $\mathsf{N} \equiv N_{total} - 2^n N_{test}$ copies that were not used for the tests in the previous steps. The chosen single copy is called the target copy. The others are discarded.

4: If $N_{pass} \equiv \sum_{j=1}^{2^n} N_{pass,j} \geq 2^n N_{test} - \frac{N_{test}}{2\times 2^n}$, they use the target copy for their application; otherwise the target copy is discarded.

Let us then take $\rho_H^{|\mathcal{G}\rangle}$ to be the reduced state of the honest players in the ideal case (*i.e.* when they share $|\mathcal{G}\rangle$), and ρ_H^{avg} to be the reduced state of the honest players of the averaged state of the target copy (over all random selections from the remaining N copies).

We prove the security of our protocol in the following Theorem.

Theorem 6.1. *If we set $N_{total} = 2 \times 2^n N_{test}$ and $N_{test} = \lceil m 2^{4n} \ln n \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol 6.1 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n \left(1 - \frac{N_{pass}}{2^n N_{test}}\right) \tag{6.1}$$

is at least $\left[1 - n^{-\frac{2cm}{3}}\right]^{2^n}$, where m, c are positive constants chosen such that the probability is greater than zero and $0 < c < \frac{(2^n-1)^2}{4}$.

Proof. Our proof proceeds in stages. We will start by proving that the only state that can pass all stabiliser tests perfectly is the ideal graph state, up to local unitaries on the dishonest parts of the state. This means that in order to pass perfectly, the source must create entanglement between the honest and dishonest players. This is given in the following Lemma.

Lemma 6.2. *The only state that can pass all stabiliser tests perfectly in each round is* $|\Psi\rangle = U_D |\mathcal{G}\rangle$*, where* U_D *is a unitary on the dishonest part of the state.*

Proof. Let s be the Schmidt rank of the graph state $|\mathcal{G}\rangle$ corresponding to the partition (H, D) into honest and dishonest vertices, $|\mathcal{H}\rangle$ be the state corresponding to the honest subgraph, and $E_{\mathcal{H}}$ be the set of edges within the honest subgraph.

Let $bn(x)$ be a function that converts a decimal number x into its binary representation, and let us define classical $|H|$-bit strings $\bar{\mathbf{z}}, \bar{\mathbf{x}} \in \{bn(0), ..., bn(2^{|H|} - 1)\}$, where $|H|$ is the number of honest players in the network. We will use z_a to refer to the a^{th} element of $\bar{\mathbf{z}}$.

We will start by writing the Schmidt decomposition of the ideal state for the partition (H, D) from [170]. Some terms in $\{|\bar{\mathbf{z}}\rangle\}$ may be grouped together as they have the same dishonest part, as given by

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \otimes \prod_{a\in H} \Big(\prod_{b\in N(a)} \sigma_Z^{(b)} \Big)^{z_a} |\mathcal{G} - \mathcal{H}\rangle_D \tag{6.2}$$

$$= \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \otimes \left|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\right\rangle_D , \tag{6.3}$$

where $f(\bar{\mathbf{z}})$ depends on $\bigoplus_{i\in N(d)} z_i, \forall d \in D$, and $\mathcal{G} - \mathcal{H}$ is the dishonest subgraph. Then, $\left|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\right\rangle$ is the state corresponding to the dishonest subgraph with σ_Zs applied to some vertices depending on $\bar{\mathbf{z}}$. This means that for terms where $\bigoplus_{i\in N(d)} z_i$ is the same for all $d \in D$, the corresponding dishonest part $\left|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\right\rangle$ is the same, and so the $|\bar{\mathbf{z}}\rangle$s of these are grouped together.

Let $\left|\mathcal{H}_{(\bar{\mathbf{x}})}\right\rangle$ be the state corresponding to the honest subgraph with σ_Zs applied according to $\bar{\mathbf{x}}$ (for example, $\left|\mathcal{H}_{(001)}\right\rangle$ corresponds to a 3-qubit graph with σ_Z applied to the third qubit). The set $\{\left|\mathcal{H}_{(\bar{\mathbf{x}})}\right\rangle\}$ for all $\bar{\mathbf{x}}$ forms a complete basis (the graph state basis), as does the set $\{|\bar{\mathbf{z}}\rangle\}$.

The unknown state in any round of Protocol 6.1 can then be written using the following decomposition:

$$\text{honest computational basis:} \quad |\Psi\rangle = \sum_{\overline{\mathbf{z}}} \alpha_{\overline{\mathbf{z}}} \left|\overline{\mathbf{z}}\right\rangle_H \otimes |\psi_{\overline{\mathbf{z}}}\rangle_D \,, \tag{6.4}$$

$$\text{honest subgraph basis:} \quad |\Psi\rangle = \sum_{\overline{\mathbf{x}}} \beta_{\overline{\mathbf{x}}} \left|\mathcal{H}_{(\overline{\mathbf{x}})}\right\rangle_H \otimes |\phi_{\overline{\mathbf{x}}}\rangle_D \,, \tag{6.5}$$

where $\alpha_{\overline{\mathbf{z}}}, \beta_{\overline{\mathbf{x}}}$ are complex coefficients, and both sets $\{|\psi_{\overline{\mathbf{z}}}\rangle\}, \{|\phi_{\overline{\mathbf{x}}}\rangle\}$ are the corresponding states on the dishonest side. So far, we have assumed nothing about the portion of the state in control of the dishonest players, since no matter what the source supplies, the dishonest players may do anything to their part to cheat in the protocol.

In Protocol 6.1, the test measurements are the elements $\mathcal{S}_{j\in\{1,\ldots,2^n\}}$ belonging to the full stabiliser group. These measurements are generated by the stabiliser generators $K_{i\in\{1,\ldots,n\}}$ of each qubit i. Thus, the full stabiliser group $\mathcal{S}$ is given by

$$\mathcal{S} = \langle \{K_i = X_i \prod_{e\in N(i)} Z_e\}_{i=1}^n \rangle. \tag{6.6}$$

We want to determine the form of the state given that all the test measurements pass perfectly. Let us now group the test measurements into two sets, such that Group 1 contains only $\mathbb{1}, Z$ for the honest part, and Group 2 contains everything else.

We first consider the measurements in Group 1. This set contains the stabiliser generators corresponding to the dishonest qubits, *i.e.* $K_{i\in D}$. For each dishonest qubit, the honest part of the corresponding stabiliser generator measurement will be composed of Z measurements on the honest qubits that are in the neighbourhood of the dishonest qubit, and $\mathbb{1}$ on those that are not. We can then write the set of stabiliser generators belonging to Group 1 as

$$\{\forall d \in D, \Big[\bigotimes_{i\in N(d)} Z_i \bigotimes_{i\notin N(d)} \mathbb{1}_i \Big]_H \otimes (M'_d)_D\}, \tag{6.7}$$

where $(M'_d)_D$ is the measurement on the dishonest part, the form of which does not matter

here. Let $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ be two strings in the computational basis expansion of $|\Psi\rangle$. If $\bigoplus_{i\in N(d)} z_i \neq \bigoplus_{i\in N(d)} z'_i$, then each honest measurement $\bigotimes_{i\in N(d)} Z_i \bigotimes_{i\notin N(d)} \mathbb{1}_i$ will give different outcomes for $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$, since the outcome of the Z measurement on all $i \in N(d)$ depends on the parity of the string (how many 1s). So, to pass perfectly, $(M'_d)_D$ must also give different outcomes. In order to do this, the dishonest players must be able to guess the honest players' outcome perfectly, which means that they must be able to perfectly discriminate between the corresponding $|\psi_{\overline{\mathbf{z}}}\rangle, |\psi_{\overline{\mathbf{z}}'}\rangle$; this tells them the outcome they should get in order to pass the test. This means that we must have $\langle\psi_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}'}\rangle = 0$. In general, we can write this as

$$\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}', \text{ if } \exists d \in D \text{ such that } \bigoplus_{i\in N(d)} z_i \neq \bigoplus_{i\in N(d)} z'_i, \text{ then } \langle\psi_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}'}\rangle = 0. \tag{6.8}$$

We will now see that if the measurements in Group 2 pass perfectly, we get certain $\beta_{\overline{\mathbf{x}}} = 0$, and for all $\beta_{\overline{\mathbf{x}}} \neq 0$, the corresponding $|\phi_{\overline{\mathbf{x}}}\rangle$s will be orthogonal to each other.

To prove orthogonality, note that the set of stabiliser generators in Group 2 contain all the stabiliser measurements with X in the honest part (the stabiliser generator corresponding to each qubit in the honest set). So, the honest part of the measurements in the group is of the form $\{X_1M_2M_3...M_{|H|}, M_1X_2M_3...M_{|H|}, M_1M_2X_3...M_{|H|}, ..., M_1...X_{|H|}\}$, where the honest measurement $M_{i\in\{1,...,|H|\}}$ is either $\mathbb{1}, Z$. Since no two states in the $\left|\mathcal{H}_{(\overline{\mathbf{x}})}\right\rangle$ basis will give the same outcome for every one of these measurements, in order to pass perfectly, the dishonest players must be able to discriminate between all corresponding $|\phi_{\overline{\mathbf{x}}}\rangle$ to perfectly guess the honest outcome. We can write this as

$$\forall \overline{\mathbf{x}} \neq \overline{\mathbf{x}}', \langle\phi_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}'}\rangle = 0. \tag{6.9}$$

To determine which $\beta_{\overline{\mathbf{x}}} = 0$, we will use the measurements with dishonest part $M'_D = (\mathbb{1}...\mathbb{1})'$. Let $A \subset H$ be a set containing vertices in H such that all $d \in D$ has an even number of neighbours in A. (Note that there may be multiple such sets A.) Now, let K_i be the stabiliser generator of qubit i of $|\mathcal{G}\rangle$, and k_i be the stabiliser generator of qubit i of $|\mathcal{H}\rangle$. We

can then write a subset of the Group 2 measurements as

$$\prod_{i\in A} K_i = \prod_{i\in A} (k_i)_H \otimes \mathbb{1}'_D. \tag{6.10}$$

When the dishonest players are asked to measure $\mathbb{1}$, they must always give outcome $+1$. So, in order to pass perfectly, the honest part must also give $+1$ outcome. In the expansion of the state in Equation (6.5), if for any set A, we do not have an even number of σ_Zs on the qubits $i \in A$ in the honest subgraph, then the honest measurement will not give outcome $+1$. Since the positions of the σ_Zs are determined by the string $\overline{\mathbf{x}}$, passing the Group 2 measurements perfectly tells us that

$$\text{if } \exists A \text{ s.t. } \bigoplus_{i\in A} x_i = 1, \text{ then } \beta_{\overline{\mathbf{x}}} = 0. \tag{6.11}$$

In this way, we are left with s non-zero $\beta_{\overline{\mathbf{x}}}$s. We can write the set A as

$$A = \{i \in H \mid \exists \overline{\mathbf{z}}, \overline{\mathbf{z}}' \text{ such that } \forall d \in D, \bigoplus_{i\in N(d)} z_i = \bigoplus_{i\in N(d)} z'_i, \text{ and } z_i \oplus z'_i = 1\}. \tag{6.12}$$

Writing $i \in A$ using Equation (6.12), the condition on $\beta_{\overline{\mathbf{x}}}$ in Equation (6.11) can be written as

$$\begin{aligned} &\text{if } \exists \overline{\mathbf{z}}, \overline{\mathbf{z}}' \text{ such that } \forall d \in D, \bigoplus_{i\in N(d)} z_i = \bigoplus_{i\in N(d)} z'_i, \\ &\text{then } \beta_{\overline{\mathbf{x}}} = 0 \text{ if } \bigoplus_{i\in H} (z_i \oplus z'_i) \wedge x_i = 1. \end{aligned} \tag{6.13}$$

We will now relate the two expressions we have for the honest parts of the state. The graph state basis can be expressed in terms of the computational basis by

$$\left|\mathcal{H}_{(\overline{\mathbf{x}})}\right\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} \left|\overline{\mathbf{z}}\right\rangle. \tag{6.14}$$

Substituting in Equation (6.5) and grouping, we get

$$
\begin{aligned}
|\Psi\rangle &= \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{x}}} \beta_{\bar{\mathbf{x}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} |\bar{\mathbf{z}}\rangle_H |\phi_{\bar{\mathbf{x}}}\rangle_D \\
&= \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{x}}} \beta_{\bar{\mathbf{x}}} (-1)^{\bigoplus_i x_i \wedge z_i} |\phi_{\bar{\mathbf{x}}}\rangle_D .
\end{aligned} \tag{6.15}
$$

Comparing the above expression with Equation (6.4) in terms of the coefficients of each $|\bar{\mathbf{z}}\rangle$,

$$
\begin{aligned}
\alpha_{\bar{\mathbf{z}}} |\psi_{\bar{\mathbf{z}}}\rangle &= (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{x}}} \beta_{\bar{\mathbf{x}}} (-1)^{\bigoplus_i x_i \wedge z_i} |\phi_{\bar{\mathbf{x}}}\rangle , \ \forall \bar{\mathbf{z}}, \\
(-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\bar{\mathbf{z}}} |\psi_{\bar{\mathbf{z}}}\rangle &= \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{x}}} \beta_{\bar{\mathbf{x}}} (-1)^{\bigoplus_i x_i \wedge z_i} |\phi_{\bar{\mathbf{x}}}\rangle , \ \forall \bar{\mathbf{z}}.
\end{aligned} \tag{6.16}
$$

On the other hand, expressing the computational basis in terms of the graph state basis gives

$$
|\bar{\mathbf{z}}\rangle = \frac{1}{\sqrt{2^{|H|}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \sum_{\bar{\mathbf{x}}} (-1)^{\bigoplus_i x_i \wedge z_i} \left|\mathcal{H}_{(\bar{\mathbf{x}})}\right\rangle . \tag{6.17}
$$

Substituting in Equation (6.4) and grouping, we get

$$
\begin{aligned}
|\Psi\rangle &= \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} \alpha_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \sum_{\bar{\mathbf{x}}} (-1)^{\bigoplus_i x_i \wedge z_i} \left|\mathcal{H}_{(\bar{\mathbf{x}})}\right\rangle_H |\psi_{\bar{\mathbf{z}}}\rangle_D \\
&= \sum_{\bar{\mathbf{x}}} \left|\mathcal{H}_{(\bar{\mathbf{x}})}\right\rangle_H \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} \alpha_{\bar{\mathbf{z}}} |\psi_{\bar{\mathbf{z}}}\rangle_D .
\end{aligned} \tag{6.18}
$$

Comparing the above expression with Equation (6.5) in terms of the coefficients of $\left|\mathcal{H}_{(\bar{\mathbf{x}})}\right\rangle$,

$$
\beta_{\bar{\mathbf{x}}} |\phi_{\bar{\mathbf{x}}}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} \alpha_{\bar{\mathbf{z}}} |\psi_{\bar{\mathbf{z}}}\rangle , \ \forall \bar{\mathbf{x}}. \tag{6.19}
$$

Note that for certain $\bar{\mathbf{x}}$, $\beta_{\bar{\mathbf{x}}} = 0$. In Equation (6.16), some terms will then be zero. In Equation (6.19), the whole left-hand side will then be zero. If any of the expressions are equal to zero, we can use them to show that the terms are grouped as in the Schmidt decomposition of $|\mathcal{G}\rangle$ in Equation (6.3), which will allow us to simplify Equations (6.19) and (6.4). If none of the expressions are equal to zero, we will see that the same simplification applies. This is

encapsulated in Lemma 6.2.1.

Lemma 6.2.1. *Equations (6.19) and (6.4) can be written as*

$$\beta_{\overline{\boldsymbol{v}}} \left|\phi_{\overline{\boldsymbol{v}}}\right\rangle = \frac{\sqrt{2^{|H|}}}{s} \sum_{\overline{\boldsymbol{w}}} (-1)^{\bigoplus_i v_i \wedge w_i} \alpha_{\overline{\boldsymbol{w}}} \left|\psi_{\overline{\boldsymbol{w}}}\right\rangle, \quad \forall \overline{\boldsymbol{v}}, \tag{6.20}$$

$$\left|\Psi\right\rangle = \sum_{\overline{\boldsymbol{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\boldsymbol{w}}} \left|\overline{\boldsymbol{z}}\right\rangle_H \otimes \left|\psi_{\overline{\boldsymbol{w}}}\right\rangle_D, \tag{6.21}$$

where $\overline{\boldsymbol{w}}, \overline{\boldsymbol{v}} \in \{bn(0), ..., bn(s-1)\}$.

Proof. We will prove this in a series of steps. First, we show that the $|\psi_{\overline{\mathbf{z}}}\rangle$s are equal for the $|\overline{\mathbf{z}}\rangle$ terms that are grouped together in the Schmidt decomposition of $|\mathcal{G}\rangle$ in Equation (6.3), and that their corresponding $\alpha_{\overline{\mathbf{z}}}$s are equal up to ± 1. For any strings $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\forall d \in D, \bigoplus_{i\in N(d)} z_i = \bigoplus_{i\in N(d)} z'_i$, we have using Equation (6.16),

$$\begin{aligned}(-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{z}}} \left|\psi_{\overline{\mathbf{z}}}\right\rangle - (-1)^{\bigoplus_{(k,l)\in E_H} z'_k \wedge z'_l} \alpha_{\overline{\mathbf{z}}'} \left|\psi_{\overline{\mathbf{z}}'}\right\rangle \\ = \frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{x}}} \beta_{\overline{\mathbf{x}}} \Big[(-1)^{\bigoplus_i x_i \wedge z_i} - (-1)^{\bigoplus_i x_i \wedge z'_i}\Big] \left|\phi_{\overline{\mathbf{x}}}\right\rangle.\end{aligned} \tag{6.22}$$

From Equation (6.13), we know that for such strings $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$, if $\bigoplus_i (z_i \oplus z'_i) \wedge x_i = 1$, then $\beta_{\overline{\mathbf{x}}} = 0$. Otherwise, for the terms where $\beta_{\overline{\mathbf{x}}} \neq 0$, we have

$$0 = \bigoplus_i (z_i \oplus z'_i) \wedge x_i = \bigoplus_i \Big[(x_i \wedge z_i) \oplus (x_i \wedge z'_i)\Big] = \Big[\bigoplus_i (x_i \wedge z_i)\Big] \oplus \Big[\bigoplus_i (x_i \wedge z'_i)\Big], \tag{6.23}$$

which gives $\bigoplus_i x_i \wedge z_i = \bigoplus_i x_i \wedge z'_i$, and subsequently

$$(-1)^{\bigoplus_i x_i \wedge z_i} = (-1)^{\bigoplus_i x_i \wedge z'_i}. \tag{6.24}$$

Substituting in Equation (6.22), we get that $\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\forall d \in D, \bigoplus_{i\in N(d)} z_i = \bigoplus_{i\in N(d)} z'_i$,

$$(-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{z}}} \left|\psi_{\overline{\mathbf{z}}}\right\rangle = (-1)^{\bigoplus_{(k,l)\in E_H} z'_k \wedge z'_l} \alpha_{\overline{\mathbf{z}}'} \left|\psi_{\overline{\mathbf{z}}'}\right\rangle. \tag{6.25}$$

Next, we will simplify the expression for $\beta_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}}\rangle$, by substituting Equations (6.25) and (6.24) in Equation (6.19) to get

$$\begin{aligned}\beta_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}}\rangle &= \frac{1}{\sqrt{2^{|H|}}}\sum_{\overline{\mathbf{z}}}(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k\wedge z_l}(-1)^{\overset{\oplus}{i} x_i\wedge z_i}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle\,,\ \forall\overline{\mathbf{x}} \text{ such that } \beta_{\overline{\mathbf{x}}}\neq 0\\ &= \frac{1}{\sqrt{2^{|H|}}}\Big[\sum_{\substack{\overline{\mathbf{z}} \text{ s. t.}\\ \overset{\oplus}{i\in N(d_1)} z_i=0\wedge\ldots\\ \wedge\overset{\oplus}{i\in N(d_{|D|})} z_i=0}}(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k\wedge z_l}(-1)^{\overset{\oplus}{i} x_i\wedge z_i}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle\\ &\quad+\ldots+\sum_{\substack{\overline{\mathbf{z}} \text{ s. t.}\\ \overset{\oplus}{i\in N(d_1)} z_i=1\wedge\ldots\\ \wedge\overset{\oplus}{i\in N(d_{|D|})} z_i=1}}(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k\wedge z_l}(-1)^{\overset{\oplus}{i} x_i\wedge z_i}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle\Big].\end{aligned} \tag{6.26}$$

There are s non-zero expressions for $\beta_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}}\rangle$, since there are s non-zero $\beta_{\overline{\mathbf{x}}}$s. There are also s sum terms on the right-hand side of the above expression. There are a total of $2^{|H|}$ terms of $\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle$, grouped together if $\forall d\in D$, $\overset{\oplus}{i\in N(d)} z_i$ is the same. This means that, within each of the s sum terms, there are $\frac{2^{|H|}}{s}$ terms. From Equation (6.25), we know that $(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k\wedge z_l}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle$ is the same for each of these terms. Further, we know from Equation (6.24) that $(-1)^{\overset{\oplus}{i} x_i\wedge z_i}$ is the same for each of these terms (since $\beta_{\overline{\mathbf{x}}}\neq 0$). Then, we can write our expression using s terms (corresponding to each sum term in the above expression).

In this way, we are left with terms depending on s unique variables that can take any value 0 or 1, instead of $2^{|H|}$ variables that can only take certain values. Defining new variables $\overline{\mathbf{w}},\overline{\mathbf{v}}\in\{bn(0),\ldots,bn(s-1)\}$, we can write the above as

$$\beta_{\overline{\mathbf{v}}}|\phi_{\overline{\mathbf{v}}}\rangle = \frac{1}{\sqrt{2^{|H|}}}\frac{2^{|H|}}{s}\sum_{\overline{\mathbf{w}}}(-1)^{\overset{\oplus}{i} v_i\wedge w_i}\alpha_{\overline{\mathbf{w}}}|\psi_{\overline{\mathbf{w}}}\rangle = \frac{\sqrt{2^{|H|}}}{s}\sum_{\overline{\mathbf{w}}}(-1)^{\overset{\oplus}{i} v_i\wedge w_i}\alpha_{\overline{\mathbf{w}}}|\psi_{\overline{\mathbf{w}}}\rangle\,,\quad\forall\overline{\mathbf{v}}. \tag{6.27}$$

Note that $\forall\overline{\mathbf{w}}\neq\overline{\mathbf{w}}'$, $\langle\psi_{\overline{\mathbf{w}}}|\psi_{\overline{\mathbf{w}}'}\rangle=0$, from Equation (6.8) and the fact that any two states with different $\overline{\mathbf{w}}$ have different $\overset{\oplus}{i\in N(d)} z_i$ for some $d\in D$. As before, $\forall\overline{\mathbf{v}}\neq\overline{\mathbf{v}}'$, $\langle\phi_{\overline{\mathbf{v}}}|\phi_{\overline{\mathbf{v}}'}\rangle=0$, from Equation (6.9). This means that now, instead of having $2^{|H|}$ variables $\overline{\mathbf{z}},\overline{\mathbf{x}}\in\{bn(0),\ldots,bn(2^{|H|}-1)\}$, we have s variables $\overline{\mathbf{w}},\overline{\mathbf{v}}\in\{bn(0),\ldots,bn(s-1)\}$.

Finally, we simplify the computational basis expression for $|\Psi\rangle$ in Equation (6.4). The terms should now be grouped as in Equation (6.3), with s terms, as

$$|\Psi\rangle = \sum_{\overline{\mathbf{z}}} \alpha_{\overline{\mathbf{z}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{z}}}\rangle_D = \sum_{\overline{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{w}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{w}}}\rangle_D , \tag{6.28}$$

where $\overline{\mathbf{w}} = f(\overline{\mathbf{z}})$ depends on $\bigoplus_{i\in N(d)} z_i, \forall d \in D$.

If none of the expressions are equal to zero, we have $s = 2^{|H|}$, and so we can simply rename $\overline{\mathbf{z}}$ as $\overline{\mathbf{w}}$, as they take values from the same set $\{bn(0), ..., bn(s-1)\}$. □

Our next aim is to determine the value of $\alpha_{\overline{\mathbf{w}}}$. From the normalisation condition, $\langle\Psi|\Psi\rangle = 1$, we have

$$\sum_{\overline{\mathbf{w}}} \frac{2^{|H|}}{s} |\alpha_{\overline{\mathbf{w}}}|^2 = 1 \implies \sum_{\overline{\mathbf{w}}} |\alpha_{\overline{\mathbf{w}}}|^2 = \frac{s}{2^{|H|}}, \tag{6.29}$$

since there are $\frac{2^{|H|}}{s}$ terms of $|\overline{\mathbf{z}}\rangle$ corresponding to each $\overline{\mathbf{w}}$, as we saw before.

To get the orthogonality conditions, we take the overlap of each non-zero expression for $\beta_{\overline{\mathbf{v}}} |\phi_{\overline{\mathbf{v}}}\rangle$ with another non-zero expression for $\beta_{\overline{\mathbf{v}}'} |\phi_{\overline{\mathbf{v}}'}\rangle$, to get $(s-1)$ equations for all $\overline{\mathbf{v}} \neq \overline{\mathbf{v}}'$ given by

$$\beta^\dagger_{\overline{\mathbf{v}}} \beta_{\overline{\mathbf{v}}'} \langle\phi_{\overline{\mathbf{v}}}|\phi_{\overline{\mathbf{v}}'}\rangle = 0 = \frac{2^{|H|}}{s^2} \Big[\sum_{\overline{\mathbf{w}}} (-1)^{\bigoplus_i v_i \wedge w_i} (-1)^{\bigoplus_i v'_i \wedge w_i} |\alpha_{\overline{\mathbf{w}}}|^2 \langle\psi_{\overline{\mathbf{w}}}|\psi_{\overline{\mathbf{w}}}\rangle \Big], \tag{6.30}$$

which we can write as

$$\sum_{\overline{\mathbf{w}}} (-1)^{\bigoplus_i p_i \wedge w_i} |\alpha_{\overline{\mathbf{w}}}|^2 = 0, \quad \forall \overline{\mathbf{p}} \in \{bn(1), ..., bn(s-1)\}. \tag{6.31}$$

(Note that since the overlap is taken with two different expressions, $\overline{\mathbf{p}}$ can never be $0...0$.)

We will now solve the s equations for s variables (from the normalisation and orthogonality conditions) using the matrix method, formulating the system of equations as $\mathcal{A}u = b$. The matrix $\mathcal{A}$ is of size $s \times s$, while u, b are of size $s \times 1$. u is a column vector containing each $|\alpha_{\overline{\mathbf{w}}}|^2$, and b is a column vector giving the normalisation and orthogonality conditions. $\mathcal{A}$ has

1s in its first row and column, and the other elements are ± 1. The 1s on the first row are from the normalisation condition. The 1s on the first column occur because for $\overline{\mathbf{w}} = 0...0$, the exponent of (-1) will always be 0 (since the AND of anything with $0...0$ gives $0...0$), and so the sign of $|\alpha_{\overline{\mathbf{w}}}|^2$ is always $+1$. We then have

$$\mathcal{A} = \begin{bmatrix} 1 & 1 & ... & 1 \\ 1 & \pm 1 & ... & \pm 1 \\ ... & ... & ... & ... \\ 1 & \pm 1 & ... & \pm 1 \end{bmatrix}, u = \begin{bmatrix} |\alpha_{00...00}|^2 \\ |\alpha_{00...01}|^2 \\ ... \\ |\alpha_{11...11}|^2 \end{bmatrix}, b = \frac{s}{2^{|H|}} \begin{bmatrix} 1 \\ 0 \\ ... \\ 0 \end{bmatrix}. \tag{6.32}$$

The values of $|\alpha_{\overline{\mathbf{w}}}|^2$ are then determined by

$$\begin{bmatrix} |\alpha_{00...00}|^2 \\ |\alpha_{00...01}|^2 \\ ... \\ |\alpha_{11...11}|^2 \end{bmatrix} = \mathcal{A}^{-1} \frac{s}{2^{|H|}} \begin{bmatrix} 1 \\ 0 \\ ... \\ 0 \end{bmatrix} = \frac{s}{2^{|H|}} \begin{bmatrix} \mathcal{A}^{-1}_{1,1} \\ \mathcal{A}^{-1}_{2,1} \\ ... \\ \mathcal{A}^{-1}_{s,1} \end{bmatrix}. \tag{6.33}$$

Thus, the solution to the set of equations is equal to $\frac{s}{2^{|H|}}$ times the first column of $\mathcal{A}^{-1}$. Using Equations (6.29) and (6.31), let us now write more precisely what the elements of $\mathcal{A}$ are:

$$\mathcal{A} = \begin{bmatrix} (-1)^{\oplus 00...00 \wedge 00...00} & (-1)^{\oplus 00...00 \wedge 00...01} & ... & (-1)^{\oplus 00...00 \wedge 11...11} \\ (-1)^{\oplus 00...01 \wedge 00...00} & (-1)^{\oplus 00...01 \wedge 00...01} & ... & (-1)^{\oplus 00...01 \wedge 11...11} \\ ... & ... & ... & ... \\ (-1)^{\oplus 11...11 \wedge 00...00} & (-1)^{\oplus 11...11 \wedge 00...01} & ... & (-1)^{\oplus 11...11 \wedge 11...11} \end{bmatrix}. \tag{6.34}$$

where by $\oplus \mathsf{a} \wedge \mathsf{b}$ we mean computing the AND operation of the strings a, b, and then XORing all the resulting bits (or, in other words, finding the parity of the AND of the strings a, b).

Let us take $\overline{\mathbf{p}}_i, \overline{\mathbf{w}}_j$ to be the i^{th} and j^{th} strings in the set $\{bn(0), ..., bn(s-1)\}$, where $i, j \in \{1, ..., s\}$. (For example, if $i = 2, j = 3$, we have $\overline{\mathbf{p}}_2 = 00...01, \overline{\mathbf{w}}_3 = 00...10$.) Then,

taking i to denote the row and j to denote the column, $\mathcal{A}$ is given by

$$\mathcal{A} = \begin{bmatrix} (-1)^{\oplus \overline{\mathbf{p}}_1 \wedge \overline{\mathbf{w}}_1} & (-1)^{\oplus \overline{\mathbf{p}}_1 \wedge \overline{\mathbf{w}}_2} & ... & (-1)^{\oplus \overline{\mathbf{p}}_1 \wedge \overline{\mathbf{w}}_s} \\ (-1)^{\oplus \overline{\mathbf{p}}_2 \wedge \overline{\mathbf{w}}_1} & (-1)^{\oplus \overline{\mathbf{p}}_2 \wedge \overline{\mathbf{w}}_2} & ... & (-1)^{\oplus \overline{\mathbf{p}}_2 \wedge \overline{\mathbf{w}}_s} \\ ... & ... & ... & ... \\ (-1)^{\oplus \overline{\mathbf{p}}_s \wedge \overline{\mathbf{w}}_1} & (-1)^{\oplus \overline{\mathbf{p}}_s \wedge \overline{\mathbf{w}}_2} & ... & (-1)^{\oplus \overline{\mathbf{p}}_s \wedge \overline{\mathbf{w}}_s} \end{bmatrix}. \tag{6.35}$$

In general, the $(i,j)^{\text{th}}$ element of $\mathcal{A}$ is given by

$$\mathcal{A}_{i,j} = (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_j}. \tag{6.36}$$

Note that since $\overline{\mathbf{p}}_i = \overline{\mathbf{w}}_i \forall i$, we have $\mathcal{A}_{i,j} = (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_j} = (-1)^{\oplus \overline{\mathbf{w}}_i \wedge \overline{\mathbf{p}}_j} = (-1)^{\oplus \overline{\mathbf{p}}_j \wedge \overline{\mathbf{w}}_i} = \mathcal{A}_{j,i}$, and so $\mathcal{A}$ is symmetric. We will now show that the inverse of the matrix $\mathcal{A}$ is given by $\mathcal{A}^{-1} = \frac{1}{s}\mathcal{A}$. To prove this, we just have to show that $\mathcal{A}\mathcal{A}^{-1} = \mathbb{1}$. Denoting $\mathcal{A}\mathcal{A} = \mathcal{M}$, we have

$$\mathcal{A}\mathcal{A}^{-1} = \mathcal{A}\frac{1}{s}\mathcal{A} = \frac{1}{s}\mathcal{A}\mathcal{A} = \frac{1}{s}\mathcal{M}. \tag{6.37}$$

The $(i,j)^{\text{th}}$ element of $\mathcal{M}$ is given by

$$\mathcal{M}_{i,j} = \sum_{k=1}^{s} (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_k} (-1)^{\oplus \overline{\mathbf{p}}_k \wedge \overline{\mathbf{w}}_j} = \sum_{k=1}^{s} (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_k} (-1)^{\oplus \overline{\mathbf{p}}_j \wedge \overline{\mathbf{w}}_k} = \sum_{k=1}^{s} (-1)^{\oplus (\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j) \wedge \overline{\mathbf{w}}_k}. \tag{6.38}$$

When $i = j$, we have $\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j = 00...00$, and so for every $\overline{\mathbf{w}}_k$, we always have $(-1)^0$. Thus, we have $\mathcal{M}_{i,i} = \sum_{k=1}^{s} 1 = s$. When $i \neq j$, the AND operation is performed on the same string $\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j$ and $\overline{\mathbf{w}}_k, \forall k$. In this case, $\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j \in \{bn(1), ..., bn(s-1)\}$, as their sum can only be $00...00$ if $i = j$. Thus, if we sum over the AND of this string with each possible $\overline{\mathbf{w}} \in \{00...00, ..., 11...11\}$, we get an equal number of $+1$s and -1s. So, this sum is equal to 0.

We can therefore say

$$\mathcal{M}_{i,j} = \delta_i^j s, \tag{6.39}$$

which means $\mathcal{M} = s\mathbb{1}$. Substituting in Equation (6.37), we find $\mathcal{A}\mathcal{A}^{-1} = \mathbb{1}$. Thus, $\mathcal{A}^{-1} = \frac{1}{s}\mathcal{A}$, which we substitute in Equation (6.33) to get

$$\begin{bmatrix} |\alpha_{0\ldots0}|^2 \\ |\alpha_{0\ldots1}|^2 \\ \ldots \\ |\alpha_{1\ldots1}|^2 \end{bmatrix} = \frac{s}{2^{|H|}} \begin{bmatrix} \mathcal{A}^{-1}_{1,1} \\ \mathcal{A}^{-1}_{2,1} \\ \ldots \\ \mathcal{A}^{-1}_{s,1} \end{bmatrix} = \frac{1}{s} \times \frac{s}{2^{|H|}} \begin{bmatrix} \mathcal{A}_{1,1} \\ \mathcal{A}_{2,1} \\ \ldots \\ \mathcal{A}_{s,1} \end{bmatrix} = \frac{1}{s} \times \frac{s}{2^{|H|}} \begin{bmatrix} 1 \\ 1 \\ \ldots \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2^{|H|}} \\ \frac{1}{2^{|H|}} \\ \ldots \\ \frac{1}{2^{|H|}} \end{bmatrix}. \tag{6.40}$$

This gives each $\alpha_{\overline{\mathbf{w}}} = \pm\frac{1}{\sqrt{2^{|H|}}}$. Let us substitute the value of $\alpha_{\overline{\mathbf{w}}}$ in Equation (6.28). We get

$$\begin{aligned} |\Psi\rangle &= \pm\frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{w}}}\rangle_D \\ &= \pm\frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l} |\overline{\mathbf{z}}\rangle_H \otimes \left|\psi_{(f(\overline{\mathbf{z}}))}\right\rangle_D . \end{aligned} \tag{6.41}$$

Finally, $\rho_H^{|\Psi\rangle}$ only depends on the honest Schmidt basis. Comparing the above expression with Equation (6.3) shows that the honest Schmidt basis of the actual state $|\Psi\rangle$ is equal to the honest Schmidt basis of the ideal state $|\mathcal{G}\rangle$, giving $\rho_H^{|\Psi\rangle} = \rho_H^{|\mathcal{G}\rangle}$. If $|\Psi\rangle$ is a purification of $\rho_H^{|\Psi\rangle}$, and $|\mathcal{G}\rangle$ is a purification of $\rho_H^{|\mathcal{G}\rangle}$, then due to the unitary equivalence of purifications, we must have $|\Psi\rangle = U_D |\mathcal{G}\rangle$ if all the test measurements pass perfectly. This concludes the proof of Lemma 6.2. □

The above Lemma 6.2 tells us that only the state $U_D |\mathcal{G}\rangle$ (the ideal state up to local unitaries on the dishonest side), or equivalently $\rho_H^{|\mathcal{G}\rangle}$, always passes the stabiliser test $\mathcal{S}_j$ in any round j. Recall that we fix N_{total} such that $\mathsf{N} \equiv N_{total} - 2^n N_{test} = 2^n N_{test}$ is the total number of remaining copies, out of which one is chosen to be the target copy. Let k be the number of copies out of the remaining N copies that would pass all the stabiliser tests. Now, using the

Serfling bound, we will find a bound on $\frac{\mathsf{k}}{\mathsf{N}}$ in the following Lemma, which is an adaptation of the method of Takeuchi et al. [175] to our scenario of verifying general graph states with any number of dishonest players.

Lemma 6.3 (adapted from [175]). *The probability that the fraction of states that would pass all stabiliser tests out of the remaining copies in Protocol 6.1 is given by*

$$\frac{\mathsf{k}}{\mathsf{N}} \geq 1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n \Big(1 - \frac{N_{pass}}{2^n N_{test}}\Big). \tag{6.42}$$

is at least $\Big[1 - n^{-\frac{2cm}{3}}\Big]^{2^n}$.

Proof. Consider a set of binary random variables $Y = \{Y_1, ..., Y_{\mathcal{T}}\}$ where $Y_t \in \{0, 1\}$. Let us set the value of $Y_t = 0$ if the stabiliser test passes on copy t, and otherwise $Y_t = 1$. Then, by Serfling's bound [176], where $\mathcal{T} = \mathcal{L} + \mathcal{R}$, for any $0 < \nu < 1$,

$$\Pr\Big[\sum_{t\in\overline{\Pi}} Y_t \leq \frac{\mathcal{L}}{\mathcal{R}} \sum_{t\in\Pi} Y_t + \mathcal{L}\nu\Big] \geq 1 - \exp\big[-\frac{2\nu^2\mathcal{L}\mathcal{R}^2}{(\mathcal{L}+\mathcal{R})(\mathcal{R}+1)}\big], \tag{6.43}$$

where Π is a set of $\mathcal{R}$ samples chosen independently and uniformly randomly from Y without replacement, and $\overline{\Pi}$ is the complementary set of Π. The expression inside the probability bracket is then an upper bound on the number of copies out of the remaining that would fail the stabiliser test, given a number of copies that pass.

Now, let us consider the stabiliser measurement $\mathcal{S}_{j\in\{1,...,2^n\}}$. We take $\mathcal{L} = N_{total} - jN_{test}$, and $\mathcal{R} = N_{test}$. Let us then set $\nu = \frac{\sqrt{c}}{2^{2n}}$, which is chosen in this way to maximise both the fidelity and probability in our resulting expression (this implies $0 < \sqrt{c} < 2^{2n}$). Let $\Pi^{(j)}$ be the set of copies on which each $\mathcal{S}_j$ was measured, and $\overline{\Pi}^{(j)}$ be the set of remaining copies after measuring $\mathcal{S}_j$. Finally, we denote the probability expression on the right-hand side of Equation (6.43) for the stabiliser test in round j as q_j. Then, after the stabiliser test for $\mathcal{S}_j$ is

performed, we have

$$\Pr\Big[\sum_{t\in\overline{\Pi}^{(j)}} Y_t \leq \frac{N_{total}-jN_{test}}{N_{test}}\sum_{t\in\Pi^{(j)}} Y_t + (N_{total}-jN_{test})\nu\Big] \geq 1-\exp\left[-\frac{2\nu^2(N_{total}-jN_{test})N_{test}^2}{(N_{total}-jN_{test}+N_{test})(N_{test}+1)}\right] \equiv q_j. \tag{6.44}$$

In other words, with probability at least q_j, the maximum number of copies that would fail the stabiliser test of $\mathcal{S}_j$ out of the remaining is given by $\frac{N_{total}-jN_{test}}{N_{test}}\sum_{t\in\Pi^{(j)}} Y_t + (N_{total}-jN_{test})\nu$. Then, the minimum number of copies that would pass the $\mathcal{S}_j$ test is given by the total number of remaining copies minus this maximum number of failed copies. Thus, after all stabiliser tests are performed, we can lower bound the number of remaining copies which would pass all of the stabiliser tests by summing over all j's corresponding to all stabilisers $\mathcal{S}_j$. Recalling that we denote the number of 'good' remaining copies by k, we then have

$$\begin{aligned}
\mathsf{k} &\geq (N_{total}-2^nN_{test}) - \sum_{j=1}^{2^n}\left(\frac{N_{total}-jN_{test}}{N_{test}}\sum_{t\in\Pi^{(j)}} Y_t + (N_{total}-jN_{test})\nu\right)\\
&= 2\times 2^nN_{test} - 2^nN_{test} - \frac{N_{total}}{N_{test}}\sum_{j=1}^{2^n}\sum_{t\in\Pi^{(j)}} Y_t + \sum_{j=1}^{2^n} j\sum_{t\in\Pi^{(j)}} Y_t - \nu 2^nN_{total} + \sum_{j=1}^{2^n} jN_{test}\nu\\
&\geq 2^nN_{test} - \nu 2^nN_{total} - \frac{N_{total}}{N_{test}}\sum_{j=1}^{2^n}\sum_{t\in\Pi^{(j)}} Y_t\\
&\geq 2^nN_{test} - \nu 2^nN_{total} - \frac{N_{total}}{N_{test}}(2^nN_{test}-N_{pass})\\
&= 2^nN_{test} - \nu 2^n\times 2\times 2^nN_{test} - \frac{2\times 2^nN_{test}}{N_{test}}(2^nN_{test}-N_{pass})\\
&= \Big(2^n - 2\times 2^{2n}\nu - 2\times 2^{2n} + 2\times 2^n\frac{N_{pass}}{N_{test}}\Big)N_{test}\\
&= \Big(2^n - 2\sqrt{c} - 2\times 2^{2n} + 2\times 2^n\frac{N_{pass}}{N_{test}}\Big)N_{test},
\end{aligned} \tag{6.45}$$

which gives the fraction of 'good' remaining copies, $\frac{\mathsf{k}}{\mathsf{N}}$, as

$$\begin{aligned}\frac{\mathsf{k}}{\mathsf{N}} &\geq \frac{\left(2^n - 2\sqrt{c} - 2\times 2^{2n} + 2\times 2^n \frac{N_{pass}}{N_{test}}\right) N_{test}}{N_{total} - 2^n N_{test}} \\ &= \frac{2^n - 2\sqrt{c} - 2\times 2^{2n} + 2\times 2^n \frac{N_{pass}}{N_{test}}}{2^n} \\ &= 1 - \frac{2\sqrt{c}}{2^n} - 2\times 2^n\left(1 - \frac{N_{pass}}{2^n N_{test}}\right). \end{aligned} \tag{6.46}$$

From Equation (6.43), we then get for q_j, the probability corresponding to the test $\mathcal{S}_j$,

$$\begin{aligned} q_j &= 1 - \exp\left[-\frac{2\nu^2(N_{total} - jN_{test})N_{test}^2}{(N_{total} - jN_{test} + N_{test})(N_{test}+1)}\right] \\ &= 1 - \exp\left[-2\nu^2 N_{test}\frac{1}{\frac{N_{total}-jN_{test}+N_{test}}{N_{total}-jN_{test}} \times \frac{N_{test}+1}{N_{test}}}\right] \\ &= 1 - \exp\left[-2\nu^2 N_{test}\frac{1}{1+\frac{N_{test}}{N_{total}-jN_{test}}}\frac{1}{1+\frac{1}{N_{test}}}\right] \\ &= 1 - \exp\left[-2\nu^2 N_{test}\frac{1}{1+\frac{1}{2\times 2^n - j}}\frac{1}{1+\frac{1}{N_{test}}}\right]. \end{aligned} \tag{6.47}$$

Now, let us compute the total probability corresponding to the full set of stabiliser tests. Since, in the most general case, the players need to measure all the stabilisers, there will be 2^n measurements in total. (We will later see that this can be reduced to n test measurements, corresponding to only the stabiliser generators, in many cases.)

Using $n \geq 1 \implies \frac{1}{1+\frac{1}{2^n}} \geq \frac{2}{3}$, and $N_{test} \geq 1 \implies \frac{1}{1+\frac{1}{N_{test}}} \geq \frac{1}{2}$, we get the total probability

corresponding to 2^n stabiliser tests to be greater than

$$\begin{aligned}
\prod_{j=1}^{2^n} q_j \geq q_{2^n}^{2^n} &= \left[1 - \exp\Big(- 2\nu^2 N_{test} \frac{1}{1+\frac{1}{2\times 2^n - 2^n}} \frac{1}{1+\frac{1}{N_{test}}}\Big)\right]^{2^n} \\
&\geq \left[1 - \exp\Big(- 2\nu^2 N_{test} \times \frac{2}{3} \times \frac{1}{2}\Big)\right]^{2^n} \\
&\geq \left[1 - \exp\Big(- \frac{2\nu^2 m 2^{4n}}{3} \ln n\Big)\right]^{2^n} \\
&= \left[1 - \exp\Big(\ln n^{-\frac{2\nu^2 m 2^{4n}}{3}}\Big)\right]^{2^n} \\
&= \left[1 - n^{-\frac{2cm}{3}}\right]^{2^n}. \qquad (6.48)
\end{aligned}$$

Thus, the event that the fraction of 'good' copies that pass all the stabiliser tests $\mathcal{S}_j$ is lower bounded by $\frac{\mathsf{k}}{\mathsf{N}} \geq 1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n\big(1 - \frac{N_{pass}}{2^n N_{test}}\big)$ occurs with probability greater than or equal to $\left[1 - n^{-\frac{2cm}{3}}\right]^{2^n}$.

□

In the final step of the protocol, one copy is chosen, out of the remaining $\mathsf{N} \equiv N_{total} - 2^n N_{test}$ copies, to be the target copy. Let us now finish the proof by proving Lemma 6.4, relating the above analysis to the averaged state of this target copy.

Lemma 6.4. *The probability that the fidelity of the averaged state of the target copy in Protocol 6.1 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq \frac{\mathsf{k}}{\mathsf{N}} \qquad (6.49)$$

is at least $\left[1 - n^{-\frac{2cm}{3}}\right]^{2^n}$.

Proof. Now, ρ_H^{avg} is the reduced state of the honest players of the averaged state, where the average is taken over all uniformly random selections of the target copy from the total number

of remaining copies N, and given by

$$\rho_H^{avg} = \frac{1}{\mathsf{N}} \sum_{i=1}^{\mathsf{N}} \rho_H^i. \tag{6.50}$$

Here, ρ_H^i denotes the reduced state of the honest players in each round (for each one of the remaining copies). We now want to find the fidelity $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg})$ between this averaged state and the ideal state (in terms of the honest reduced states). From the concavity of fidelity,

$$F(\rho, \sum_i p_i \sigma_i) \geq \sum_i p_i F(\rho, \sigma_i). \tag{6.51}$$

We can use this to get

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) = F(\rho_H^{|\mathcal{G}\rangle}, \frac{1}{\mathsf{N}} \sum_{i=1}^{\mathsf{N}} \rho_H^i) \geq \frac{1}{\mathsf{N}} \sum_{i=1}^{\mathsf{N}} F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^i). \tag{6.52}$$

Now, we know that for a number k of the remaining states, we have $\rho_H^i = \rho_H^{|\mathcal{G}\rangle}$ with probability at least $\left[1 - n^{-\frac{2cm}{3}}\right]^{2^n}$. Assuming the worst case scenario that the rest of the states, each denoted by $\rho_H^{unknown}$, have zero fidelity with the ideal state, we get

$$\begin{aligned} F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) &\geq \frac{1}{\mathsf{N}} \Big[\mathsf{k} F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{|\mathcal{G}\rangle}) + (\mathsf{N} - \mathsf{k}) F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{unknown}) \Big] \\ &\geq \frac{1}{\mathsf{N}} \Big[\mathsf{k} \times 1 + (\mathsf{N} - \mathsf{k}) \times 0 \Big] \\ &= \frac{\mathsf{k}}{\mathsf{N}}. \end{aligned} \tag{6.53}$$

□

Our final result then tells us that, with the appropriate choice of N_{total}, N_{test}, the players can ensure that with probability at least $\left[1 - n^{-\frac{2cm}{3}}\right]^{2^n}$, the fidelity of the averaged state of the target copy satisfies $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n \big(1 - \frac{N_{pass}}{2^n N_{test}}\big)$. Note that in order to ensure that the fidelity is greater than zero, the choice of the constant c must be such that $c < \frac{(2^n-1)^2}{4}$, and the choice of m must ensure that the probability is greater than zero. This concludes the proof of Theorem 6.1.

□

If the condition on N_{pass} in Step 4 of Protocol 6.1 is satisfied, we can write the lower bound on the fidelity as $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}+1}{2^n}$.

6.6 Examples

Let us now give some examples of types of graph states that are useful for specific purposes, demonstrating how to verify them (in the presence of dishonest players) in a resource-efficient way. For these cases, we will show that the players can run a simpler version of our protocol, as given in Protocol 6.2, which only requires them to measure the set of n stabiliser generators rather than the full set of 2^n stabilisers.

To prove such a statement, we start by inspecting the proof of Theorem 6.1, to understand how the information about passing the stabiliser tests is used. In Lemma 6.2, this is firstly used to identify which elements of $\{|\psi_{\bar{\mathbf{z}}}\rangle\}, \{|\phi_{\bar{\mathbf{x}}}\rangle\}$ are orthogonal; however, as we see in Equations (6.8) and (6.9), this follows from passing purely the set of stabiliser generator measurements. It then remains to show that the conditions on which $\beta_{\bar{\mathbf{x}}}$s are zero, given in Equation (6.11), may also be deduced from only passing the stabiliser generator tests. (We point out that if the set A is empty, which can be checked by examining the graph for the partition (H, D), then from passing the full set of stabiliser measurements, we cannot set any $\beta_{\bar{\mathbf{x}}}$ to be zero, and so we can trivially see that only the stabiliser generator measurements are required.) If this is true, it is possible for the players to protect themselves against dishonest action even by running Protocol 6.2.

Recall that once we know which $\beta_{\bar{\mathbf{x}}}$s must be zero, we can determine which terms have the same $\alpha_{\bar{\mathbf{z}}}, |\psi_{\bar{\mathbf{z}}}\rangle$, allowing us to group the $|\bar{\mathbf{z}}\rangle$ terms in Equation (6.4) in the same way as in the Schmidt decomposition of the ideal graph state, leading to the conclusion that $|\Psi\rangle = U_D |\mathcal{G}\rangle$. Thus, once we have derived the conditions for $\beta_{\bar{\mathbf{x}}}$ to be zero, we can simply continue with the remainder of the proof of Lemma 6.2. The analogous statements of Lemmas 6.3 and 6.4 must then take into account the fact that there are now n measurements instead of 2^n; otherwise,

Protocol 6.2 VERIFICATION OF GRAPH STATE USING ONLY STABILISER GENERATORS (adapted from [175])

Input: The players choose values of N_{test}, N_{total}.
Goal: The players verify that they share the n-qubit graph state $|\mathcal{G}\rangle$.

1: An untrusted source generates N_{total} copies of the graph state, and sends it to the players.

2: The players repeat the following for $i = 1, ..., n$:

   (a) The Verifier chooses N_{test} copies from the remaining $N_{total} - (i-1)N_{test}$ copies independently and uniformly at random.

   (b) For each copy, the Verifier instructs each player to perform the measurement corresponding to their part of the stabiliser generator K_i.

   (c) For each copy, the players send their measurement outcome to the Verifier, who calculates the total measurement outcome. The copy passes the test if the total measurement outcome is $+1$. Let $N_{pass,i}$ be the number of copies that pass the stabiliser test for K_i.

3: The Verifier uniformly randomly chooses a single copy from the remaining $\mathsf{N} \equiv N_{total} - nN_{test}$ copies that were not used for the tests in the previous steps. The chosen single copy is called the target copy. The others are discarded.

4: If $N_{pass} \equiv \sum_{i=1}^{n} N_{pass,i} \geq nN_{test} - \frac{N_{test}}{2n}$, they use the target copy for their application; otherwise the target copy is discarded.

these steps do not change.

In the following, we adapt our general proof in this way to cater to the specificities of complete graphs, cycle graphs and cluster states, with particular characteristics of the dishonest set of players. Armed with this information, we will show that our players can verify each graph state in an efficient way.

6.6.1 Complete graphs

Complete graphs, where every vertex is connected to every other vertex, are locally equivalent to GHZ states. As we have seen, such states are central to schemes for quantum anonymous transmission [2, 73], as well as secret sharing [48], metrology [49], and many other applications. A verification test for GHZ states was already proposed and analysed in [160]; however,

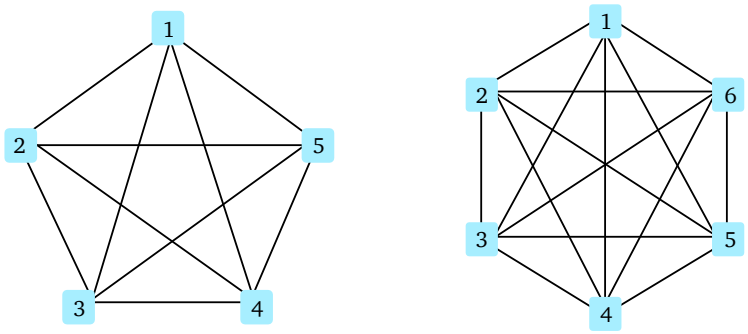


Figure 6.1: 5-qubit and 6-qubit complete graphs.

we now approach this goal using the Serfling bound method. This subsection also serves to provide a comprehensive example of how our protocol and analysis work for this particular graph state, and so we will go through all steps of the proof.

Due to the symmetry of complete graphs (Figure 6.1), we will see that we can protect against any number of dishonest players anywhere in the network by only measuring the stabiliser generators. Recall that we denote the stabiliser generator corresponding to the i^{th} qubit as K_i. Let the players now run Protocol 6.2; our result is given in the following Theorem.

Theorem 6.5. *If $|\mathcal{G}\rangle$ is a complete graph, and we set $N_{total} = 2nN_{test}$ and $N_{test} = \lceil mn^4 \ln n \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol 6.2 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{n} - 2n\Big(1 - \frac{N_{pass}}{nN_{test}}\Big) \tag{6.54}$$

is at least $1 - n^{1-\frac{cm}{2}}$, where m, c are positive constants chosen such that the probability is greater than zero and $\frac{2}{m} < c < \frac{(n-1)^2}{4}$.

Proof. As before, we prove this in stages, now for the specific case of complete graphs.

Lemma 6.6. *The only state that can pass all stabiliser generator tests perfectly in each round is $|\Psi\rangle = U_D |\mathcal{G}\rangle$, where U_D is a unitary on the dishonest part of the state.*

Proof. Complete graphs are of Schmidt rank 2, *i.e.* there are always exactly two terms in their Schmidt decomposition. The Schmidt decomposition of a complete graph state with respect

to any partition (H, D) is

$$
\begin{aligned}
|\mathcal{G}\rangle &= \frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} |\overline{\mathbf{z}}\rangle_H \otimes \prod_{a\in H} \Big(\prod_{b\in N(a)} \sigma_Z^{(b)} \Big)^{z_a} |\mathcal{G} - \mathcal{H}\rangle_D \\
&= \frac{1}{\sqrt{2^{|H|}}} \Bigg[\Big(\sum_{\Delta(\overline{\mathbf{z}})=0 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=2 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle \Big)_H \otimes \left|\mathcal{G} - \mathcal{H}_{(00\ldots00)}\right\rangle_D \\
&\quad + \Big(\sum_{\Delta(\overline{\mathbf{z}})=1 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=3 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle \Big)_H \otimes \left|\mathcal{G} - \mathcal{H}_{(11\ldots11)}\right\rangle_D \Bigg], \qquad (6.55)
\end{aligned}
$$

where $\left|\mathcal{G} - \mathcal{H}_{(00\ldots00)}\right\rangle$ is the dishonest subgraph with no σ_Zs on any vertices, and $\left|\mathcal{G} - \mathcal{H}_{(11\ldots11)}\right\rangle$ is the dishonest subgraph with σ_Zs on all vertices. Thus, the reduced state of the honest players of this ideal state is given by

$$
\begin{aligned}
\rho_H^{|\mathcal{G}\rangle} = \frac{1}{2^{|H|}} \Bigg[&\Big(\sum_{\Delta(\overline{\mathbf{z}})=0 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=2 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle \Big) \Big(\sum_{\Delta(\overline{\mathbf{z}})=0 (\mathrm{mod}\ 4)} \langle\overline{\mathbf{z}}| - \sum_{\Delta(\overline{\mathbf{z}})=2 (\mathrm{mod}\ 4)} \langle\overline{\mathbf{z}}| \Big) \\
&+ \Big(\sum_{\Delta(\overline{\mathbf{z}})=1 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=3 (\mathrm{mod}\ 4)} |\overline{\mathbf{z}}\rangle \Big) \Big(\sum_{\Delta(\overline{\mathbf{z}})=1 (\mathrm{mod}\ 4)} \langle\overline{\mathbf{z}}| - \sum_{\Delta(\overline{\mathbf{z}})=3 (\mathrm{mod}\ 4)} \langle\overline{\mathbf{z}}| \Big) \Bigg]. \qquad (6.56)
\end{aligned}
$$

From Equations (6.4) and (6.5), we know that our state can be written in general as $|\Psi\rangle = \sum_{\overline{\mathbf{z}}} \alpha_{\overline{\mathbf{z}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{z}}}\rangle_D$ and $|\Psi\rangle = \sum_{\overline{\mathbf{x}}} \beta_{\overline{\mathbf{x}}} \left|\mathcal{H}_{(\overline{\mathbf{x}})}\right\rangle_H \otimes |\phi_{\overline{\mathbf{x}}}\rangle_D$. Let us now write the test measurements, which are the stabiliser generators here. Since, for the complete graph, each vertex shares an edge with every other vertex, the stabiliser generators are given by

$$
K_i = X_i \prod_{e\in V} Z_e, \qquad (6.57)
$$

where V is the set of vertices in the graph. We will again group the test measurements into Group 1, where the honest measurement only consists of Zs, and Group 2, which contains the remaining measurements. In order to pass perfectly, the overall outcome of each measurement must be $+1$.

Let us first consider the Group 1 measurements. Any $|\overline{\mathbf{z}}\rangle$ that has an even number of 1s (parity of $\overline{\mathbf{z}}$ is 0) will give outcome $+1$ for the honest measurement $Z...Z$, and so the dishonest measurement must give outcome $+1$ in order to pass the test. Any $|\overline{\mathbf{z}}\rangle$ that has an odd number

of 1s (parity of $\overline{\mathbf{z}}$ is 1) will give outcome -1 for $Z...Z$, and so the dishonest measurement must give outcome -1. So, in order to pass perfectly, the dishonest players must be able to discriminate perfectly between the states $\left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right\rangle$ and $\left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right\rangle$, where $\Delta(\overline{\mathbf{z}})$ is the Hamming weight of $\overline{\mathbf{z}}$ (number of 1s in the string). This means that for all $\overline{\mathbf{z}}$, we have $\left\langle\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\middle|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right\rangle = 0$. (Note that this can be seen from the general proof, which tells us in this case that $\forall\overline{\mathbf{z}},\overline{\mathbf{z}}'$ such that $\bigoplus_i z_i \neq \bigoplus_i z'_i$, we have $\langle\psi_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}'}\rangle = 0$.)

Now, let us see what happens if the Group 2 measurements pass perfectly. This group will have all measurements $XZ...Z, ZXZ...Z, ..., Z...ZX$ in the honest part, and the dishonest part of each will be $(Z...Z)'$ (so the same dishonest part for each). To pass perfectly, the dishonest players must be able to always give the correct outcome; however, they only know that the measurement they must do is $(Z...Z)'$, and this does not tell them whether the honest players are measuring $XZ...Z, ZXZ...Z, ..., Z...ZX$. In order for the dishonest players to always output the correct outcome for all of these measurements (to make the overall outcome $+1$), the only terms that can appear in Equation (6.5) are the honest subgraph ($\left|\mathcal{H}_{(00...00)}\right\rangle$), and the honest subgraph with σ_Zs on all the vertices ($\left|\mathcal{H}_{(11...11)}\right\rangle$). So, passing the Group 2 measurements tells us that $\beta_{\overline{\mathbf{x}}} = 0$ for $\overline{\mathbf{x}} \notin \{00...00, 11...11\}$. (Note that this is the same conclusion that can be derived from measuring the full set of stabilisers in the general proof. Every pair of honest vertices forms a possible set A here, and we have $\beta_{\overline{\mathbf{x}}} = 0$ if $\exists A$ such that $\bigoplus_{i\in A} x_i = 1$. The only remaining strings are then those $\overline{\mathbf{x}}$ that have all elements equal to one another.)

We can then write the state in Equation (6.5) as

$$|\Psi\rangle = \beta_{00...00}\left|\mathcal{H}_{(00...00)}\right\rangle_H|\phi_{00...00}\rangle_D + \beta_{11...11}\left|\mathcal{H}_{(11...11)}\right\rangle_H|\phi_{11...11}\rangle_D\,. \tag{6.58}$$

Since measuring $(Z...Z)'$ on $|\phi_{00...00}\rangle$ must give outcome $+1$, and on $|\phi_{11...11}\rangle$ it must give outcome -1 (in order to always get the total outcome to be $+1$), the dishonest players must be able to perfectly discriminate between these two states, and so we must have

$\langle \phi_{00\ldots00} | \phi_{11\ldots11} \rangle = 0$. Then, following the steps in the general proof, we get

$$\beta_{\overline{\mathbf{x}}} |\phi_{\overline{\mathbf{x}}}\rangle = \frac{1}{\sqrt{2^{|H|}}} \Big[\sum_{\overline{\mathbf{z}}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\overset{\oplus}{i} x_i \wedge z_i} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle_D \Big], \ \forall \overline{\mathbf{x}} \text{ such that } \beta_{\overline{\mathbf{x}}} \neq 0, \tag{6.59}$$

$$0 = \frac{1}{\sqrt{2^{|H|}}} \Big[\sum_{\overline{\mathbf{z}}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\overset{\oplus}{i} x_i \wedge z_i} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle_D \Big], \ \forall \overline{\mathbf{x}} \text{ such that } \beta_{\overline{\mathbf{x}}} = 0. \tag{6.60}$$

The solution of Equation (6.60), as adapted for complete graphs from the general proof, is $\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\Delta(\overline{\mathbf{z}}) \bmod 2 = \Delta(\overline{\mathbf{z}}') \bmod 2$, we have

$$(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle = (-1)^{\overset{\oplus}{(k,l)\in E_H} z'_k \wedge z'_l} \alpha_{\overline{\mathbf{z}}'} |\psi_{\overline{\mathbf{z}}'}\rangle . \tag{6.61}$$

Recall that for complete graphs, all the honest vertices are connected to each other. Using this, we can simplify the exponent $\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l$. Each $(z_k \wedge z_l)$ will give 1 only if both z_k, z_l are 1. So, we can rephrase this using the Hamming weight $\Delta(\overline{\mathbf{z}})$, which tells us how many 1s are in the string $\overline{\mathbf{z}}$. Then, finding how many pairs $(z_k \wedge z_l)$ give 1 is equivalent to calculating ${}^{\Delta(\overline{\mathbf{z}})}C_2$.

Let us first take $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\Delta(\overline{\mathbf{z}}), \Delta(\overline{\mathbf{z}}') = 0 \pmod 2$. We see that $(-1)^{{}^{\Delta(\overline{\mathbf{z}})}C_2} = (-1)^{{}^{\Delta(\overline{\mathbf{z}}')}C_2}$ for $\Delta(\overline{\mathbf{z}}) \bmod 4 = \Delta(\overline{\mathbf{z}}') \bmod 4$. Similarly, if we take $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\Delta(\overline{\mathbf{z}}), \Delta(\overline{\mathbf{z}}') = 1 \pmod 2$, we again find that $(-1)^{{}^{\Delta(\overline{\mathbf{z}})}C_2} = (-1)^{{}^{\Delta(\overline{\mathbf{z}}')}C_2}$ for $\Delta(\overline{\mathbf{z}}) \bmod 4 = \Delta(\overline{\mathbf{z}}') \bmod 4$. Thus, we have

$$\begin{aligned} &\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}' \text{ such that } \Delta(\overline{\mathbf{z}}) = 0 (\text{mod } 4), \Delta(\overline{\mathbf{z}}') = 2 (\text{mod } 4), \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle = -\alpha_{\overline{\mathbf{z}}'} |\psi_{\overline{\mathbf{z}}'}\rangle , \\ &\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}' \text{ such that } \Delta(\overline{\mathbf{z}}) = 1 (\text{mod } 4), \Delta(\overline{\mathbf{z}}') = 3 (\text{mod } 4), \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle = -\alpha_{\overline{\mathbf{z}}'} |\psi_{\overline{\mathbf{z}}'}\rangle . \end{aligned} \tag{6.62}$$

We can now write our state as

$$
\begin{aligned}
|\Psi\rangle &= \sum_{\overline{\mathbf{z}}} \alpha_{\overline{\mathbf{z}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{z}}}\rangle_D \\
&= \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)} \Big[\sum_{\Delta(\overline{\mathbf{z}})=0(\text{mod }4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=2(\text{mod }4)} |\overline{\mathbf{z}}\rangle \Big]_H \otimes \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right\rangle_D \\
&\quad + \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)} \Big[\sum_{\Delta(\overline{\mathbf{z}})=1(\text{mod }4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=3(\text{mod }4)} |\overline{\mathbf{z}}\rangle \Big]_H \otimes \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right\rangle_D . \qquad (6.63)
\end{aligned}
$$

Then, our expressions for $\beta_{\overline{\mathbf{x}}} |\phi_{\overline{\mathbf{x}}}\rangle$ can be written using Equation (6.27) as

$$
\begin{aligned}
\beta_{00\ldots00} |\phi_{00\ldots00}\rangle &= \frac{\sqrt{2^{|H|}}}{2} \Big[\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)} \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right\rangle + \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)} \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right\rangle \Big], \\
\beta_{11\ldots11} |\phi_{11\ldots11}\rangle &= \frac{\sqrt{2^{|H|}}}{2} \Big[\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)} \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right\rangle - \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)} \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right\rangle \Big].
\end{aligned} \qquad (6.64)
$$

Now, recall that $\langle \phi_{00\ldots00} | \phi_{11\ldots11} \rangle = 0$, and $\left\langle \psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)} \middle| \psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)} \right\rangle = 0$. Using these orthogonality conditions and taking the inner product of the two expressions above, we get

$$
\left|\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right|^2 - \left|\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right|^2 = 0. \qquad (6.65)
$$

By normalisation, we have

$$
\left|\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right|^2 + \left|\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right|^2 = \frac{2}{2^{|H|}}. \qquad (6.66)
$$

Solving these, we find that $\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}, \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)} = \pm\frac{1}{\sqrt{2^{|H|}}}$. Substituting this in Equation (6.63) gives the state as

$$
\begin{aligned}
|\Psi\rangle = \pm \frac{1}{\sqrt{2^{|H|}}} \Bigg[&\Big(\sum_{\Delta(\overline{\mathbf{z}})=0(\text{mod }4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=2(\text{mod }4)} |\overline{\mathbf{z}}\rangle \Big)_H \otimes \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\text{mod }2)}\right\rangle_D \\
&\pm \Big(\sum_{\Delta(\overline{\mathbf{z}})=1(\text{mod }4)} |\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=3(\text{mod }4)} |\overline{\mathbf{z}}\rangle \Big)_H \otimes \left|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\text{mod }2)}\right\rangle_D \Bigg],
\end{aligned} \qquad (6.67)
$$

which gives

$$\begin{aligned}\rho_H^{|\Psi\rangle} = \frac{1}{2^{|H|}}\Bigg[&\Big(\sum_{\Delta(\overline{\mathbf{z}})=0(\text{mod }4)}|\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=2(\text{mod }4)}|\overline{\mathbf{z}}\rangle\Big)\Big(\sum_{\Delta(\overline{\mathbf{z}})=0(\text{mod }4)}\langle\overline{\mathbf{z}}| - \sum_{\Delta(\overline{\mathbf{z}})=2(\text{mod }4)}\langle\overline{\mathbf{z}}|\Big)\\ &+\Big(\sum_{\Delta(\overline{\mathbf{z}})=1(\text{mod }4)}|\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=3(\text{mod }4)}|\overline{\mathbf{z}}\rangle\Big)\Big(\sum_{\Delta(\overline{\mathbf{z}})=1(\text{mod }4)}\langle\overline{\mathbf{z}}| - \sum_{\Delta(\overline{\mathbf{z}})=3(\text{mod }4)}\langle\overline{\mathbf{z}}|\Big)\Bigg]\\ &= \rho_H^{|\mathcal{G}\rangle}. \end{aligned} \tag{6.68}$$

Thus, $|\Psi\rangle = U_D\,|\mathcal{G}\rangle$.

□

Now, we must modify Lemma 6.3 to account for the fact that the players only do n test measurements. This then reduces to the case shown in [175].

Lemma 6.7 (adapted from [175])**.** *The probability that the fraction of states that would pass all stabiliser generator tests out of the remaining copies in Protocol 6.2 is given by*

$$\frac{\mathsf{k}}{\mathsf{N}} \geq 1 - \frac{2\sqrt{c}}{n} - 2n\Big(1 - \frac{N_{pass}}{nN_{test}}\Big) \tag{6.69}$$

is at least $1 - n^{1-\frac{cm}{2}}$.

Proof sketch. The proof follows straightforwardly from Lemma 6.3 by substituting, as in [175], the values $N_{test} = mn^4 \ln n, N_{total} = 2nN_{test}, \nu = \frac{\sqrt{c}}{n^2}$, and noting that there are now n test measurements instead of 2^n. This then gives the desired result.

□

The remainder of the proof follows from Lemma 6.4 with this different probability. We state this in Lemma 6.8 for clarity.

Lemma 6.8. *The probability that the fidelity of the averaged state of the target copy in Protocol 6.2 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq \frac{\mathsf{k}}{\mathsf{N}} \tag{6.70}$$

is at least $1 - n^{1-\frac{cm}{2}}$.

Thus, we have $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{n} - 2n\big(1 - \frac{N_{pass}}{nN_{test}}\big)$ with probability at least $1 - n^{1-\frac{cm}{2}}$. Note that in order for the fidelity to be greater than zero, the choice of c must be such that $c < \frac{(n-1)^2}{4}$, and for the probability to be greater than zero, the choice of m must be such that $c > \frac{2}{m}$.

□

If the condition on N_{pass} in Step 4 of Protocol 6.2 is satisfied, we can write the lower bound on the fidelity as $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}+1}{n}$.

6.6.2 Pentagon graph

The 5-qubit cycle graph, in the shape of a pentagon, is known to be useful for secret sharing [52], as well as being the smallest quantum error correcting code that tolerates an arbitrary error on a single qubit [178]. Let us now consider all possible sets of dishonest players sharing such a graph (Figure 6.2), and see how we can reduce the resources required. We will show that in certain cases, by purely measuring the stabiliser generators, we can determine that if all tests pass perfectly, the state $|\Psi\rangle = U_D |\mathcal{G}\rangle$; this means that the players can run Protocol 6.2. We summarise the result in Theorem 6.9.

Theorem 6.9. *If* $|\mathcal{G}\rangle$ *is a pentagon graph with either one, three or four dishonest players anywhere in the network, or two dishonest players who are adjacent, and we set* $N_{total} = 2nN_{test}$ *and* $N_{test} = \lceil mn^4 \ln n \rceil$*, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol 6.2 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{n} - 2n\Big(1 - \frac{N_{pass}}{nN_{test}}\Big) \tag{6.71}$$

is at least $1 - n^{1-\frac{cm}{2}}$*, where* m, c *are positive constants chosen such that the probability is greater than zero and* $\frac{2}{m} < c < \frac{(n-1)^2}{4}$.

Proof. We will tackle this proof taking all possible sets of dishonest players separately. For the sets of dishonest players specified in the statement of Theorem 6.9, we will show certain steps

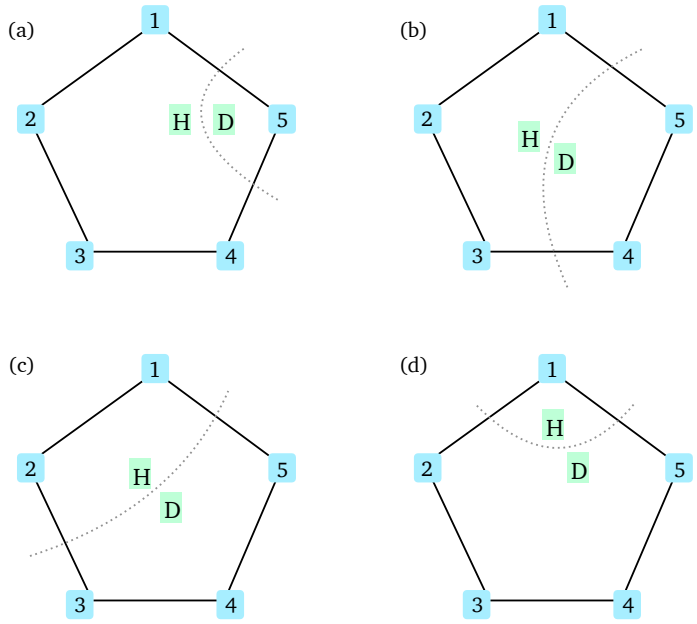


Figure 6.2: Sets of honest (H) and dishonest (D) players for the pentagon graph considered in Theorem 6.9.

in proving that by passing all stabiliser generator tests, our state must be $|\Psi\rangle = U_D\,|\mathcal{G}\rangle$. Then, as long as the honest players know that the set of dishonest players belongs to this 'allowed set', they may simply measure the stabiliser generators instead of the full stabiliser group.

One dishonest player

We will start with a scenario where one player in the network is dishonest. Without loss of generality, let us assume player 5 is dishonest, as shown in Figure 6.2(a). Then, we can write the Schmidt decomposition of the ideal state $|\mathcal{G}\rangle$ with respect to the partition (H, D) as

$$\begin{aligned}|\mathcal{G}\rangle &= \frac{1}{\sqrt{2^4}}\sum_{\bar{\mathbf{z}}}(-1)^{(z_1\wedge z_2)\oplus(z_2\wedge z_3)\oplus(z_3\wedge z_4)}\,|\bar{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(5)})^{z_1}(\sigma_Z^{(5)})^{z_4}\,|\mathcal{G}-\mathcal{H}\rangle_D \\ &= \frac{1}{4}\Big[(|0000\rangle + |1001\rangle + |0010\rangle - |1011\rangle + |0100\rangle - |1101\rangle - |0110\rangle - |1111\rangle)_H \otimes \left|\mathcal{G}-\mathcal{H}_{(0)}\right\rangle_D \\ &\quad + (|0001\rangle + |1000\rangle - |0011\rangle + |1010\rangle + |0101\rangle - |1100\rangle + |0111\rangle + |1110\rangle)_H \otimes \left|\mathcal{G}-\mathcal{H}_{(1)}\right\rangle_D\Big].\end{aligned} \tag{6.72}$$

(Note that, as expected, the dishonest part of the state, $\left|\mathcal{G} - \mathcal{H}_{(f(\overline{\mathbf{z}}))}\right\rangle$, is the same for honest parts with the same value of $\bigoplus_{i \in N(d)} z_i = z_1 \oplus z_4$.)

As usual, we start by writing our state in the honest computational and subgraph bases as in Equations (6.4) and (6.5). Now, the test measurements, or the stabiliser generators in this case, are given by $\{XZ\mathbb{1}\mathbb{1}Z',\ ZXZ\mathbb{1}\mathbb{1}',\ \mathbb{1}ZXZ\mathbb{1}',\ \mathbb{1}\mathbb{1}ZXZ',\ Z\mathbb{1}\mathbb{1}ZX'\}$. We group them into Group 1 measurements $\{Z\mathbb{1}\mathbb{1}ZX'\}$ and Group 2 measurements $\{XZ\mathbb{1}\mathbb{1}Z', ZXZ\mathbb{1}\mathbb{1}', \mathbb{1}ZXZ\mathbb{1}', \mathbb{1}\mathbb{1}ZXZ'\}$. From the Group 1 measurement passing perfectly, we see that $\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $z_1 \oplus z_4 \neq z_1' \oplus z_4'$, we must have $\langle \psi_{\overline{\mathbf{z}}} | \psi_{\overline{\mathbf{z}}'} \rangle = 0$. (Note that this matches Equation (6.8).) From the Group 2 measurements passing perfectly, we know that $\forall \overline{\mathbf{x}}, \overline{\mathbf{x}}'$, we have $\langle \phi_{\overline{\mathbf{x}}} | \phi_{\overline{\mathbf{x}}'} \rangle = 0$.

We will now see how to set certain $\beta_{\overline{\mathbf{x}}} = 0$ from just the stabiliser generators alone. The measurements $ZXZ\mathbb{1}\mathbb{1}', \mathbb{1}ZXZ\mathbb{1}'$ must give outcome $+1$ to pass the test. Since the dishonest player asked to measure $\mathbb{1}'$ will always output $+1$, the honest measurements $ZXZ\mathbb{1}, \mathbb{1}ZXZ$ must also give outcome $+1$. Further, the measurements $XZ\mathbb{1}\mathbb{1}Z', \mathbb{1}\mathbb{1}ZXZ'$ give outcome $+1$. Since the dishonest player asked to measure Z' does not know whether the honest players are measuring $XZ\mathbb{1}\mathbb{1}$ or $\mathbb{1}\mathbb{1}ZX$, yet still manages to make the test pass perfectly, this means that the honest part of the state must give the same outcome for these two measurements. With these conditions, we have $\beta_{\overline{\mathbf{x}}} = 0\ \forall \overline{\mathbf{x}} \notin \{0000, 1001\}$. (Note that we get the same result from the full stabiliser group: the possible sets A are $\{1,4\}, \{2\}, \{3\}, \{2,3\}, \{1,2,4\}, \{1,3,4\}, \{1,2,3,4\}$ and so $\beta_{\overline{\mathbf{x}}} = 0$ if $x_1 \oplus x_4 = 1, x_2 = 1$, or $x_3 = 1$.)

Following the remaining steps of the general proof, we then get

$$|\Psi\rangle = \pm \frac{1}{\sqrt{2^4}} \Big[(|0000\rangle + |1001\rangle + |0010\rangle - |1011\rangle + |0100\rangle - |1101\rangle - |0110\rangle - |1111\rangle)_H \otimes |\phi_{0000}\rangle_D \\ \pm (|0001\rangle + |1000\rangle - |0011\rangle + |1010\rangle + |0101\rangle - |1100\rangle + |0111\rangle + |1110\rangle)_H \otimes |\phi_{1001}\rangle_D \Big], \tag{6.73}$$

which gives $|\Psi\rangle = U_D |\mathcal{G}\rangle$.

Two dishonest players

Let us start by considering players 1, 2 and 3 as honest and players 4 and 5 as dishonest, pictured in Figure 6.2(b). We will vary the dishonest players later and see how this affects the results, but for now let us consider the two dishonest players to be adjacent to one another. The Schmidt decomposition of the ideal graph state for this partition is given by

$$\begin{aligned}|\mathcal{G}\rangle &= \frac{1}{\sqrt{2^3}}\sum_{\overline{\mathbf{z}}}(-1)^{(z_1\wedge z_2)\oplus(z_2\wedge z_3)}\,|\overline{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(5)})^{z_1}(\sigma_Z^{(4)})^{z_3}\,|\mathcal{G}-\mathcal{H}\rangle_D \\ &= \frac{1}{2\sqrt{2}}\Big[(|000\rangle+|010\rangle)_H \otimes \left|\mathcal{G}-\mathcal{H}_{(00)}\right\rangle_D + (|001\rangle-|011\rangle)_H \otimes \left|\mathcal{G}-\mathcal{H}_{(10)}\right\rangle_D \\ &\quad + (|100\rangle-|110\rangle)_H \otimes \left|\mathcal{G}-\mathcal{H}_{(01)}\right\rangle_D + (|101\rangle+|111\rangle)_H \otimes \left|\mathcal{G}-\mathcal{H}_{(11)}\right\rangle_D\Big]. \qquad (6.74)\end{aligned}$$

(It is easy to see that for states with the same $\bigoplus_{i\in N(d)} z_i$, $\forall d \in D$, which here refers to states with the same value of z_1 and z_3, the corresponding dishonest part $\left|\mathcal{G}-\mathcal{H}_{(f(\overline{\mathbf{z}}))}\right\rangle$ is the same.)

Let us now see whether we can make the desired statement by purely considering the stabiliser generators, $\{XZ\mathbb{1}(\mathbb{1}Z)', ZXZ(\mathbb{1}\mathbb{1})', \mathbb{1}ZX(Z\mathbb{1})', \mathbb{1}\mathbb{1}Z(XZ)', Z\mathbb{1}\mathbb{1}(ZX)'\}$. We group them, as usual, into Group 1 given by $\{\mathbb{1}\mathbb{1}Z(XZ)', Z\mathbb{1}\mathbb{1}(ZX)'\}$, and Group 2 given by $\{XZ\mathbb{1}(\mathbb{1}Z)', ZXZ(\mathbb{1}\mathbb{1})', \mathbb{1}ZX(Z\mathbb{1})'\}$. By the measurements in Group 1 passing perfectly, we see that $\forall\overline{\mathbf{z}},\overline{\mathbf{z}}'$ such that $z_1 \neq z_1'$ or $z_3 \neq z_3'$, we have $\langle\psi_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}'}\rangle = 0$, which can also be seen from Equation (6.8). By the measurements in Group 2 passing perfectly, we have $\forall\overline{\mathbf{x}},\overline{\mathbf{x}}'$, $\langle\phi_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}'}\rangle = 0$.

Now, Group 2 contains the measurement $ZXZ(\mathbb{1}\mathbb{1})'$. In order to get outcome $+1$ here, the only terms of the honest subgraph that can appear in Equation (6.5) are those that give $+1$ when measuring ZXZ. Thus, the Group 2 measurements passing perfectly tells us that $\beta_{\overline{\mathbf{x}}} = 0$ $\forall\overline{\mathbf{x}} \notin \{000, 001, 100, 101\}$. (Note that by using the full set of stabiliser measurements, we do not get more information than this, as the only possible set $A = \{2\}$ and so we know that if $x_2 = 1$, then $\beta_{\overline{\mathbf{x}}} = 0$.) Continuing with the steps of the general proof, we obtain $|\Psi\rangle = U_D\,|\mathcal{G}\rangle$.

By inspecting the stabiliser generators, we see that such an analysis holds whenever the two dishonest players are adjacent, as there will always be a measurement $(\mathbb{1}\mathbb{1})'$ that forces

the corresponding honest outcome to be $+1$. Thus, in this case, it suffices to measure the stabiliser generators. If the two dishonest players are not adjacent, however, there will not be such a measurement $(\mathbb{1}\mathbb{1})'$, and so the players must measure the full set of stabilisers.

Three dishonest players

Let us now assume players 1 and 2 are honest, while players 3, 4 and 5 are dishonest, as in Figure 6.2(c), to start with. The Schmidt decomposition is given by

$$\begin{aligned}|\mathcal{G}\rangle &= \frac{1}{\sqrt{2^2}}\sum_{\overline{\mathbf{z}}}(-1)^{z_1\wedge z_2}\,|\overline{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(5)})^{z_1}(\sigma_Z^{(3)})^{z_2}\,|\mathcal{G}-\mathcal{H}\rangle_D \\ &= \frac{1}{2}\Big[\,|00\rangle_H \otimes \big|\mathcal{G}-\mathcal{H}_{(000)}\big\rangle_D + |01\rangle_H \otimes \big|\mathcal{G}-\mathcal{H}_{(100)}\big\rangle_D \\ &\qquad + |10\rangle_H \otimes \big|\mathcal{G}-\mathcal{H}_{(001)}\big\rangle_D - |11\rangle_H \otimes \big|\mathcal{G}-\mathcal{H}_{(101)}\big\rangle_D\Big]. \end{aligned} \tag{6.75}$$

(Here, as in the general proof, we see that both z_1 and z_2 must be the same in order for the corresponding $\big|\mathcal{G}-\mathcal{H}_{(f(\overline{\mathbf{z}}))}\big\rangle$ to be the same.)

As we see here, there is no grouping of $|\overline{\mathbf{z}}\rangle$ terms, and so there will be no $\beta_{\overline{\mathbf{x}}}=0$. The Group 1 measurements are then $\{\mathbb{1}Z(XZ\mathbb{1})', \mathbb{1}\mathbb{1}(ZXZ)', Z\mathbb{1}(\mathbb{1}ZX)'\}$, and the Group 2 measurements are $\{XZ(\mathbb{1}\mathbb{1}Z)', ZX(Z\mathbb{1}\mathbb{1})'\}$. We see that if $z_1\neq z_1'$ or $z_2\neq z_2'$, the respective states are orthogonal. This implies that $\langle\psi_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}'}\rangle = 0\ \forall\overline{\mathbf{z}},\overline{\mathbf{z}}'$. We also have $\forall\overline{\mathbf{x}},\overline{\mathbf{x}}'$, $\langle\phi_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}'}\rangle = 0$. From passing the Group 2 measurements, we cannot set any $\beta_{\overline{\mathbf{x}}}=0$ (using the full stabiliser set, we see that A is the empty set). Then, we simply follow the steps of the general proof to get $|\Psi\rangle = U_D\,|\mathcal{G}\rangle$. This reasoning holds for any two players being dishonest, no matter whether they are adjacent, and so for this case, the players only need to measure the stabiliser generators.

Four dishonest players

In this scenario where only one player is honest, the analysis is again simple. Without loss of generality, let us assume only player 1 is honest, as shown in Figure 6.2(d). First, let us write

the Schmidt decomposition for this partition (H, D) as

$$
\begin{aligned}
|\mathcal{G}\rangle &= \frac{1}{\sqrt{2^1}} \sum_{\bar{\mathbf{z}}} |\bar{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(2)} \sigma_Z^{(5)})^{z_1} |\mathcal{G} - \mathcal{H}\rangle_D \\
&= \frac{1}{\sqrt{2}} \Big[|0\rangle_H \otimes \left|\mathcal{G} - \mathcal{H}_{(0000)}\right\rangle_D + |1\rangle_H \otimes \left|\mathcal{G} - \mathcal{H}_{(1001)}\right\rangle_D \Big]. \qquad (6.76)
\end{aligned}
$$

(Note that, as in the general proof, if $\bigoplus_{i \in N(d)} z_i = z_1$ is the same, the corresponding $\left|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\right\rangle$ is the same.)

Now, the set of measurements is given by the stabiliser generators again, which we will separate into Group 1 containing $\{Z(XZ\mathbb{1}\mathbb{1})', \mathbb{1}(ZXZ\mathbb{1})', \mathbb{1}(\mathbb{1}ZXZ)', Z(\mathbb{1}\mathbb{1}ZX)'\}$, and Group 2 containing $\{X(Z\mathbb{1}\mathbb{1}Z)'\}$. Group 1 passing perfectly gives $\langle\psi_0|\psi_1\rangle = 0$, since $|0\rangle_H, |1\rangle_H$ will give different outcomes for Z, and so the dishonest players must be able to perfectly discriminate between their corresponding parts of the state in order to pass perfectly (we reach the same conclusion using Equation (6.8)). Similarly, Group 2 passing perfectly gives $\langle\phi_0|\phi_1\rangle = 0$, since $|+\rangle_H, |-\rangle_H$ give different outcomes for X. When there is only one honest player, we cannot set any $\beta_{\bar{\mathbf{x}}} = 0$ from passing perfectly (the set A is the empty set, so this gives the same result as measuring the full stabiliser set). We then proceed with the proof to get $|\Psi\rangle = U_D |\mathcal{G}\rangle$.

Thus, for any number of adjacent dishonest players, passing all the tests of Protocol 6.2 allows us to conclude that the state in each round is $|\Psi\rangle = U_D |\mathcal{G}\rangle$. It then remains to invoke Lemmas 6.7 and 6.8, since there are n test measurements, to complete the proof.

□

6.6.3 Cycle graphs

With the example of the pentagon graph in the previous subsection, we notice some features which can be extended to general n-qubit cycle (or ring) graphs (Figure 6.3), used in various applications such as quantum error correction [168]. In Theorem 6.10, we give some cases for the cycle graph where it suffices to measure only stabiliser generators as in Protocol 6.2. We will outline the reasoning behind this, although it can be seen explicitly in the pentagon

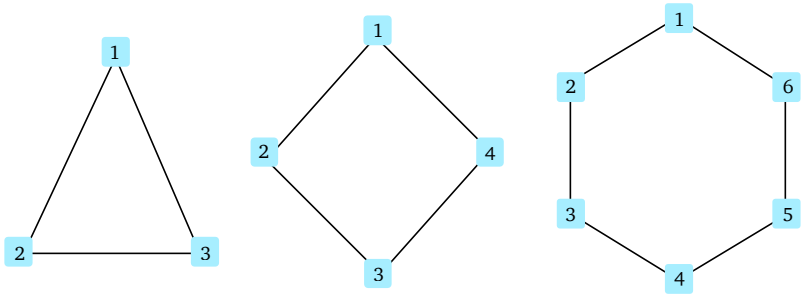


Figure 6.3: 3-qubit, 4-qubit and 6-qubit cycle (ring) graphs.

graph example.

Theorem 6.10. *If $|\mathcal{G}\rangle$ is a cycle graph with either one, $n-2$ or $n-1$ dishonest players anywhere in the network, or any other number of dishonest players who are adjacent, and we set $N_{total} = 2nN_{test}$ and $N_{test} = \lceil mn^4 \ln n \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol 6.2 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{n} - 2n\Big(1 - \frac{N_{pass}}{nN_{test}}\Big) \tag{6.77}$$

is at least $1 - n^{1-\frac{cm}{2}}$, where m, c are positive constants chosen such that the probability is greater than zero and $\frac{2}{m} < c < \frac{(n-1)^2}{4}$.

Proof sketch. Whenever there are $n-1$ or $n-2$ dishonest players in the network, the Schmidt decomposition is given by

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\overset{\oplus}{k,l\in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \otimes \left|\mathcal{G} - \mathcal{H}_{(\bar{\mathbf{z}})}\right\rangle_D , \tag{6.78}$$

where each $|\bar{\mathbf{z}}\rangle$ corresponds to a different dishonest part $\left|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\right\rangle$. This means that there is no grouping of $|\bar{\mathbf{z}}\rangle$ terms, and so the Group 2 measurements do not tell us that any $\beta_{\bar{\mathbf{x}}} = 0$, as we saw in the previous example. Thus, in this case the players can simply measure the stabiliser generators (the full stabiliser group would give no additional information, as the set A is empty).

Let us now consider the case of one dishonest player. The dishonest measurements of $\mathbb{1}'$, corresponding to the generators of qubits $i \notin N(d)$, ensure that if $x_{i\notin N(d)} = 1$, then $\beta_{\bar{\mathbf{x}}} = 0$.

Further, the two dishonest measurements of Z', corresponding to the generators of the two qubits $i \in N(d)$, ensure that if $x_{i\in N(d)}$ are not the same (in order to give the same honest outcome), then $\beta_{\overline{\mathbf{x}}} = 0$. This means that the only terms in the honest subgraph are $\left|\mathcal{H}_{(00\ldots00)}\right\rangle$ and $\left|\mathcal{H}_{(10\ldots01)}\right\rangle$, which allows us to arrive at our result from just the stabiliser generators. (Note that using the full stabiliser group, Equation (6.11) would imply that if $\bigoplus_{i\in N(d)} x_i = 1$, or $x_{i\notin N(d)} = 1$, then $\beta_{\overline{\mathbf{x}}} = 0$, which gives the same result.)

Finally, for any other number of honest/dishonest players, if the dishonest players are adjacent then there will be measurements $(\mathbb{1}\ldots\mathbb{1})'$ in the set of stabiliser generators, corresponding to the generators of honest vertices that are not connected to any of the dishonest vertices (for qubits $i \notin N(D)$). Since the dishonest part must give outcome $+1$ for this measurement, the honest part must also give outcome $+1$ in order to pass perfectly. This means that any terms where $x_{i\notin N(D)} = 1$ must have $\beta_{\overline{\mathbf{x}}} = 0$. (Note that using the full stabiliser group, the possible sets A are all combinations of honest vertices that are not connected to any dishonest vertex, which gives the same result.) Thus, we can conclude that $|\Psi\rangle = U_D\,|\mathcal{G}\rangle$ from only measuring the stabiliser generators.

As before, with n test measurements, the statements of Lemmas 6.7 and 6.8 hold, thus completing the proof.

□

In fact, there are additional examples that do not fall into these categories, but where it suffices to measure the stabiliser generators only. For example, consider the 6-qubit cycle graph with $D = \{2, 3, 6\}$, the 7-qubit cycle graph with $D = \{2, 3, 4, 7\}$, or the 8-qubit cycle graph with $D = \{2, 3, 6, 7\}$. There are no $\beta_{\overline{\mathbf{x}}} = 0$ in the Schmidt decomposition for these cases, which means that by passing the measurements in Protocol 6.2 perfectly, we can determine that $|\Psi\rangle = U_D\,|\mathcal{G}\rangle$.

6.6.4 Cluster states

Cluster states correspond to lattices of dimension $\mathcal{D}$, and have been shown to be a central resource in MBQC [50, 51]. For verification of such states in an untrusted network, we will

now give some examples of scenarios where we can reduce the number of test measurements to purely the stabiliser generators (thus allowing the players to run the simpler verification scheme of Protocol 6.2). Again, these are not the only possible sets of dishonest players in a cluster state network that allow such a simplification; there may be many more examples.

Linear, or one-dimensional, cluster states (also known as path graphs) correspond to qubits connected in a line (Figure 6.4). In Theorem 6.11, we give some cases where it is sufficient to measure the stabiliser generators.

Theorem 6.11. *If $|\mathcal{G}\rangle$ is a $1\mathcal{D}$ cluster state with either one or $n-1$ dishonest players anywhere in the network, or any other number of adjacent honest or dishonest players, and we set $N_{total} = 2nN_{test}$ and $N_{test} = \lceil mn^4 \ln n \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol 6.2 satisfies*

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{n} - 2n\Big(1 - \frac{N_{pass}}{nN_{test}}\Big) \tag{6.79}$$

is at least $1 - n^{1-\frac{cm}{2}}$, where m, c are positive constants chosen such that the probability is greater than zero and $\frac{2}{m} < c < \frac{(n-1)^2}{4}$.

Proof. The stabiliser generators of an n-qubit $1\mathcal{D}$ cluster state are given by $\{XZ\mathbb{1}...\mathbb{1}$, $ZXZ\mathbb{1}...\mathbb{1}$, ..., $\mathbb{1}...\mathbb{1}ZX\}$. As we noted for cycle graphs, if there are $n-1$ dishonest players in the network, it suffices to measure only stabiliser generators, as passing the Group 2 measurements perfectly does not tell us to set any $\beta_{\overline{\mathbf{x}}} = 0$.

If there is one dishonest player at either end of the line, we see that to get overall outcome $+1$, the honest part of the stabiliser generator measurements corresponding to every honest vertex $i \notin N(d)$ must give outcome $+1$. This means that if $x_{i \notin N(d)} = 1$, we must have $\beta_{\overline{\mathbf{x}}} = 0$. (Note that from the full stabiliser group, we see that all possible sets A contain only honest vertices $i \notin N(d)$, and so we come to the same conclusion.) If the dishonest player is not at the end of the line, but at a vertex connected to two other (honest) vertices, we again must have that if $x_{i \notin N(d)} = 1$ then $\beta_{\overline{\mathbf{x}}} = 0$, and further, the honest part of the stabiliser generators for $i \in N(d)$ must give the same outcome (as they have the same dishonest part). This means

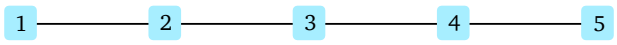


Figure 6.4: 5-qubit path graph, or $1\mathcal{D}$ cluster state.

that if x_i does not have the same value for both $i \in N(d)$, then $\beta_{\overline{\mathbf{x}}} = 0$. (Note that this gives the same result as using the full stabiliser group, as the set A may consist of any combination of honest vertices $i \notin N(d)$ as well as both honest vertices $i \in N(d)$.)

Further, for any other number of dishonest players, if it is known that the honest players are all adjacent to each other, or the dishonest players are all adjacent to each other, then the players could measure only the stabiliser generators. In such a setting, there will be $(\mathbb{1}...\mathbb{1})'$ measurements in the stabiliser generators (corresponding to $i \notin N(D)$) that allow us to set $\beta_{\overline{\mathbf{x}}} = 0$ if $x_{i \notin N(D)} = 1$. (Note that from the full stabiliser group, all possible sets A will consist of $i \notin N(D)$, and so this gives the same result.)

In these cases where only n test measurements are required, using Lemmas 6.7 and 6.8 we can prove our statement.

□

Additional examples of path graphs where it is sufficient to measure only the stabiliser generators include, for the 5-qubit path graph, the sets $D = \{1, 2, 5\}$, or $D = \{1, 3, 5\}$, where there are no $\beta_{\overline{\mathbf{x}}} = 0$ in the Schmidt decomposition, and so measuring the stabiliser generators suffices.

Two-dimensional cluster states have the underlying structure of a $t \times t$ square grid, where the total number of qubits in the lattice is $n = t \times t$. In Theorem 6.12, we give certain sets of dishonest players for which it is possible to verify such states with the resource-efficient Protocol 6.2, which is a useful result for verification in the MBQC paradigm.

Theorem 6.12. *If $|\mathcal{G}\rangle$ is a $2\mathcal{D}$ cluster state with either one or $n-1$ dishonest players anywhere in the network, or any other set of adjacent dishonest players that forms a square or rectangle anywhere in the network, and we set $N_{total} = 2nN_{test}$ and $N_{test} = \lceil mn^4 \ln n \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested*

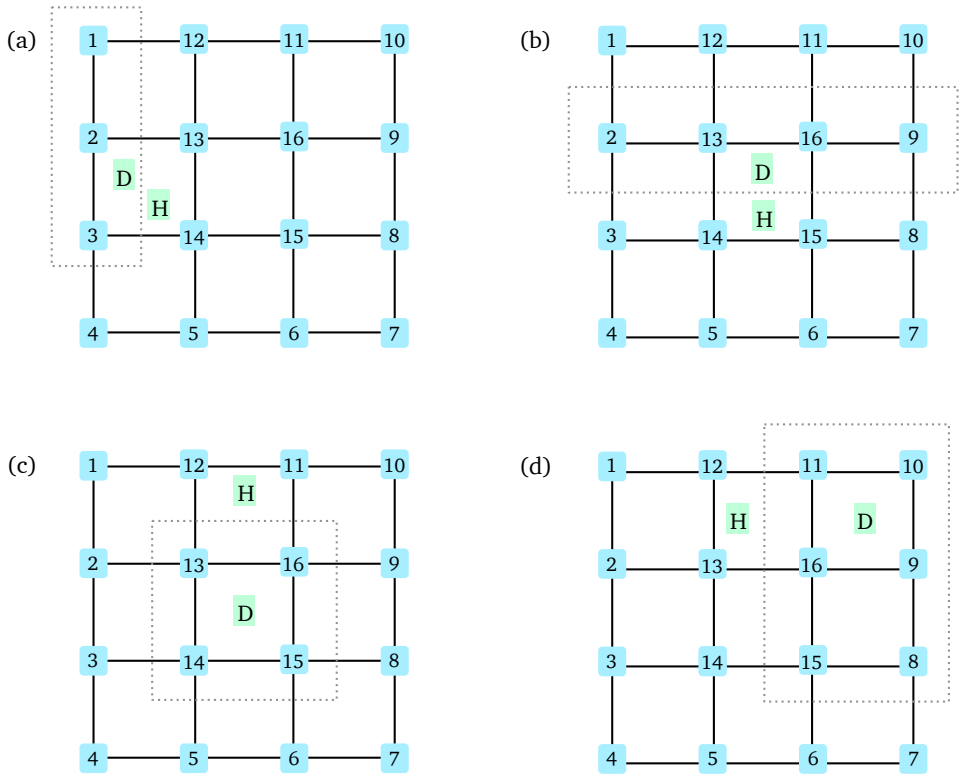


Figure 6.5: Sets of honest (H) and dishonest (D) players for the 4×4 cluster state considered in Theorem 6.12.

copies and target copy) in Protocol 6.2 satisfies

$$F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{pass}}{nN_{test}}\right) \tag{6.80}$$

is at least $1 - n^{1-\frac{cm}{2}}$*, where* m, c *are positive constants chosen such that the probability is greater than zero and* $\frac{2}{m} < c < \frac{(n-1)^2}{4}$.

Proof. Similarly to what we have seen in previous examples, if there is one honest player, or one dishonest player, it is enough to measure only the stabiliser generators. We will now show that, for any number of dishonest players in a $2\mathcal{D}$ cluster state, if they form a square or rectangle in the lattice, it is possible to do the verification using only the generators.

Consider the example of a 4×4 (or 16-qubit) cluster state, with example sets of honest and dishonest players as shown in Figure 6.5. Let us start with the players 1, 2 and 3 being dishonest, while the remaining are honest, as in Figure 6.5(a). If we write down the set of

stabiliser generators, we find that the generators corresponding to qubits 5, 6, 7, 8, 9, 10, 11, 15 and 16 will have dishonest part $(\mathbb{1}\mathbb{1}\mathbb{1})'$, as they are not connected to the dishonest set. This means that the corresponding honest measurements on the state $|\Psi\rangle$ must give outcome $+1$. Recall that the generator of qubit i contains the measurement X_i, which tells us that if $x_i = 1$ for $i \in \{5, 6, 7, 8, 9, 10, 11, 15, 16\}$ (or equivalently, if $x_{i \notin N(D)} = 1$), then $\beta_{\overline{\mathbf{x}}} = 0$. Further, the dishonest part of the measurement will be the same for generators of qubits 4 and 14 (since they are both connected to dishonest qubit 3). This means that in order to pass these test measurements, the corresponding honest part of the measurements must give the same outcome, and so we must have that if $x_4 \neq x_{14}$, then $\beta_{\overline{\mathbf{x}}} = 0$. (Note that from the full stabiliser group, we have all possible sets A containing $i \notin N(D)$ as well as both $i = 4, 14$ which are evenly connected to all $d \in D$. This gives the same conclusions as previously, and so it is clear that only measuring the generators is necessary.)

Now, consider the example shown in Figure 6.5(b), where players 2, 13, 16 and 9 are dishonest, while the remaining are honest. Again, writing down the set of stabiliser generators, we find that the generators corresponding to qubits 4, 5, 6 and 7 have dishonest part $(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1})'$, which tells us that if $x_i = 1$ for $i \in \{4, 5, 6, 7\}$, then $\beta_{\overline{\mathbf{x}}} = 0$. Further, the generators of qubits 1 and 3, 12 and 14, 11 and 15, and 8 and 10 have the same dishonest part, and so we must have that if either $x_1 \neq x_3, x_{12} \neq x_{14}, x_{11} \neq x_{15}$, or $x_8 \neq x_{10}$, then $\beta_{\overline{\mathbf{x}}} = 0$. (Note that from the full stabiliser group, the set A consists of all combinations of $i \notin N(D)$, as well as combinations of the pairs of vertices $(1, 3), (12, 14), (11, 15), (8, 10)$ which are evenly connected to all $d \in D$, leading to the same result.)

Let us now move on to the example shown in Figure 6.5(c), where players 13, 14, 15 and 16 are dishonest, and the remaining are honest. The generators of qubits 1, 4, 7 and 10 have dishonest part $(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1})'$, which means that if $x_i = 1$ for $i \in \{1, 4, 7, 10\}$, then $\beta_{\overline{\mathbf{x}}} = 0$. Further, the generators of qubits 1 and 12, 9 and 11, 3 and 5, and 6 and 8 have the same dishonest part, which means that additionally, if either $x_1 \neq x_{12}, x_9 \neq x_{11}, x_3 \neq x_5$, or $x_6 \neq x_8$, then $\beta_{\overline{\mathbf{x}}} = 0$. (Note that from the full stabiliser group, we come to the same conclusions, as the set A contains all combinations of $i \notin N(D)$ as well as the pairs $(1, 12), (9, 11), (3, 5), (6, 8)$.)

As another example, consider the dishonest set to comprise of players 8, 9, 10, 11, 15 and 16, as shown in Figure 6.5(d). From the generators whose dishonest part is $(\mathbb{1}...\mathbb{1})'$, we must have that if $x_i = 1$ for $i \in \{1, 2, 3, 4, 5\}$, then $\beta_{\overline{\mathbf{x}}} = 0$. Further, from the generators whose dishonest part is the same, we have that if $x_6 \neq x_{14}$, then $\beta_{\overline{\mathbf{x}}} = 0$. (Note that from the full stabiliser group, we see that the set A can contain all combinations of $i \notin N(D)$ along with the pair $(6, 14)$.)

Such an analysis easily extends to all cases where the dishonest players lie in a square or rectangular section of the lattice; for example, where $D = \{8, 9, 10, 11, 12, 13, 14, 15, 16\}$, or $D = \{5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

We finish the proof by invoking Lemmas 6.7 and 6.8.

□

Note that there are many other sets of dishonest players for the $2\mathcal{D}$ cluster state for which passing only the stabiliser generator measurements perfectly implies $|\Psi\rangle = U_D |\mathcal{G}\rangle$; as before, here we are only giving some examples of cases where such a simplification is allowed.

6.7 Discussion

In this final Chapter, we have shown how to verify any graph state shared between a network of players who may or may not be trusted. As our starting point, we have employed a protocol by Takeuchi et al. [175] that can verify any graph state, and further extended it to allow for dishonest players. This is a step towards practical, implementable graph state verification in untrusted networks, which in turn is important for many applications such as MBQC, quantum metrology, quantum secret sharing, and secure multiparty quantum computation.

Previous work on verification of graph states came under two main approaches: a client wishing to verify the graph state generated by an untrusted server, and self-testing of graph states. Our work, on the other hand, tackles verification in a distributed setting, and thus corresponds to the general case of the work of Pappa et al. [160]. Our results give a bound on the fidelity, up to unitaries on the dishonest part, of the graph state generated by an untrusted

source and shared between a network of players who may be dishonest. Such a statement is powerful, as in addition to detecting the creation of entanglement, it gives us concrete information on the quality of the state from the outcome of the verification test. Further, as the operations carried out by the players are local, they reveal nothing about their inputs, which is essential for secure multiparty quantum computation.

There are quite a few different avenues to explore related to this work. It is clear that our general result is not an achievable bound in terms of practicality, as it requires a very high number of copies. However, this is due in part to the power of the adversarial model we consider, and can be relaxed by placing constraints on what the dishonest players are allowed to do (for example, not allowing them to work together). In our work, we permit any player to be dishonest, allow them to work together, and apply any operation on their part of the state. Further, our general proof works for any arbitrary graph state. If we know more about the structure of the graph or the dishonest players (for example, which players or how many of them may be dishonest, or whether they are in the neighbourhood of each other), we may not need to measure all the stabilisers, which leads to a much lower required number of copies in our final result.

In fact, as we have shown, there are many examples where we do not need the full stabiliser set, the most obvious being if the graph is complete. In this case, it is enough to measure the stabiliser generators, giving us the same bound (up to unitaries on the dishonest part) as [175] where all players are honest. Comparing this result with the GHZ verification protocol in [160] (and assuming an honest Verifier for a fair comparison), we see that guaranteeing a certain fidelity with a certain probability would require $O(n^5 \ln n)$ copies using our protocol, and $O(n^{\frac{cm}{2}})$ using their protocol (see Appendix 6.A.1 for more details). With appropriate choices of N_{total}, N_{test}, c and m in our protocol, we can then achieve the same result with much fewer copies. Thus, by supplying these additional parameters, the Serfling bound approach allows us to derive more resource-efficient results.

We have also considered specific examples of graph states that are suited for some purpose, for example, the pentagon graph for secret sharing, or the cluster state for MBQC. Knowing

some information about the structure of the graph or the set of dishonest players, we were able to derive much more practical results. Such an analysis can of course be extended to other subsets of graph states.

Finally, we note that we have assumed the player acting as the Verifier is honest; modifying the protocol to incorporate a possibly dishonest Verifier is an important next step. To do this, we may follow the method of Pappa et al. [160], where a random player is chosen to be the Verifier. This would require the use of a trusted common random source (CRS) that provides the players with shared randomness. This randomness would then be used to pick which player acts as the Verifier, and further to replace any random choice by the Verifier (*i.e.* which copies are used for each stabiliser test, and which copy out of the remaining untested N copies is used for the application). In this way, the honest players are protected against a dishonest Verifier who may attempt to cheat by biasing the 'random' choices. Of course, if the randomly chosen Verifier is dishonest, which happens with probability $\frac{|D|}{n}$, the protocol would fail, as a dishonest Verifier can force any state to pass the tests and thus be accepted. There are perhaps other approaches, aside from the Serfling bound, that may suit this scenario; this would be interesting future work.

6.A Appendix

6.A.1 Comparison with GHZ verification protocol of [160]

In the work of Pappa et al. [160], they give a protocol for verification of a GHZ state shared between a network of possibly untrusted players. For a fair comparison, let us first derive the soundness bound of their verification protocol in the case that the Verifier is always an honest player. Let C_ϵ be the event that the protocol has not aborted and that, no matter what operation the dishonest players apply on their part of the state, the fidelity of the used copy of the state is at most $1-\epsilon^2$. Then, after 2^S rounds (*i.e.* the number of copies the source is asked to produce), we have

$$\Pr[C_\epsilon] \leq 2^{-S} \int_0^\infty \left(1-\frac{\epsilon^2}{4}\right)^l dl \leq 2^{-S}\frac{4}{\epsilon^2}. \tag{6.81}$$

We can reformulate this as, after 2^S rounds, with probability at least $1-2^{-S}\frac{4}{\epsilon^2}$, the protocol does not abort and the fidelity of the copy of the state to be used, $|\Psi\rangle$, is given by $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{|\Psi\rangle}) \geq 1-\epsilon^2$.

Recall that our statement in the case of GHZ states is that after $N_{total} = 2mn^5 \ln n$ rounds, with probability at least $1-n^{1-\frac{cm}{2}}$, the fidelity of the averaged state of the target copy is given by $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geq 1-\frac{2\sqrt{c}+1}{n}$, where $\frac{2}{m} < c < \frac{(n-1)^2}{4}$.

Let us now do a comparison, as in [175], of the number of rounds required to achieve the same fidelity and probability using both protocols. We have

$$1-\epsilon^2 = 1-\frac{2\sqrt{c}+1}{n}; \quad 1-2^{-S}\frac{4}{\epsilon^2} = 1-n^{1-\frac{cm}{2}}. \tag{6.82}$$

Solving, we get the number of rounds required in their protocol to achieve the same fidelity and probability as ours to be

$$2^S = \frac{4}{2\sqrt{c}+1} n^{\frac{cm}{2}}. \tag{6.83}$$

This means the number of rounds of their protocol scales as $O(n^{\frac{cm}{2}})$ while ours scales as

$O(n^5 \ln n)$, to obtain the same fidelity and probability. We see that for a choice of c, m such that $cm \geq 10$, our protocol performs better than theirs. Further, as n increases, the performance of our protocol improves drastically over their protocol. For example, if $n = 20$, a fidelity of at least 0.73 can be ensured with a probability greater than $1 - 3.5 \times 10^{-9}$ for a choice of $c = 5, m = 3$ in our protocol, which requires a total number of rounds (or copies) of $N_{total} = 5.75 \times 10^7$. Using their protocol, guaranteeing such a fidelity and probability would require 4.19×10^9 copies.

Chapter 7

Conclusions

The development of quantum networks allows one to exploit the power of quantum theory to facilitate secure communication, computation and many other tasks between players in different locations. While progress has been abundant and fast-paced on both the theoretical and experimental sides, it is of utmost importance to unify these approaches. The overarching aim of this thesis is to bridge this gap for work on verification, and to further apply this to build simple yet vital protocols for quantum networks. We do this in a myriad of different ways: by considering realistic noise as in Chapter 3, by extending and optimising self-testing tools as in Chapter 4, by introducing the notion of imperfections in quantum anonymous transmission as in Chapter 5, or by modifying a resource-efficient verification scheme to incorporate adversarial players as in Chapter 6.

Furthermore, the analysis of such networks from a cryptographic perspective requires one to think carefully about who or what to trust. This notion of trust (and in particular, guaranteeing trust in a practical way) is central to ensuring secure communication across quantum networks. We delve into a range of scenarios: where the source of entanglement is untrusted (Chapters 3 - 6), where measurement devices may be corrupted (Chapter 4), where one wishes to communicate anonymously (Chapter 5), or when any player in your network may be out to get you (Chapters 5, 6). In each case, we have constructed protocols that incorporate verification to accomplish their tasks, and illustrated their security in a cryptographic

context. Let us now discuss in a little more detail the main takeaways from our work, and how to build upon these in the future.

In Chapter 3, we outlined a simple scenario in which verification of the Bell state allows two players to carry out an authenticated teleportation, by first testing their 'quantum channel' through which a message is sent. We discussed how noise in the measurement devices affects the security analysis, and how a demonstration with noisy states is likely to work. We ended with a brief description of how such an analysis can be extended to more complicated stabiliser states, such as graph states, in a straightforward way. Our approach can be thought of as achieving the same goal as previous work on authentication of quantum messages [38], however with a significantly simpler implementation that comes at a tradeoff with security. Future work in this direction may consider alternative noise models, perhaps more specific to an experimental setup. One may also apply these results in the certification of other protocols, for example, those that include teleportation as a subroutine, or simply other applications of such states.

In Chapter 4, we took the problem of authenticated teleportation to the more paranoid one-sided device-independent setting. Our aims here were manifold. First, we used a state-of-the-art self-testing tool called the SWAP method [122] to compute new, tighter bounds for the Bell state and the Pauli σ_X, σ_Z measurements, with respect to an observed violation of the steering inequality. We then went a step further than the usual self-testing approach, by translating our results to a realistic (and moreover, fully adversarial) setting, and relating the self-testing statements about a measured state to an untested copy of the state that will be used for some application. We finally applied this to propose a scheme for authenticated teleportation with one-sided trust. To tailor our protocol to possible experimental implementations, we introduced parameters that provide a tradeoff between the number of copies and inequality violation required, and showed that we can achieve values in line with cutting-edge experiments. To further build upon this work, one could investigate the use of other steering inequalities that may simplify the experimental demonstration, or look into a fully device-independent teleportation scheme. In any case, our methods may be useful in bring-

ing the theoretical tool of self-testing closer to verification protocols, for a variety of states, measurements, and applications.

In Chapter 5, we looked at a crucial feature of communication networks: anonymity, or the ability to hide one's identity. We combined existing protocols in a novel way, using as building blocks protocols for anonymous quantum communication with GHZ states, experimentally-demonstrated verification of GHZ states, and several classical anonymous protocols both new and from the literature. This resulted in an ϵ-anonymous protocol for communicating quantum messages, where the parameter ϵ encompasses imperfections in the network. We demonstrated the resistance of our new scheme to an all-powerful adversary who may corrupt both the entanglement source and any number of players in the network. In terms of future work, one could consider a specific noise model (again, this could be tailored to particular experimental noise). An interesting question, to further improve the practicality of anonymous quantum communication, would be whether there are other states suitable for this task (and perhaps those which are less susceptible to particle loss). One may also think of numerous applications: a verified, anonymous quantum channel could be used to build anonymous schemes for QKD or voting, among others.

In Chapter 6, we considered a network of players sharing an arbitrary graph state that they wish to verify, while some among them may be dishonest. We started by employing an existing resource-efficient protocol [175] and modifying it for an untrusted network of players. We then derived a bound on the expected fidelity of the shared state, guaranteed despite any number of dishonest players. Although this general result is not practical, we showed how our analysis and the resources required can be greatly simplified and tailored to scenarios where some information is known about, for example, the structure of the graph state, or the number or location of the dishonest players in the network. In particular, we gave specific examples of graph states that are used for purposes as varied as quantum secret sharing, metrology and computation, and demonstrated the power of our verification protocol in each case. One can view this as an extension of the GHZ verification protocol in [160] to the more general case of any graph state. There are, of course, many open questions related

to this work, such as further exploring the case of a dishonest Verifier, or applying these results to simplify the resource requirements for secure multiparty quantum computation.

We end by commenting on the potential applications, implementations and scope of our work. Our protocols in Chapters 3, 4 and 5 are set to be experimentally demonstrated in a photonics lab, through a collaboration with the group of Eleni Diamanti at LIP6, Sorbonne Université, Paris. Before our work, implementations of the types of protocols we consider were far from easy, with demanding requirements on fidelities and very small margins of allowed errors. For example, previous theoretical work on anonymous communication of quantum messages required perfect GHZ states or carrying out complicated quantum circuits, and the application of self-testing results to propose an actually feasible device-independent protocol has not been done in the past. Our work in this thesis thus contributes towards drawing theoretical and experimental quantum cryptography closer together.

Each of our protocols fits in well with the aims of the Quantum Internet Alliance, a collaboration focused on constructing and developing applications for an extensive near-future quantum network. As part of this, our anonymous quantum communication scheme (Protocol 5.7) is featured in the Quantum Protocol Zoo [40], a repository of fundamental protocols that can be performed on quantum networks, and the other protocols we have developed will shortly be added to this. In this era of tremendous technological progress, we expect to soon see fully operational quantum networks that will revolutionise secure computing and communication.

Bibliography

[1] A. Unnikrishnan and D. Markham, "Authenticated teleportation with one-sided trust," *Physical Review A*, vol. 100, no. 3, 2019.

[2] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Physical Review Letters*, vol. 122, no. 24, 2019.

[3] M. Planck, "Zur theorie des gesetzes der energieverteilung im normal spectrum," *Verhandlungen der Deutschen Physikalischen Gesellschaft*, vol. 2, pp. 237–245, 1900.

[4] A. Einstein, "Zum gegenwärtigen Stand der Strahlungsproblems," *Physikalische Zeitschrift*, vol. 10, pp. 185–193, 1909.

[5] L. de Broglie, "Ondes et quanta," *Académie des Sciences Paris*, vol. 177, pp. 507–510, 1923.

[6] E. Schrödinger, "Quantisierung als Eigenwertproblem," *Annalen der Physik*, vol. 79, pp. 361–376, 1926.

[7] W. Heisenberg, "Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen," *Zeitschrift für Physik*, vol. 33, no. 1, pp. 879–893, 1925.

[8] P. A. Dirac, "The quantum theory of the electron," *Proceedings of the Royal Society of London*, vol. 117, 1928.

[9] R. Feynman, "Simulating physics with quantum computers," *International Journal of Theoretical Physics*, vol. 21, no. 6/7, pp. 467–488, 1982.

[10] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of The Royal Society of London, Series A: Mathematical and Physical Sciences*, vol. 400, pp. 97–117, 1985.

[11] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, pp. 46–52, 2001.

[12] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Physical Review Letters*, vol. 74, no. 20, 1994.

[13] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, "Stable solid-state source of single photons," *Physical Review Letters*, vol. 85, no. 2, 2000.

[14] D. Loss and D. P. DiVincenzo, "Quantum computation with quantum dots," *Physical Review A*, vol. 57, no. 1, pp. 120–126, 1998.

[15] Y. Makhlin, G. Schön, and A. Shnirman, "Josephson-junction qubits with controlled couplings," *Nature*, vol. 398, pp. 305–307, 1999.

[16] T. Farrow, R. A. Taylor, and V. Vedral, "Towards witnessing quantum effects in complex molecules," *Faraday Discussions*, vol. 184, pp. 183–191, 2015.

[17] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, 1994.

[18] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, pp. 212–219, 1996.

[19] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," *Proceedings of the 43rd Annual ACM Symposium on the Theory of Computing*, pp. 333–342, 2011.

[20] D. Ristè, M. P. Da Silva, C. A. Ryan, *et al.*, "Demonstration of quantum advantage in machine learning," *npj Quantum Information*, vol. 3, 2017.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[22] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proceedings of the International Conference on Computers, Systems and Signal Processing*, vol. 175, pp. 175–179, 1984.

[23] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, 2008.

[24] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: a vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[25] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, 1998.

[26] P. Kómár, E. M. Kessler, M. Bishof, *et al.*, "A quantum network of clocks," *Nature Physics*, vol. 10, no. 8, pp. 582–587, 2014.

[27] M. Ben-Or and A. Hassidim, "Fast quantum byzantine agreement," *Proceedings of the 37th Annual ACM Symposium on the Theory of Computing*, pp. 481–485, 2005.

[28] B. A. Bell, D. Markham, D. A. Herrera-Marti, *et al.*, "Experimental demonstration of graph state quantum secret sharing," *Nature Communications*, vol. 5, 2014.

[29] B. A. Bell, M. S. Tame, D. Markham, W. J. Wadsworth, and J. G. Rarity, "Experimental demonstration of a graph state quantum error-correction code," *Nature Communications*, vol. 5, 2014.

[30] A. Pappa, P. Jouguet, T. Lawson, *et al.*, "Experimental plug and play quantum coin flipping," *Nature Communications*, vol. 5, 2014.

[31] W. McCutcheon, A. Pappa, B. A. Bell, *et al.*, "Experimental verification of multipartite entanglement in quantum networks," *Nature Communications*, vol. 7, 2016.

[32] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, 2016.

[33] M. Bozzio, A. Orieux, L. Trigo Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Information*, vol. 4, no. 1, 2018.

[34] D. Mayers and A. Yao, "Self testing quantum apparatus," *Quantum Information and Computation*, vol. 4, no. 4, 2004.

[35] M. McKague, T. H. Yang, and V. Scarani, "Robust self-testing of the singlet," *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 45, 2012.

[36] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," *Physical Review A*, vol. 96, no. 1, 2017.

[37] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, "Verification of quantum computation: an overview of existing approaches," *Theory of Computing Systems*, vol. 63, no. 4, pp. 715–808, 2017.

[38] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," *Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science*, pp. 449–458, 2002.

[39] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, "Anonymous quantum communication," in *Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science* (K. Kurosawa, ed.), vol. 4833, Springer (Berlin, Heidelberg), 2007.

[40] "Quantum Protocol Zoo," *https://wiki.veriqloud.fr*, 2019.

[41] L. Zyga, "Practical anonymous communication protocol developed for quantum networks," *https://phys.org/news/2019-08-anonymous-protocol-quantum-networks.html*, 2019.

[42] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[43] M. A. Neumark, "On a representation of additive operator set functions," *USSR Academy of Sciences*, vol. 41, pp. 359–361, 1943.

[44] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, 1964.

[45] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, 1993.

[46] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[47] D. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Bell's Theorem, Quantum Theory and Conceptions of the Universe* (M. Kafatos, ed.), pp. 69–72, 1989.

[48] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, 1999.

[49] G. Tóth and I. Apellaniz, "Quantum metrology from a quantum information science perspective," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 42, 2014.

[50] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, no. 22, 2001.

[51] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Physical Review A*, vol. 68, no. 2, 2003.

[52] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Physical Review A*, vol. 78, no. 4, 2008.

[53] W. F. Stinespring, "Positive functions on C*-algebras," *Proceedings of the American Mathematical Society*, vol. 6, no. 2, pp. 211–216, 1955.

[54] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[55] A. Chefles, "Quantum state discrimination," *Contemporary Physics*, vol. 41, pp. 401–424, 2000.

[56] S. M. Barnett and S. Croke, "Quantum state discrimination," *Advances in Optics and Photonics*, vol. 1, no. 2, pp. 238–278, 2009.

[57] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[58] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, 1983.

[59] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, 1926.

[60] A. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, 1991.

[61] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.

[62] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters*, vol. 88, no. 5, 2002.

[63] H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, 2005.

[64] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, 2012.

[65] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.

[66] M. Blum, "Coin flipping by telephone: a protocol for solving impossible problems," *ACM SIGACT News*, vol. 15, no. 1, pp. 23–27, 1983.

[67] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Physical Review Letters*, vol. 109, no. 13, 2012.

[68] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, no. 3, 1999.

[69] D. Chaum, C. Crépeau, and I. Damgärd, "Multiparty unconditionally secure protocols," in *Advances in Cryptology - CRYPTO '87. Lecture Notes in Computer Science* (C. Pomerance, ed.), vol. 293, pp. 11–19, Springer (Berlin, Heidelberg), 1988.

[70] C. Crépeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," *Proceedings of the 34th Annual ACM Symposium on the Theory of Computing*, pp. 643–652, 2002.

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

[72] M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," *Physical Review A*, vol. 99, no. 2, 2019.

[73] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *Advances in Cryptology - ASIACRYPT 2005. Lecture Notes in Computer Science* (B. Roy, ed.), vol. 3788, pp. 217–235, Springer (Berlin, Heidelberg), 2005.

[74] V. Lipinska, G. Murta, and S. Wehner, "Anonymous transmission in a quantum network using the W state," *Physical Review A*, vol. 98, no. 5, 2018.

[75] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, no. 10, 1935.

[76] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical Review Letters*, vol. 23, no. 15, 1969.

[77] B. S. Cirel'son, "Quantum generalizations of Bell's inequality," *Letters in Mathematical Physics*, vol. 4, no. 2, pp. 93–100, 1980.

[78] E. Schrödinger, "Discussion of probability relations between separated systems," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, no. 4, pp. 555–563, 1935.

[79] H. M. Wiseman, S. J. Jones, and A. C. Doherty, "Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox," *Physical Review Letters*, vol. 98, no. 14, 2007.

[80] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, "Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox," *Physical Review A*, vol. 80, no. 3, 2009.

[81] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," *Physical Review A*, vol. 40, no. 8, pp. 4277–4281, 1989.

[82] J. S. Bell, *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, 1987.

[83] C. Abellán, A. Acín, A. Alarcón, *et al.*, "Challenging local realism with human choices," *Nature*, vol. 557, no. 7704, pp. 212–216, 2018.

[84] P. M. Pearle, "Hidden-variable example based upon data rejection," *Physical Review D*, vol. 2, no. 8, pp. 1418–1425, 1970.

[85] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum key distribution systems," *Physical Review A*, vol. 75, no. 3, 2007.

[86] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[87] I. Gerhardt, Q. Liu, A. A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Communications*, vol. 2, no. 1, 2011.

[88] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, 2011.

[89] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pp. 503–509, 1998.

[90] J. Barrett, L. Hardy, and A. Kent, "No signalling and quantum key distribution," *Physical Review Letters*, vol. 95, no. 1, 2005.

[91] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," *Physical Review Letters*, vol. 113, no. 14, 2014.

[92] R. Colbeck, *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, University of Cambridge, 2006.

[93] Y. Liu, Q. Zhao, M. H. Li, *et al.*, "Device-independent quantum random-number generation," *Nature*, vol. 562, no. 7728, pp. 548–551, 2018.

[94] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering," *Physical Review A*, vol. 85, no. 1, 2012.

[95] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, "Optimal randomness certification in the quantum steering and prepare-and-measure scenarios," *New Journal of Physics*, vol. 17, 2015.

[96] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, 2009.

[97] N. Gisin and B. Gisin, "A local hidden variable model of quantum correlation exploiting the detection loophole," *Physics Letters*, vol. 260, no. 5, pp. 323–327, 1999.

[98] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, no. 1, pp. 49–95, 1996.

[99] S. Wehner, "Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities," *Physical Review A*, vol. 73, no. 2, 2006.

[100] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," *Physical Review Letters*, vol. 98, no. 1, 2007.

[101] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New Journal of Physics*, vol. 10, 2008.

[102] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[103] C. H. Bennett, G. Brassard, and S. Breidbart, "Quantum cryptography II: how to re-use a one-time pad safely even if P=NP," *Natural Computing*, vol. 13, no. 4, pp. 453–458, 2014.

[104] I. B. Damgård, T. B. Pedersen, and L. Salvail, "A quantum cipher with near optimal key-recycling," in *Advances in Cryptology - CRYPTO 2005. Lecture Notes in Computer Science* (V. Shoup, ed.), vol. 3621, pp. 494–510, Springer (Berlin, Heidelberg), 2005.

[105] M. Curty and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A*, vol. 64, no. 6, 2001.

[106] S. Fehr and L. Salvail, "Quantum authentication and encryption with key recycling," in *Advances in Cryptology - EUROCRYPT 2017. Lecture Notes in Computer Science* (J. Coron and J. Nielsen, eds.), pp. 311–338, Springer (Cham), 2017.

[107] P. Hayden, D. W. Leung, and D. Mayers, "The universal composable security of quantum message authentication with key recycling," *arXiv:1610.09434*, 2016.

[108] C. Portmann, "Quantum authentication with key recycling," in *Advances in Cryptology - EUROCRYPT 2017. Lecture Notes in Computer Science* (J. S. Coron and J. Nielsen, eds.), vol. 10212, pp. 339–368, Springer (Cham), 2017.

[109] D. Markham and A. Marin, "Practical sharing of quantum secrets over untrusted channels," in *Information Theoretic Security - ICITS 2015. Lecture Notes in Computer Science* (A. Lehmann and S. Wolf, eds.), vol. 9063, pp. 1–14, Springer (Cham), 2015.

[110] M. Horodecki, P. Horodecki, and R. Horodecki, "General teleportation channel, singlet fraction and quasi-distillation," *Physical Review A*, vol. 60, no. 3, 1999.

[111] A. Orieux, M. Kaplan, V. Venuti, T. Pramanik, I. Zaquine, and E. Diamanti, "Experimental detection of steerability in Bell local states with two measurement settings," *Journal of Optics*, vol. 20, 2018.

[112] D. Markham and A. Krause, "A simple protocol for certifying graph states and applications in quantum networks," *arXiv:1801.05057*, 2018.

[113] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, 2007.

[114] S. Pironio, A. Acín, S. Massar, *et al.*, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[115] N. Walk, S. Hosseini, J. Geng, *et al.*, "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution," *Optica*, vol. 3, no. 6, pp. 634–642, 2016.

[116] M. McKague and M. Mosca, "Generalized self-testing and the security of the 6-state protocol," in *Theory of Quantum Computation, Communication, and Cryptography - TQC 2010. Lecture Notes in Computer Science* (W. van Dam, V. Kendon, and S. Severini, eds.), vol. 6519, pp. 113–130, Springer (Berlin, Heidelberg), 2010.

[117] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, "Robust self-testing of the three-qubit W state," *Physical Review A*, vol. 90, no. 4, 2014.

[118] K. F. Pál, T. Vértesi, and M. Navascués, "Device-independent tomography of multipartite quantum states," *Physical Review A*, vol. 90, no. 4, 2014.

[119] F. Baccari, D. Cavalcanti, P. Wittek, and A. Acín, "Efficient device-independent entanglement detection for multipartite systems," *Physical Review X*, vol. 7, no. 2, 2017.

[120] A. Coladangelo, K. T. Goh, and V. Scarani, "All pure bipartite entangled states can be self-tested," *Nature Communications*, vol. 8, 2017.

[121] J. Kaniewski, "Self-testing of binary observables based on commutation," *Physical Review A*, vol. 95, no. 6, 2017.

[122] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, "Physical characterization of quantum devices from nonlocal correlations," *Physical Review A*, vol. 91, no. 2, 2015.

[123] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, "Self-testing of Pauli observables for device-independent entanglement certification," *Physical Review A*, vol. 98, no. 3, 2018.

[124] A. Gheorghiu, P. Wallden, and E. Kashefi, "Rigidity of quantum steering and one-sided device-independent verifiable quantum computation," *New Journal of Physics*, vol. 19, 2017.

[125] I. Šupić and M. J. Hoban, "Self-testing through EPR-steering," *New Journal of Physics*, vol. 18, 2016.

[126] I. Šupić and J. Bowles, "Self-testing of quantum systems: a review," *arXiv:1904.10042*, 2019.

[127] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," *Nature*, vol. 496, 2013.

[128] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, "Robust and versatile black-box certification of quantum devices," *Physical Review Letters*, vol. 113, no. 4, 2014.

[129] J. Kaniewski, "Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities," *Physical Review Letters*, vol. 117, no. 7, 2016.

[130] M. Hajdušek, C. Pérez-Delgado, and J. F. Fitzsimons, "Device-independent verifiable blind quantum computation," *arXiv:1502.02563v2*, 2015.

[131] R. Arnon-Friedman and J.-D. Bancal, "Device-independent certification of one-shot distillable entanglement," *New Journal of Physics*, vol. 21, 2019.

[132] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, "Phase-compensated ultra-bright source of entangled photons," *Optics Express*, vol. 13, no. 22, 2005.

[133] B. G. Christensen, K. T. McCusker, J. B. Altepeter, *et al.*, "Detection-loophole-free test of quantum nonlocality, and applications," *Physical Review Letters*, vol. 111, no. 13, 2013.

[134] F. Kaiser, L. A. Ngah, A. Issautier, *et al.*, "Polarization entangled photon-pair source based on quantum nonlinear photonics and interferometry," *Optics Communications*, vol. 327, pp. 7–16, 2014.

[135] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, "Experimental EPR-steering of Bell-local states," *Nature Physics*, vol. 6, pp. 845–849, 2010.

[136] T. Pramanik, M. Kaplan, and A. S. Majumdar, "Fine-grained EPR-steering inequalities," *Physical Review A*, vol. 90, no. 5, 2014.

[137] B. Wittmann, S. Ramelow, F. Steinlechner, *et al.*, "Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering," *New Journal of Physics*, vol. 14, 2012.

[138] D. H. Smith, G. Gillett, M. P. De Almeida, *et al.*, "Conclusive quantum steering with superconducting transition-edge sensors," *Nature Communications*, vol. 3, 2012.

[139] A. J. Bennet, D. A. Evans, D. J. Saunders, *et al.*, "Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole," *Physical Review X*, vol. 2, no. 3, 2012.

[140] B. Hensen, H. Bernien, A. E. Dréau, *et al.*, "Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km," *Nature*, vol. 526, 2015.

[141] M. Giustina, M. A. Versteegh, S. Wengerowsky, *et al.*, "Significant-loophole-free test of Bell's theorem with entangled photons," *Physical Review Letters*, vol. 115, no. 25, 2015.

[142] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, *et al.*, "Strong loophole-free test of local realism," *Physical Review Letters*, vol. 115, no. 25, 2015.

[143] CVX Research Inc., "CVX: Matlab software for disciplined convex programming, version 2.0," *http://cvxr.com/cvx*, 2012.

[144] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control. Lecture Notes in Control and Information Sciences* (V. Blondel, S. Boyd, and H. Kimura, eds.), vol. 371, pp. 95–110, Springer (London), 2008.

[145] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *The Annals of Mathematical Statistics*, vol. 23, no. 4, pp. 493–507, 1952.

[146] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[147] K. Azuma, "Weighted sums of certain dependent random variables," *Tohoku Mathematical Journal*, vol. 19, no. 3, pp. 357–367, 1967.

[148] S. Pironio, V. Scarani, and T. Vidick, "Focus on device independent quantum information," *New Journal of Physics*, vol. 18, 2016.

[149] S. Popescu, "Bell's inequalities versus teleportation: what is nonlocality?," *Physical Review Letters*, vol. 72, no. 6, pp. 797–799, 1994.

[150] P.-S. Lin, D. Rosset, Y. Zhang, J.-D. Bancal, and Y.-C. Liang, "Device-independent point estimation from finite data and its application to device-independent property estimation," *Physical Review A*, vol. 97, no. 3, 2018.

[151] M. O. Renou, J. Kaniewski, and N. Brunner, "Self-testing entangled measurements in quantum networks," *Physical Review Letters*, vol. 121, no. 25, 2018.

[152] J.-D. Bancal, N. Sangouard, and P. Sekatski, "Noise-resistant device-independent certification of Bell state measurements," *Physical Review Letters*, vol. 121, no. 25, 2018.

[153] S. Wollmann, N. Walk, A. J. Bennet, H. M. Wiseman, and G. J. Pryde, "Observation of genuine one-way Einstein-Podolsky-Rosen steering," *Physical Review Letters*, vol. 116, no. 16, 2016.

[154] J. Boyan, "The Anonymizer: protecting user privacy on the Web," *Computer-Mediated Communication Magazine*, vol. 4, no. 9, 1997.

[155] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[156] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[157] A. Yao, "Protocols for secure computations," *Proceedings of the 23rd Annual Symposium on the Foundations of Computer Science*, pp. 160–164, 1982.

[158] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game, or a completeness theorem for protocols with honest majority," *Proceedings of the 19th Annual ACM Symposium on the Theory of Computing*, pp. 218–229, 1987.

[159] A. Broadbent and A. Tapp, "Information-theoretic security without an honest majority," in *Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science* (K. Kurosawa, ed.), vol. 4833, pp. 410–426, Springer (Berlin, Heidelberg), 2007.

[160] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties," *Physical Review Letters*, vol. 108, no. 26, 2012.

[161] T. Monz, P. Schindler, J. T. Barreiro, *et al.*, "14-qubit entanglement: creation and coherence," *Physical Review Letters*, vol. 106, no. 13, 2011.

[162] X.-L. Wang, L.-K. Chen, W. Li, *et al.*, "Experimental ten-photon entanglement," *Physical Review Letters*, vol. 117, no. 21, 2016.

[163] T. Okamoto, K. Suzuki, and Y. Tokunaga, "Quantum voting scheme based on conjugate coding," *NTT Technical Review*, vol. 6, no. 1, 2008.

[164] R.-R. Zhou and L. Yang, "Distributed quantum election scheme," *arXiv:1304.0555*, 2013.

[165] M. Arapinis, E. Kashefi, N. Lamprou, and A. Pappa, "A comprehensive analysis of quantum e-voting protocols," *arXiv:1810.05083*, 2018.

[166] A. Uhlmann, "The 'transition probability' in the state space of a *-algebra," *Reports on Mathematical Physics*, vol. 9, no. 2, 1976.

[167] E. Kashefi and A. Pappa, "Multiparty delegated quantum computing," *Cryptography*, vol. 1, no. 2, p. 12, 2017.

[168] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[169] N. Shettell and D. Markham, "Graph states as a resource for quantum metrology," *arXiv:1908.05047*, 2019.

[170] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," *Physical Review A*, vol. 69, no. 6, pp. 1–22, 2004.

[171] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. van den Nest, and H. J. Briegel, "Entanglement in graph states and its applications," *Quantum Computers, Algorithms and Chaos*, pp. 1–99, 2006.

[172] D. Browne and H. Briegel, "One-way quantum computation," *arXiv:quant-ph/0603226*, 2006.

[173] M. Hayashi and T. Morimae, "Verifiable measurement-only blind quantum computing with stabilizer testing," *Physical Review Letters*, vol. 115, no. 22, 2015.

[174] Y. Takeuchi and T. Morimae, "Verification of many-qubit states," *Physical Review X*, vol. 8, no. 2, 2018.

[175] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, "Resource-efficient verification of quantum computing using Serfling's bound," *npj Quantum Information*, vol. 5, 2019.

[176] R. J. Serfling, "Probability inequalities for the sum in sampling without replacement," *The Annals of Statistics*, vol. 2, no. 1, pp. 39–48, 1974.

[177] M. McKague, "Self-testing graph states," in *Theory of Quantum Computation, Communication, and Cryptography - TQC 2011. Lecture Notes in Computer Science* (D. Bacon, M. Martin-Delgado, and M. Roetteler, eds.), vol. 6745, pp. 104–120, Springer (Berlin, Heidelberg), 2011.

[178] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Physical Review Letters*, vol. 77, no. 1, 1996.