Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources

Abstract. The problem of reliably certifying the outcome of a computation performed by a quantum device is rapidly gaining relevance. We present two protocols for a classical verifier to verifiably delegate a quantum computation to two non-communicating but entangled quantum provers. Our protocols have near-optimal complexity in terms of the total resources employed by the verifier and the honest provers, with the total number of operations of each party, including the number of entangled pairs of qubits required of the honest provers, scaling as $O(g \log g)$ for delegating a circuit of size g. This is in contrast to previous protocols, whose overhead in terms of resources employed, while polynomial, is far beyond what is feasible in practice. Our first protocol requires a number of rounds that is linear in the depth of the circuit being delegated, and is blind, meaning neither prover can learn the circuit or its input. The second protocol is not blind, but requires only a constant number of rounds of interaction.
Our main technical innovation is an efficient rigidity theorem which allows a verifier to test that two entangled provers perform measurements specified by an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs, with a robustness that is independent of m. Our two-prover classical-verifier delegation protocols are obtained by combining this rigidity theorem with a single-prover quantum-verifier protocol for the verifiable delegation of a quantum computation, introduced by Broadbent.

1 Introduction

Quantum computers hold the potential to speed up a wide range of computational tasks (see, for example, [Mon16]). Recent progress towards implementing limited quantum devices has added urgency to the already important question of how a classical verifier can test a quantum device. This verifier could be an experimentalist running a new experimental setup; a consumer who has purchased a purported quantum device; or a client who wishes to delegate some task to a quantum server. In all cases, the user would like to exert some form of control over the quantum device. For example, the experimentalist may think that she is testing that a particular experiment prepares a certain quantum state by performing a series of measurements, i.e. by state tomography, but this assumes some level of trust in the measurement apparatus being used. For a classical party to truly test a quantum system, that system should be modeled in a device-independent way, having classical inputs (e.g. measurement settings) and classical outputs (e.g. measurement results).

Tests of quantum mechanical properties of a system first appeared in the form of Bell tests [Bel64,CHSH69]. In a Bell test, a verifier asks classical questions to a quantum-device and receives classical answers. These tests make one crucial assumption on the system to be tested: that it consists of two spatially isolated components that are unable to communicate throughout the experiment. One can then upper bound the value of some statistical quantity of interest subject to the constraint that the two devices do not share any entanglement. Such a bound is referred to as a Bell inequality. While the violation of a Bell inequality can be seen as a certificate of entanglement, the area of self-testing, first introduced in [MY04], allows for the certification of much stronger statements, including about which measurements are being performed, and on which state. Informally, a *robust rigidity theorem* is a statement about which kind of apparatus, quantum state and measurements, must be used by a pair of isolated devices in order to succeed in a given statistical test. Following a well-established tradition, we will refer to such tests as *games*, call the devices *players* (or *provers*), and the quantum state and measurements that they implement the *strategy* of the players. A rigidity theorem is a statement about the necessary structure of near-optimal strategies for a game.

In 2012, Reichardt, Unger and Vazirani proved a robust rigidity theorem for playing a sequence of n CHSH games [RUV13]. Aside from its intrinsic interest, this rigidity theorem had two important consequences. One was the first device-independent protocol for quantum key distribution. The second was a protocol whereby a completely classical verifier can test a universal quantum computer consisting of two non-communicating devices. The resulting protocol for delegating quantum computations has received a lot of attention as the first classical-verifier delegation protocol. The task is well-motivated: for the foreseeable future, making use of a quantum computer will likely require delegating the computation to a potentially untrusted cloud service, such as that announced by IBM [Cas17].

Unfortunately, the complexity overhead of the delegation protocol from [RUV13], in terms of both the number of EPR pairs needed for the provers and the overall time complexity of the provers as well as the (classical) verifier, while polynomial, is prohibitively large. Although the authors of [RUV13] do not provide an explicit value for the exponent, in [HPDF15] it is estimated that their protocol requires resources that scale like $\Omega(g^{8192})$, where g is the number of gates in the delegated circuit (notwithstanding the implicit constant, this already makes the approach thoroughly impractical for even a 2-gate circuit!). The large overhead is in part due to a very small (although still inverse polynomial) gap between the completeness and soundness parameters of the rigidity theorem; this requires the verifier to perform many more Bell tests than the actual number of EPR pairs needed to implement the computation, which would scale linearly with the circuit size.

Subsequent work has presented significantly more efficient protocols for achieving the same, or similar, functionality [McK16,GKW15,HPDF15]. We refer to Table 1 for a summary of our estimated lower bounds on the complexity of each of these results (not all papers provide explicit bounds, in which case our estimates, although generally conservative, should be taken with caution). Prior to our work, the best two-prover delegation protocol required resources scaling like g^{2048} for delegating a g-gate circuit. Things improve significantly if we allow for more than two provers, however, the most efficient multi-prover delegation protocols still required resources that scale as at least

$\Omega(g^4 \log g)$ for delegating a g-gate circuit on n qubits. Since we expect that in the foreseeable future most quantum computations will be delegated to a third-party server, even such small polynomial overhead is unacceptable, as it already negates the quantum advantage for a number of problems, such as quantum search.

The most efficient classical-verifier delegation protocols known [FH15,NV17], with $\mathrm{poly}(n)$ and 7 provers, respectively, require resources that scale as $O(g^3)$, but this efficiency comes at the cost of a technique of "post-hoc" verification. In this technique, the provers must learn the verifier's input even before they are separated, so that they can prepare the history state for the computation.[1] As a result, these protocols are not blind[2]. Moreover, while the method does provide a means for verifying the outcome of an arbitrary quantum computation, in contrast to [RUV13] it does not provide a means for the verifier to test the provers' implementation of the required circuit on a gate-by-gate basis. Other works, such as [HH16], achieve two-prover verifiable delegation with complexity that scales like $O(g^4 \log g)$, but in much weaker models; for example, in [HH16] the provers' private system is assumed a priori to be in tensor product form, with well-defined registers. General techniques are available to remove the strong assumption, but they would lead to similar large overhead as previous results.

In contrast, in the setting where the verifier is allowed to have some limited quantum power, such as the ability to generate single-qubit states and measure them with observables from a small finite set, efficient schemes for blind verifiable delegation do exist [ABE10,FK17,Mor14,Bro18,HM15,MF16,FH17,MTH17] (see also [Fit16] for a recent survey). In this case, only a single prover is needed, and the most efficient *single-prover quantum-verifier* protocols can evaluate a quantum circuit with g gates in time $O(g)$. The main reason these protocols are much more efficient than the classical-verifier multi-prover protocols is that they avoid the need for directly testing any of the qubits used by the prover, instead requiring the trusted verifier to directly either prepare or measure the qubits used for the computation.

New rigidity results. We overcome the efficiency limitations of multi-prover delegation protocols by introducing a new robust rigidity theorem. Our theorem allows a classical verifier to certify that two non-communicating provers apply a measurement associated with an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs. This is the first result to achieve self-testing for such a large class of measurements. The majority of previous works in self-testing have been primarily concerned with certifying the state and were limited to simple single-qubit measurements in the X-Z plane. Prior self-testing results for multi-qubit measurements only allow to test for tensor products of σ_X and σ_Z observables. While this is sufficient for verification in the post-hoc model of [FH15], testing for σ_X and σ_Z observables does not directly allow for the verification of a general computation (unless one relies on techniques such as process tomography [RUV13], which introduce substantial additional overhead).

[1] Using results of Ji [Ji16], this allows the protocol to be single-round. Alternatively, the state can be created by a single prover and teleported to the others with the help of the verifier, resulting in a two-round protocol.

[2] *Blindness* is a property of delegation protocols, which informally states that the prover learns nothing about the verifier's private circuit.

	Provers	Rounds	Total Resources	Blind
RUV 2012 [RUV13]	2	poly(n)	$\geq g^{8192}$	yes
McKague 2013 [McK16]	poly(n)	poly(n)	$\geq 2^{153} g^{22}$	yes
GKW 2015 [GKW15]	2	poly(n)	$\geq g^{2048}$	yes
HDF 2015 [HPDF15]	poly(n)	poly(n)	$\Theta(g^4 \log g)$	yes
Verifier-on-a-Leash Protocol (Section 4)	2	$O(\text{depth})$	$\Theta(g \log g)$	yes
Dog-Walker Protocol (Section 5)	2	$O(1)$	$\Theta(g \log g)$	no

Table 1: Resource requirements of various delegation protocols in the multi-prover model. We use n to denote the number of qubits and g the number of gates in the delegated circuit. "depth" refers to the depth of the delegated circuit. "Total Resources" refers to the gate complexity of the provers, the number of EPR pairs of entanglement needed, and the number of bits of communication in the protocol. To ensure fair comparison, each protocol is required to produce the correct answer with probability 99%. For all protocols except our two new protocols, this requires a polynomial number of sequential repetitions, which is taken into account when computing the total resources.

Our first contribution is to extend the "Pauli braiding test" of [NV17], which allows to test tensor products of σ_X and σ_Z observables with constant robustness, to allow for σ_Y observables as well. This is somewhat subtle due to an ambiguity in the complex phase that cannot be detected by any classical two-player test; we formalize the ambiguity and show how it can be effectively accounted for. Our second contribution is to substantially increase the set of elementary gates that can be tested, to include arbitrary m-qubit tensor products of single-qubit Clifford observables. This is achieved by introducing a new "conjugation test", which tests how an observable applied by the provers acts on the Pauli group. The test is inspired by general results of Slofstra [Slo16], but is substantially more direct.

A key feature of our rigidity results is that their robustness scales independently of the number of EPR pairs tested, as in [NV17]. This is crucial for the efficiency of our delegation protocols. The robustness for previous results in parallel self-testing typically had a polynomial dependence on the number of EPR pairs tested. We give an informal statement of our robust rigidity theorem.

Theorem 1 (Informal). *Let $m \in \mathbb{Z}_{>0}$. Let $\mathcal{G}$ be a fixed, finite set of single-qubit Clifford observables. Then there exists an efficient two-prover test* $\text{RIGID}(\mathcal{G}, m)$ *with $O(m)$-bit questions (a constant fraction of which are of the form $W \in \mathcal{G}^m$) and answers such that the following properties hold:*

- *(Completeness) There is a strategy for the provers that uses $m+1$ EPR pairs and succeeds with probability at least $1 - e^{-\Omega(m)}$ in the test.*
- *(Soundness) For any $\varepsilon > 0$, any strategy for the provers that succeeds with probability $1 - \varepsilon$ in the test must be* $\text{poly}(\varepsilon)$*-close, up to local isometries, to a strategy in which the provers begin with $(m+1)$ EPR pairs and is such that upon receipt of a question of the form $W \in \mathcal{G}^m$ the prover measures the "correct" observable W.*

Although we do not strive to obtain the best dependence on ε, we believe it should be possible to obtain a scaling of the form $C\sqrt{\varepsilon}$ for a reasonable constant C. We discuss the test in Section 3. The complete analysis is given in Section A of the supplemental material.

New delegation protocols. We employ the new rigidity theorem to obtain two new efficient two-prover classical-verifier protocols in which the complexity of verifiably delegating a g-gate quantum circuit scales as $O(g \log g)$.[3]

We achieve our protocols by adapting the efficient single-prover quantum-verifier delegation protocol introduced by Broadbent [Bro18] (we refer to this as the "EPR protocol"), which has the advantage of offering a direct implementation of the delegated circuit, in the circuit model of computation and with very little modification needed to ensure verifiability, as well as a relatively simple and intuitive analysis.

Our first protocol is blind, and requires a number of rounds of interaction that scales linearly with the depth of the circuit being delegated. The second protocol is not blind, but only requires a constant number of rounds of interaction with the provers. Our work is the first to propose verifiable two-prover delegation protocols that overcome the prohibitively large resource requirements of all previous multi-prover protocols, requiring only a quasilinear amount of resources, in terms of number of EPR pairs and time. However, notwithstanding our improvements, a physical implementation of verifiable delegation protocols remains a challenging task for the available technology.

We introduce the protocols in more detail. The protocols provide different methods to delegate the quantum computation performed by the quantum verifier from [Bro18] to a second prover (call him PV for Prover V). The rigidity test is used to verify that the second prover indeed performs the same actions as the honest verifier, which are sequences of single-qubit measurements of Clifford observables from the set $\Sigma = \{X, Y, Z, F, G\}$ (where F and G are defined in (2)).

In the first protocol, one of the provers plays the role of Broadbent's prover (call him PP for Prover P), and the other plays the role of Broadbent's verifier (PV). The protocol is divided into two sub-games; which game is played is chosen by the verifier by flipping a biased coin with appropriately chosen probabilities.

– The first game is a sequential version of the rigidity game $\text{RIGID}(\Sigma, m)$ (from Theorem 1) described in Figure 9. This aims to enforce that PV performs precisely the right measurements;
– The second game is the delegation game, described in Figures 6, 7, and 8, and whose structure is summarized in Figure 4. Here the verifier guides PP through the computation in a similar way as in the EPR Protocol.

We remark that in both sub-games, the questions received by PV are of the form $W \in \Sigma^m$, where $\Sigma = \{X, Y, Z, F, G\}$ is the set of measurements performed by the verifier in Broadbent's EPR protocol. The questions for PV in the two sub-games are sampled from the same distribution. This ensures that the PV is not able to tell which

[3] The $\log g$ overhead is due to the complexity of sampling from the right distribution in rigidity tests. We leave the possibility of removing this by derandomization for future work. Another source of overhead is in achieving blindness: in order to hide the circuit, we encode it as part of the input to a universal circuit, introducing a factor of $O(\log g)$ overhead.

kind of game is being played. Hence, we can use our rigidity result of Theorem 1 to guarantee honest behavior of PV in the delegation sub-game. We call this protocol *Verifier-on-a-Leash Protocol*, or "leash protocol" for short.

The protocol requires $(2d+1)$ rounds of interaction, where d is the depth of the circuit being delegated (see Section 2.3 for a precise definition of how this is computed). The protocol requires $O(n+g)$ EPR pairs to delegate a g-gate circuit on n qubits, and the overall time complexity of the protocol is $O(g \log g)$. The input to the circuit is hidden from the provers, meaning that the protocol can be made blind by encoding the circuit in the input, and delegating a universal circuit.

The completeness of the protocol follows directly from the completeness of [Bro18]. Once we ensure the correct behavior of PV using our rigidity test, soundness follows from [Bro18] as well, since the combined behavior of our verifier and an honest PV is nearly identical to that of Broadbent's verifier.

The second protocol also starts from Broadbent's protocol, but modifies it in a different way to achieve a protocol that only requires a constant number of rounds of interaction. The proof of security is slightly more involved, but the key ideas are the same: we use a combination of our new self-testing results and the techniques of Broadbent's protocol to control the two provers, one of which plays the role of Broadbent's verifier, and the other the role of the prover. Because of the more complicated "leash" structure in this protocol, we call it the *Dog-Walker Protocol*. Like the leash protocol, the Dog-Walker Protocol has overall time complexity $O(g \log g)$. Unlike the leash protocol, the Dog-Walker protocol is not blind. In particular, while PV and PP would have to collude after the protocol is terminated to learn the input in the leash protocol, in the Dog-Walker protocol, PV simply receives the input in clear.

Based on the Dog-Walker Protocol, it is possible to design a classical-verifier two-prover protocol for all languages in QMA. This is achieved along the same lines as the proof that QMIP = MIP* from [RUV13]. The first prover, given the input, creates the QMA witness and teleports it to the second prover with the help of the verifier. The verifier then delegates the verification circuit to the second prover, as in the Dog-Walker Protocol; the first prover can be re-used to verify the operations of the second one.

Subsequent work. Bowles et al. [BvCA18] have independently re-derived a variant of our rigidity test for multi-qubit σ_X, σ_Y and σ_Z observables in the context of entanglement certification protocols in quantum networks. Their self-test result has a slightly smaller set of questions but significantly weaker robustness bounds.

Recently [Gri17] proposed the first protocol for verifiable delegation of quantum computation by classical clients where such space-like separation can replace the non-communication assumption, but his protocol is not blind.

Open questions and directions for future work. We have introduced a new rigidity theorem and shown how it can be used to transform a specific quantum-verifier delegation protocol, due to Broadbent, into a classical-verifier protocol with an additional prover, while suffering very little overhead in terms of the efficiency of the protocol. We believe that a similar transformation could be performed starting from delegation protocols based on other models of computation, such as the protocol in the measurement-based model of [FK17] or the protocol based on computation by teleportation considered in [RUV13], and would lead to similar efficiency improvements.

Recently, [HZM+17] provided an experimental demonstration of a two-prover delegation protocol based on [RUV13] for a 3-qubit quantum circuit based on Shor's algorithm to factor the number 15; in order to obtain an actual implementation, necessitating "only" on the order of 6000 CHSH tests, the authors had to make the strong assumption that the devices behave in an i.i.d. manner at each use, and could not use the most general testing results from [RUV13]. We believe that our improved rigidity theorem could lead to an implementation that does not require any additional assumption.

We note that our protocols require the verifier to communicate with one prover after at least one round of communication with the other has been completed. Therefore, the requirement that the provers do not communicate throughout the protocol cannot be enforced through space-like separation, and must be taken as an a priori assumption. Since the protocol of [Gri17] is not blind, it is an open question whether there exists a two-prover delegation protocol that consists of a single round of simultaneous communication with each prover, and is blind and verifiable. A different avenue to achieve this is to rely on computational assumptions on the power of the provers to achieve protocols with more properties (non-interactive, blind, verifiable) [DSS16,ADSS17,Mah17,Mah18], albeit not necessarily in a truly efficient manner.

Finally, due to its efficiency and robustness, our ridigity theorem is a potentially useful tool in many other cryptographic protocols. For instance, an interesting direction to explore is the possibility of exploiting our theorem to achieve more efficient protocols for device-independent quantum key distribution, entanglement certification or other cryptographic protocols involving more complex untrusted computation of the users.

Organization. In Section 2, we give the necessary preliminaries, including outlining Broadbent's EPR Protocol (Section 2.3). In Section 3, we introduce our new rigidity theorems. In Section 4, we present our first protocol, the leash protocol, and in Section 5, we discuss our second protocol, the Dog-Walker Protocol.

2 Preliminaries

2.1 Notation

We often write $\boldsymbol{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ for a string of bits, and $W = W_1 \cdots W_m \in \Sigma^m$ for a string, where Σ is a finite alphabet. If $S \subseteq \{1, \ldots, m\}$ we write W_S for the sub-string of W indexed by S. For an event E, we use 1_E to denote the indicator variable for that event, so $1_E = 1$ if E is true, and otherwise $1_E = 0$. We write $\mathrm{poly}(\varepsilon)$ for $O(\varepsilon^c)$, where c is a universal constant that may change each time the notation is used.

$\mathcal{H}$ is a finite-dimensional Hilbert space. We denote by $\mathrm{U}(\mathcal{H})$ the set of unitary operators, $\mathrm{Obs}(\mathcal{H})$ the set of binary observables (we omit the term "binary" from here on; in this paper all observables are binary) and $\mathrm{Proj}(\mathcal{H})$ the set of projective measurements on $\mathcal{H}$ respectively. We let $|\mathrm{EPR}\rangle$ denote an EPR pair:

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right).$$

Observables. We use capital letters $X, Z, W, \ldots$ to denote observables. We use greek letters σ, τ with a subscript σ_W, τ_W, to emphasize that the observable W specified as subscript acts in a particular basis. For example, X is an arbitrary observable but σ_X is specifically the Pauli X matrix defined in (1).

For $a \in \{0,1\}^n$ and commuting observables $\sigma_{W_1}, \ldots, \sigma_{W_n}$, we write $\sigma_W(a) = \prod_{i=1}^n (\sigma_{W_i})^{a_i}$. The associated projective measurements are $\sigma_{W_i} = \sigma_{W_i}^0 - \sigma_{W_i}^1$ and $\sigma_W^u = \mathrm{E}_a(-1)^{u\cdot a}\sigma_W(a)$. Often the σ_{W_i} will be single-qubit observables acting on distinct qubits, in which case each is implicitly tensored with identity outside of the qubit on which it acts.

Pauli and Clifford groups. Let

$$\sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{and} \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

denote the standard Pauli matrices acting on a qubit. The single-qubit Weyl-Heisenberg group

$$\mathcal{H}^{(1)} = H(\mathbb{Z}_2) = \Big\{ (-1)^c \sigma_X(a)\sigma_Z(b),\ a,b,c \in \{0,1\} \Big\}$$

is the matrix group generated by the Pauli σ_X and σ_Z. We let $\mathcal{H}^{(n)} = H(\mathbb{Z}_2^n)$ be the direct product of n copies of $\mathcal{H}^{(1)}$. The n-qubit Clifford group is the normalizer of $\mathcal{H}^{(n)}$ in the unitary group, up to phase:

$$G_C^{(n)} = \big\{ G \in \mathrm{U}((\mathbb{C}^2)^{\otimes n}) :\ G\sigma G^\dagger \in \mathcal{H}^{(n)} \quad \forall \sigma \in \mathcal{H}^{(n)} \big\}.$$

Some Clifford observables we will use include

$$\sigma_H = \frac{\sigma_X + \sigma_Z}{\sqrt{2}}, \quad \sigma_{H'} = \frac{\sigma_X - \sigma_Z}{\sqrt{2}}, \quad \sigma_F = \frac{-\sigma_X + \sigma_Y}{\sqrt{2}}, \quad \sigma_G = \frac{\sigma_X + \sigma_Y}{\sqrt{2}}. \tag{2}$$

Note that σ_H and $\sigma_{H'}$ are characterized by $\sigma_X\sigma_H\sigma_X = \sigma_{H'}$ and $\sigma_Z\sigma_H\sigma_Z = -\sigma_{H'}$. Similarly, σ_F and σ_G are characterized by $\sigma_X\sigma_F\sigma_X = -\sigma_G$ and $\sigma_Y\sigma_F\sigma_Y = \sigma_G$.

2.2 Quantum circuits

We use capital letters in sans-serif font to denote gates. We work with the universal quantum gate set $\{\mathsf{CNOT}, \mathsf{H}, \mathsf{T}\}$, where the controlled-not gate is the two-qubit gate with the unitary action

$$\mathsf{CNOT}|b_1, b_2\rangle = |b_1, b_1 \oplus b_2\rangle,$$

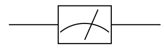
and the Hadamard and T gates are single-qubit gates with actions

$$\mathsf{H}|b\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^b|1\rangle\Big) \quad \text{and} \quad \mathsf{T}|b\rangle = e^{ib\pi/4}|b\rangle,$$

respectively. We will also use the following gates:

$$\mathsf{X}|b\rangle = |b \oplus 1\rangle, \quad \mathsf{Z}|b\rangle = (-1)^b|b\rangle, \quad \text{and} \quad \mathsf{P}|b\rangle = i^b|b\rangle.$$

Measurements in the Z basis (or computational basis) will be denoted by the standard measurement symbol:



To measure another observable, W, we can perform a unitary change of basis U_W before the measurement in the computational basis.

We assume that every circuit has a specified output wire, which is measured at the end of the computation to obtain the output bit. Without loss of generality, we can assume this is always the first wire. For an n-qubit system, we let Π_b, for $b \in \{0,1\}$, denote the orthogonal projector onto states with $|b\rangle$ in the output wire: $|b\rangle\langle b| \otimes \mathrm{Id}$. For example, the probability that a circuit Q outputs 0 on input $|\boldsymbol{x}\rangle$ is $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2$.

We can always decompose a quantum circuit into layers such that each layer contains at most one T gate applied to each wire. The minimum number of layers for which this is possible is called the T *depth* of the circuit. We note that throughout this work, we will assume circuits are compiled in a specific form that introduces extra T gates (see the paragraph on the H gadget in Section 2.3). The T depth of the resulting circuit is proportional to the depth of the original circuit.

2.3 Broadbent's EPR Protocol

In this section we summarize the main features of a delegation protocol introduced in [Bro18], highlighting the aspects that will be relevant to understanding our subsequent adaptation into two-prover protocols. The "EPR Protocol" from [Bro18] involves the interaction between a verifier V_{EPR} and a prover P. We write P_{EPR} for the "honest" behavior of the prover. The verifier V_{EPR} has limited quantum powers. Her goal is to delegate a BQP computation to the prover P in a verifiable way. Specifically, the verifier has as input a quantum circuit Q on n qubits and an input string $\boldsymbol{x} \in \{0,1\}^n$, and the prover gets as input Q. The verifier and prover interact. At the end of the protocol, the verifier outputs either accept or reject. The protocol is such that there exist values p_{sound} and p_{compl} with $p_{\text{sound}} < p_{\text{compl}}$ such that $p_{\text{compl}} - p_{\text{sound}}$, called the *soundness-completeness gap*, is a constant independent of input size, and moreover:

Completeness: If the prover is honest and $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \geq 2/3$, then the verifier outputs accept with probability at least p_{compl};

Soundness: If $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \leq 1/3$, then the probability the verifier outputs accept is at most p_{sound}.

In the EPR protocol, V_{EPR} and P_{EPR} are assumed to share $(n+t)$ EPR pairs at the start of the protocol, where t is the number of T gates in Q and n the number of input bits. (In [Bro18] the EPR protocol is only considered in the analysis, and it is assumed that the EPR pairs are prepared by the verifier.) The first n EPR pairs correspond to the input to the computation; they are indexed by $N = \{1,\ldots,n\}$. The remaining pairs are indexed by $T = \{n+1,\ldots,n+t\}$; they will be used as ancilla qubits to implement each of the T gates in the delegated circuit.

The behavior of V_{EPR} depends on a *round type* randomly chosen by V_{EPR} after her interaction with P_{EPR}. There are three possible round types:

- Computation round ($r = 0$): the verifier delegates the computation to P_{EPR}, and at the end of the round can recover its output if P_{EPR} behaves honestly;
- X-test round ($r = 1$) and Z-test round ($r = 2$): the verifier tests that P_{EPR} behaves honestly, and rejects if malicious behavior is detected.

For some constant p, V chooses $r = 0$ with probability p, and otherwise chooses $r \in \{1,2\}$ with equal probability. Since the choice of round type is made after interaction with P_{EPR}, P_{EPR}'s behavior cannot depend on the round type. In particular, any deviating behavior in a computation round is reproduced in both types of test rounds. The analysis amounts to showing that any deviating behavior that affects the outcome of the computation will be detected in at least one of the test rounds.

In slightly more detail, the high-level structure of the protocol is the following. V_{EPR} measures her halves of the n qubits in N in order to prepare the input state on P_{EPR}'s system. As a result the input is quantum one-time padded with keys that depend on V_{EPR}'s measurement results. For example, in a computation round, V_{EPR} measures each input qubit in the Z basis, and gets some result $\boldsymbol{d} \in \{0,1\}^n$, meaning the input on P_{EPR}'s side has been prepared as $\mathsf{X}^{\boldsymbol{d}}|0\rangle^{\otimes n}$. In [Bro18], the input is always considered to be $\mathbf{0}$, but we can also prepare an arbitrary classical input $\boldsymbol{x} \in \{0,1\}^n$ by reinterpreting the one-time pad key as $\boldsymbol{a} = \boldsymbol{d} \oplus \boldsymbol{x}$ so that the input state on P_{EPR}'s side is $\mathsf{X}^{\boldsymbol{a}}|\boldsymbol{x}\rangle$. In a test round, on the other hand, the input is prepared as the one-time pad of either $|0\rangle^{\otimes n}$ or $|+\rangle^{\otimes n}$. Note that as indicated in Figure 2 this choice of measurements will be made after the interaction with P_{EPR} has taken place.

The honest prover P_{EPR} applies the circuit Q, which we assume is compiled in the universal gate set $\{\mathsf{H}, \mathsf{T}, \mathsf{CNOT}\}$, to his one-time padded input. We will shortly describe gadgets that P_{EPR} can apply in order to implement each of the three gate types. The gadgets are designed in a way that in a test round each gadget amounts to an application of an identity gate; this is what enables V_{EPR} to perform certain tests in those rounds that are meant to identify deviating behavior of a dishonest prover. After each gadget, the one-time padded keys can be updated by V_{EPR}, who is able to keep track of the keys at any point in the circuit using the *update rules* in Table 2.

		Key Update Rule
T	Computation Round	$(a_j, b_j) \leftarrow (a_j + c_i, b_j + e_i + a_j + c_i + (a_j + c_i)z_i)$
	X-Test, even parity; or Z-test, odd parity	$(a_j, b_j) \leftarrow (e_i, 0)$
	Z-Test, even parity; or X-test, odd parity	$(a_j, b_j) \leftarrow (0, b_j + e_i + z_i)$
H		$(a_j, b_j) \leftarrow (b_j, a_j)$
CNOT		$(a_j, b_j, a_{j'}, b_{j'}) \leftarrow (a_j, b_j + b_{j'}, a_j + a_{j'}, b_{j'})$

Table 2: Rules for updating the one-time-pad keys after applying each type of gate in the EPR Protocol, in particular: after applying the i-th T gate to the j-th wire; applying an H gate to the j-th wire; or applying a CNOT gate controlled on the j-th wire and targeting the j'-th wire.

We now describe the three gadgets, before giving a complete description of the protocol.

CNOT Gadget To implement a CNOT gate on wires j and j', P_{EPR} simply performs the CNOT gate on those wires of his input qubits. The one-time pad keys are changed by the update rule in Table 2, because $\mathsf{CNOT} \cdot \mathsf{X}^{a_j}\mathsf{Z}^{b_j} \otimes \mathsf{X}^{a_{j'}}\mathsf{Z}^{b_{j'}} = \mathsf{X}^{a_j}\mathsf{Z}^{b_j+b_{j'}} \otimes \mathsf{X}^{a_j+a_{j'}}\mathsf{Z}^{b_{j'}} \cdot \mathsf{CNOT}$. Note that $\mathsf{CNOT}|0\rangle|0\rangle = |0\rangle|0\rangle$ and $\mathsf{CNOT}|+\rangle|+\rangle = |+\rangle|+\rangle$, so in the test runs, P_{EPR} is applying the identity.

H Gadget To implement an H gate on wire j, P_{EPR} simply performs the H on wire j, and the one-time-pad keys are changed as in Table 2. Unlike CNOT, H does not act as the identity on $|0\rangle$ and $|+\rangle$, so it is not the identity in a test round. To remedy this, assume that Q is compiled so that every H gate appears in a pattern $\mathsf{H}(\mathsf{TTH})^k$, where the maximal such k is odd. This can be accomplished by replacing each H by $\mathsf{HTTHTTHTTH}$, which implements the same unitary. In test rounds, the T gadget, described shortly, implements the identity, and since $\mathsf{H}(\mathrm{Id}\,\mathsf{H})^k$ for odd k implements the identity, $\mathsf{H}(\mathsf{TTH})^k$ will also have no effect in test rounds.

Parity of a T Gate Within a pattern $\mathsf{H}(\mathsf{TTH})^k$, the H has the effect of switching between an X-test round scenario (the state $|0\rangle$) and a Z-test round scenario (the state $|+\rangle$). In order to consistently talk about the type of a round while evaluating the circuit, we can associate a parity with each T gate in the circuit. The parity of the T gates that are not part of the pattern $\mathsf{H}(\mathsf{TTH})^k$ will be defined to be even. A H will always flip the parity, so that within such a pattern, the first two T gates will be odd, the next two will be even, etc., until the last two T gates will be odd again.

T Gadget The gadget for implementing the i-th T gate on the j-th wire is performed on P_{EPR}'s j-th input qubit, and his i-th auxiliary qubit (indexed by $n+i$), which we can think of as being prepared in a particular auxiliary state by V_{EPR} measuring her half of the corresponding EPR pair, as shown in Figure 1. The gadget depends on a random bit z_i that is chosen by V_{EPR} and sent to the prover.

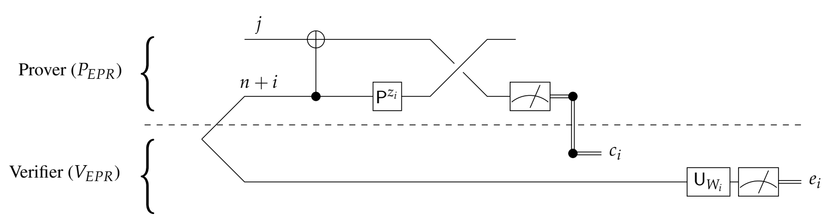


Fig. 1: The gadget for implementing the i-th T gate on the j-th wire. The gate U_{W_i} implementing the change of basis associated with observable W_i is applied as part of the procedure V^r_{EPR} (see Figure 3b) and is determined by the round type r, the parity of the i-th T gate, z_i, c_i, and a'_i (the X-key going into the i-th T gate), as in Table 3.

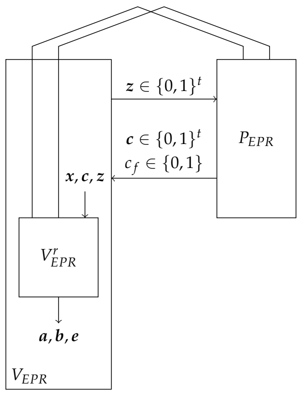


Fig. 2: This figure describes how different pieces of the protocol fit together. V_{EPR} and P_{EPR} share $n+t$ EPR pairs. The honest prover P_{EPR} can be seen as a procedure that acts on $n+t$ qubits — the EPR pair halves — depending on a t-bit string $\boldsymbol{z}$. We have separated the quantum part of V_{EPR} into its own procedure, called V^r_{EPR}, where $r \in \{0,1,2\}$ indicates the *round type*, which V_{EPR} runs on her $n+t$ EPR halves, and the $2t$ bits $\boldsymbol{c}$ and $\boldsymbol{z}$. Aside from running V^r_{EPR}, V_{EPR} is classical.

			U_{W_i} (observable W_i)
Computation Round	$a'_i \oplus c_i \oplus z_i = 0$		HT (observable G)
	$a'_i \oplus c_i \oplus z_i = 1$		HPT (observable F)
X-Test Round	even T gate		Id (observable Z)
	odd T gate	$z_i = 0$	H (observable X)
		$z_i = 1$	HP (observable Y)
Z-Test Round	odd T gate		Id (observable Z)
	even T gate	$z_i = 0$	H (observable X)
		$z_i = 1$	HP (observable Y)

Table 3: The choice of U_{W_i} in the T gadget. We also indicate the observable W_i associated with the final measurement $W_i = \mathsf{U}^\dagger_{W_i} Z \mathsf{U}_{W_i}$.

The EPR Protocol. We show how the gadgets just described are used in the complete protocol. We first describe the protocol for V_{EPR} below. For later convenience we have divided the action of V_{EPR} into classical actions and a single quantum subroutine V^r_{EPR} depending on the round type.

The procedure V^r_{EPR} measures each of the $n+t$ EPR halves according to some observable that depends on r, $\boldsymbol{c}$, and $\boldsymbol{z}$. In the case of a computation round, V^0_{EPR} measures the qubits in T adaptively. We describe the steps of V_{EPR}, V^r_{EPR} and the honest behaviour of P_{EPR} in Fig. 3.

Completeness and Soundness. We summarize the relevant part of the analysis of the EPR protocol from [Bro18]. First suppose P_{EPR} behaves honestly. If $\|\Pi_0 Q|0^n\rangle\|^2 = p$, then in a computation round, V_{EPR} outputs $\mathtt{accept}$ with probability p, whereas in a test round, V_{EPR} outputs $\mathtt{accept}$ with probability 1. This establishes completeness of the protocol:

1. V_{EPR} sends $\boldsymbol{z} \in_R \{0,1\}^t$ to P_{EPR}, and receives back $\boldsymbol{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$.
2. V_{EPR} chooses a random round type $r \in \{0,1,2\}$ and runs V^r_{EPR} (see Figure 3b) on her EPR halves, $\boldsymbol{x}$, $\boldsymbol{c}$ and $\boldsymbol{z}$, to obtain bits $\boldsymbol{a}, \boldsymbol{b} \in \{0,1\}^n$ and $\boldsymbol{e} \in \{0,1\}^t$.
3. V_{EPR} applies the update rules from Table 2 on the initial keys $(\boldsymbol{a}, \boldsymbol{b})$, gate-by-gate, to obtain, for every $i \in [t]$, the X-key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $r = 1$ (X-test round) and there exists an i such that the i-th T gate is even and $c_i \neq a'_i \oplus e_i$, output reject. If $r = 2$ (Z-test round) and there exists an i such that the i-th T gate is odd and $c_i \neq a'_i \oplus e_i$, output reject. If $r \in \{0,1\}$ (computation or X-test round) and $c_f \oplus a'_f \neq 0$, output reject. Otherwise, output accept.

(a) V_{EPR}'s point of view.

Input: A circuit Q with t T gates, $\boldsymbol{x} \in \{0,1\}^n$, $\boldsymbol{c}, \boldsymbol{z} \in \{0,1\}^t$, an n-qubit system indexed by N, and a t-qubit system indexed by T.

1. If $r \in \{0,1\}$, measure each qubit in N in the Z basis, and otherwise measure in the X basis, to get results $\boldsymbol{d} \in \{0,1\}^n$. If $r = 0$, set $(\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{d} \oplus \boldsymbol{x}, 0^n)$; if $r = 1$, set $(\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{d}, 0^n)$; and if $r = 2$ set $(\boldsymbol{a}, \boldsymbol{b}) = (0^n, \boldsymbol{d})$.
2. Going through Q gate-by-gate, use the update rules in Table 2 to update the one-time-pad keys. For every $i \in [t]$, when the i-th T gate is reached, let a'_i be the X key before the i-th T gate is applied. Choose an observable W_i according to Table 3 in which to measure the i-th qubit in T, corresponding to the i-th T gate, obtaining result e_i.

(b) The procedure V^r_{EPR}, employed by V_{EPR}.

1. Receive $\boldsymbol{z} \in \{0,1\}^t$ from V_{EPR}.
2. Evaluate Q gate-by-gate using the appropriate gadget for each gate. In particular, use z_i to implement the i-th T gadget, and obtain measurement result c_i.
3. Measure the output qubit to obtain c_f, and return $\boldsymbol{c}$ and c_f to V_{EPR}.

(c) Honest prover strategy P_{EPR}

Fig. 3: The EPR Protocol.

Theorem 2 (Completeness). *Suppose the verifier executes the EPR Protocol, choosing $r = 0$ with probability p, on an input $(Q, |\boldsymbol{x}\rangle)$ such that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \geq 1 - \delta$. Then the probability that V_{EPR} accepts when interacting with the honest prover P_{EPR} is at least $(1-p) + p(1-\delta)$.*

The following theorem is implicit in [Bro18, Section 7.6], but we include a brief proof sketch:

Theorem 3 (Soundness). *Suppose the verifier executes the EPR Protocol, choosing $r = 0$ with probability p, on an input $(Q, |\boldsymbol{x}\rangle)$ such that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \leq \delta$. Let P^*_{EPR} be an arbitrary prover such that P^*_{EPR} is accepted by V_{EPR} with probability q_t conditioned on $r \neq 0$, and q_c conditioned on $r = 0$. Then the prover's overall acceptance* *probability is* $pq_c + (1-p)q_t$*, and*

$$q_c \;\le\; 2\,(q_t\,\delta + (1-q_t)) - \delta.$$

Proof (Proof sketch). Using the notation of [Bro18], let $A = \sum_k \sum_{Q\in B'_{t,n}} |\alpha_{k,Q}|^2$. For intuition, A should be thought of as the total weight on attacks that could change the outcome of the computation, called non-benign attacks in [Bro18]. By [Bro18], the probability of rejecting in a computation round is $1-q_c \ge (1-\delta)(1-A)$, whereas the probability of rejecting in a test round is $1-q_t \;\ge\; \frac{1}{2}A$. Combining these gives $q_c \le 2(q_t\delta + (1-q_t)) - \delta$.

3 Rigidity

Each of our delegation protocols includes a *rigidity test* that is meant to verify that one of the provers measures his half of shared EPR pairs in a basis specified by the verifier, thereby preparing one of a specific family of post-measurement states on the other prover's space; the post-measurement states will form the basis for the delegated computation. This will be used to certify that one of the provers in our two-prover schemes essentially behaves as the quantum part of V_{EPR} would in the EPR protocol.

In this section we outline the structure of the test, giving the important elements for its use in our delegation protocols. We refer the reader to Section A of the supplemental material for a detailed presentation, including the soundness analysis. The test is parametrized by the number m of EPR pairs to be used. The test consists of a single round of classical interaction between the verifier and the two provers. With constant probability the verifier sends one of the provers a string W chosen uniformly at random from Σ^m where the set $\Sigma = \{X, Y, Z, F, G\}$ contains a label for each single-qubit observable to be tested. With the remaining probability, other queries, requiring the measurement of observables not in Σ^m (such as the measurement of pairs of qubits in the Bell basis), are sent.

In general, an arbitrary strategy for the provers consists of an arbitrary entangled state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ (which we take to be pure), and measurements (which we take to be projective) for each possible question.[4] This includes an m-bit outcome projective measurement $\{W^u\}_{u\in\{0,1\}^m}$ for each of the queries $W \in \Sigma^m$. Our rigidity result states that any strategy that succeeds with probability $1-\varepsilon$ in the test is within $\mathrm{poly}(\varepsilon)$ of the honest strategy, up to local isometries (see Theorem 4 for a precise statement). This is almost true, but for an irreconcilable ambiguity in the definition of the complex phase $\sqrt{-1}$. The fact that complex conjugation of observables leaves correlations invariant implies that no classical test can distinguish between the two nontrivial inequivalent irreducible representations of the Pauli group, which are given by the Pauli matrices $\sigma_X, \sigma_Y, \sigma_Z$ and their complex conjugates $\overline{\sigma_X} = \sigma_X$, $\overline{\sigma_Z} = \sigma_Z$, $\overline{\sigma_Y} = -\sigma_Y$ respectively.

[4] We make the assumption that the players employ a pure-state strategy for convenience, but it is easy to check that all proofs extend to the case of a mixed strategy. Moreover, it is always possible to consider (as we do) projective strategies only by applying Naimark's dilation theorem, and adding an auxiliary local system to each player as necessary, since no bound is assumed on the dimension of their systems.

In particular, the provers may use a strategy that uses a combination of both representations; as long as they do so consistently, no test will be able to detect this behavior.[5]. The formulation of our result accommodates this irreducible degree of freedom by forcing the provers to use a single qubit, the $(m+1)$-st, to make their choice of representation (so honest provers require the use of $(m+1)$ EPR pairs to test the operation of m-fold tensor products of observables from Σs).

Theorem 4 below summarizes the guarantees of our main test, which is denoted as $\text{RIGID}(\Sigma, m)$. Informally, Theorem 4 establishes that a strategy that succeeds in $\text{RIGID}(\Sigma, m)$ with probability at least $1-\epsilon$ must be such that (up to local unitaries):

- The players' joint state is close to a tensor product of m EPR pairs, together with an arbitrary ancilla register;
- The projective measurements performed by either player upon receipt of a query of the form $W \in \Sigma^m$ are, on average over the uniformly random choice of $W \in \Sigma^m$, close to a measurement that consists in first, measuring the ancilla register to extract a single bit that specifies whether to perform the ideal measurements or their conjugated counterparts, and second, measuring the player's m half-EPR pairs in either the bases indicated by W, or their complex conjugate, depending on the bit obtained from the ancilla register.

For an observable $W \in \Sigma$, let $\sigma_W = \sigma_W^{+1} - \sigma_W^{-1}$ be its eigendecomposition, where σ_W are the "honest" Pauli matrices defined in (1) and (2). For $u \in \{\pm 1\}$ let $\sigma_{W,+}^u = \sigma_W^u$ for $W \in \Sigma$, and

$$\sigma_{X,-}^u = \sigma_X^u, \quad \sigma_{Z,-}^u = \sigma_Z^u, \quad \sigma_{Y,-}^u = \sigma_Y^{-u}, \quad \sigma_{F,-}^u = \sigma_G^{-u}, \quad \sigma_{G,-}^u = \sigma_F^{-u} .$$

(In words, $\sigma_{W,-}^u$ is just the complex conjugate of σ_W^u.) We note that for the purpose of our delegation protocols, we made a particular choice of the set Σ. The result generalizes to any constant-sized set of single-qubit Clifford observables, yielding a test for m-fold tensor products of single-qubit Clifford observables from Σ.

Theorem 4. *Let $\varepsilon > 0$ and m an integer. Suppose a strategy for the players succeeds with probability $1-\varepsilon$ in test $\text{RIGID}(\Sigma, m)$. For $W \in \Sigma^m$ and $D \in \{A, B\}$ let $\{W_D^u\}_u$ be the measurement performed by prover D on question W. Then for $D \in \{A, B\}$ there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)_{D'}^{\otimes m} \otimes \mathcal{H}_{\hat{D}}$$

such that

$$\big\| (V_A \otimes V_B) |\psi\rangle_{AB} - |\text{EPR}\rangle^{\otimes m} \otimes |\text{AUX}\rangle_{\hat{A}\hat{B}} \big\|^2 = O(\sqrt{\varepsilon}), \tag{3}$$

[5] See [RUV12, Appendix A] for an extended discussion of this issue, with a similar resolution to ours.

and positive semidefinite matrices τ_λ *on* $\hat{\mathsf{A}}$ *with orthogonal support, for* $\lambda \in \{+,-\}$*, such that* $\mathrm{Tr}(\tau_+) + \mathrm{Tr}(\tau_-) = 1$ *and*

$$\begin{aligned}
\mathop{\mathrm{E}}_{W\in\Sigma^m} \sum_{u\in\{\pm 1\}^m} \Big\| V_A \mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_A \otimes W^u_{\mathsf{B}})|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_A \otimes W^u_{\mathsf{B}})^\dagger\big) V_A^\dagger \\
- \sum_{\lambda\in\{\pm\}} \Big(\bigotimes_{i=1}^m \frac{\sigma^{u_i}_{W_i,\lambda}}{2}\Big) \otimes \tau_\lambda \Big\|_1 \\
= O(\mathrm{poly}(\varepsilon)).
\end{aligned}$$

Moreover, players employing the honest strategy succeed with probability $1 - e^{-\Omega(m)}$ *in the test.*

The proof of the theorem is based on standard techniques developed in the literature on "rigidity theorems" for nonlocal games. We highlight two components. The first is a "conjugation test" that allows us to extend the guarantees of elementary tests based on the CHSH game or the Magic Square game, which test for Pauli σ_X and σ_Z observables, to a test for single-qubit Clifford observables — since the latter are characterized by their action on the Pauli group (see Section A.4 of the supplemental material for details). The second is an extension of the "Pauli braiding test" from [NV17] to handle tensor products of not only σ_X and σ_Z, but also σ_Y Pauli observables (see Section A.5 of the supplemental material for details). As already emphasized in the introduction, the improvements in efficiency of our scheme are partly enabled by the strong guarantees of Theorem 4, and specifically the independence of the final error dependence from the parameter m.

4 The Verifier-on-a-Leash Protocol

4.1 Protocol and statement of results

The Verifier-on-a-Leash Protocol (or "Leash Protocol" for short) involves a classical verifier and two quantum provers. The idea behind the Leash Protocol is to have a first prover, nicknamed PV for Prover V, carry out the quantum part of V_{EPR} from Broadbent's EPR Protocol by implementing the procedure V^r_{EPR}. (See Section 2.3 for a summary of the protocol and a description of V_{EPR}. Throughout this section we assume that the circuit Q provided as input is compiled in the format described in Section 2.3.). A second prover, nicknamed PP for Prover P, will play the part of the prover P_{EPR}. Unlike in the EPR Protocol, the interaction with PV (i.e. running V^r_{EPR}) will take place first, and PV will be asked to perform random measurements from the set $\Sigma = \{X, Y, Z, F, G\}$. The values z, rather than being chosen at random, will be chosen based on the corresponding choice of observable. We let n be the number of input bits and t number of T gates in Q.

The protocol is divided into two sub-games; which game is played is chosen by the verifier by flipping a biased coin with probability $(p_r, p_d = 1 - p_r)$.

- The first game is a sequential version of the rigidity game $\textsc{rigid}(\Sigma, m)$ (from Section A) described in Figure 9. This aims to enforce that PV performs precisely the right measurements;

– The second game is the delegation game, described in Figures 6, 7, and 8, and whose structure is summarized in Figure 4. Here the verifier guides PP through the computation in a similar way as in the EPR Protocol.

We call the resulting protocol the Leash Protocol with parameters (p_r, p_d). In both sub-games the parameter $m = \Theta(n+t)$ is chosen large enough so that with probability close to 1 each symbol in Σ appears in a random $W \in \Sigma^m$ at least $n+t$ times. It is important that PV is not able to tell which kind of game is being played. Notice also that in order to ensure blindness, we will require that the interaction with PV in the delegation game is sequential (more details on this are found in Section 4.4). In order for the two sub-games to be indistinguishable, we also require that the rigidity game $\text{RIGID}(\Sigma, m)$ be played sequentially (i.e. certain subsets of questions and answers are exchanged sequentially, but the acceptance condition in the test is the same). Note, importantly, that the rigidity guarantees of $\text{RIGID}(\Sigma, m)$ from Section A hold verbatim when the game is played sequentially, since this only reduces the number of ways that the provers can cheat. The following theorem states the guarantees of the Leash Protocol.

Theorem 5. *There are constants $p_r, p_d = 1 - p_r$, and $\Delta > 0$ such that the following hold of the Verifier-on-a-Leash Protocol with parameters (p_r, p_d), when executed on an input $(Q, |\boldsymbol{x}\rangle)$.*

– (Completeness:) *Suppose that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for* PV *and* PP *that is accepted with probability at least $p_{\text{compl}} = p_r(1 - e^{-\Omega(n+t)}) + 8p_d/9$.*
– (Soundness:) *Suppose that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \leq 1/3$. Then any strategy for* PV *and* PP *is accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

Further, the protocol leaks no information about $\boldsymbol{x}$ to either prover individually, aside from an upper bound on the length of $\boldsymbol{x}$.

The proof of the completeness property is given in Lemma 1. The soundness property is shown in Lemma 4. Blindness is established in Section 4.4. We first give a detailed description of the protocol. We start by describing the delegation game, specified in Figures 6, 7 and 8, which describe the protocol from the verifier's view, an honest PV's view, and an honest PP's view respectively. This will motivate the need for a sequential version of the game $\text{RIGID}(\Sigma, m)$, described in Figure 9. As we will show, the rigidity game forces PV to behave honestly. Thus, for the purpose of exposition, we assume for now that PV behaves honestly, which results in the joint behavior of PV and V being similar to that of the verifier V_{EPR} in the EPR Protocol.

From the rigidity game we may also assume that PV and PP share m EPR pairs, labeled $\{1, \ldots, m\}$, for $m = \Theta(n+t)$. We will assume that the circuit Q is broken into d layers, $Q = Q_1 \ldots Q_d$, such that in every Q_ℓ, each wire has at most one T gate applied to it, after which no other gates are applied to that wire. We will suppose the T gates are indexed from 1 to t, in order of layer.

The protocol begins with an interaction between the verifier and PV. The verifier selects a uniformly random partition $A, B_1, \ldots, B_d$ of $\{1, \ldots, m\}$, with $|A| = \Theta(n)$, and for every $\ell \in \{1, \ldots, d\}$, $|B_\ell| = \Theta(t_\ell)$, where t_ℓ is the number of T gates in

Q_ℓ. The verifier also selects a uniformly random $W \in \Sigma^m$, and partitions it into substrings W_A and $W_{B_1}, \dots, W_{B_d}$, meant to contain observables to initialize the computation qubits and auxiliary qubits for each layer of T gates respectively. The verifier instructs PV to measure his halves of the EPR pairs using the observables W_A first, and then $W_{B_1}, \dots, W_{B_d}$, sequentially. Upon being instructed to measure a set of observables, PV measures the corresponding half-EPR pairs and returns the results $\boldsymbol{e}$ to the verifier. Breaking this interaction into multiple rounds is meant to enforce that, for example, the results output by PV upon receiving W_{B_ℓ}, which we call $\boldsymbol{e}_{B_\ell}$, cannot depend on the choice of observables $W_{B_{\ell+1}}$. This is required for blindness.

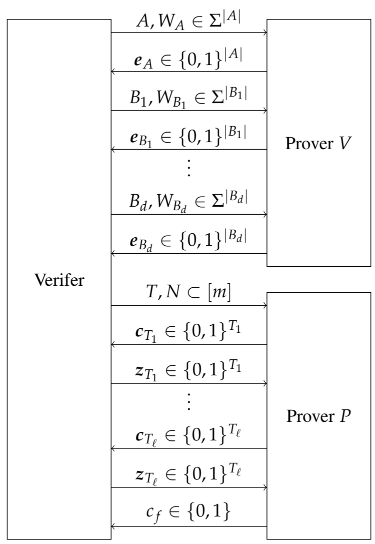


Fig. 4: Structure of the delegation game.

Once the interaction with PV has been completed, as in the EPR Protocol, V selects one of three round types: computation $(r = 0)$, X-test $(r = 1)$, and Z-test $(r = 2)$. The verifier selects a subset $N \subset A$ of size n of qubits to play the role of inputs to the computation. These are chosen from the subset of A corresponding to wires that PV has measured in the appropriate observable for the round type (see Table 4). For example, in an X-test round, PV's EPR halves corresponding to input wires should be measured in the Z basis so that PP is left with a one-time pad of the state $|0\rangle^{\otimes n}$, so in an X-test round, the computation wires are chosen from the set $\{i \in A : W_i = Z\}$. The input wires N are labeled by $\mathcal{X}_1, \dots, \mathcal{X}_n$.

The verifier also chooses subsets $T_\ell = T_\ell^0 \cup T_\ell^1 \subset B_\ell$ of sizes $t_{\ell,0}$ and $t_{\ell,1} = t_\ell - t_{\ell,0}$ respectively, where $t_{\ell,0}$ is the number of odd T gates in the ℓ-th layer of Q (recall the definition of even and odd T gates from Section 2.3). The wires T_ℓ^0 and T_ℓ^1 will play the role of auxiliary states used to perform T gates from the ℓ-th layer. They are chosen from those wires from B_ℓ whose corresponding EPR halves have been measured in a correct basis, depending on the round type. For example, in an X-test round, the auxiliaries corresponding to odd T gates should be prepared by measuring the corresponding EPR half in either the X or Y basis (see Table 3), so in an X-test round, T_ℓ^1 is chosen from $\{i \in B_\ell : W_i \in \{X, Y\}\}$ (see Table 4). We will let $\mathcal{T}_1, \dots, \mathcal{T}_t$ label those EPR pairs that will be used as auxiliary states. In particular, the system $\mathcal{T}_i$ will be used for the i-th T gate in the circuit, so if the i-th T gate is even, $\mathcal{T}_i$ should be chosen from $T^0 = \cup_\ell T_\ell^0$, and otherwise it should be chosen from $T_1 = \cup_\ell T_\ell^1$. The verifier sends labels $\mathcal{T}_1, \dots, \mathcal{T}_t$ and $\mathcal{X}_1, \dots, \mathcal{X}_n$ to PP, who will act as P_{EPR} on the $n + t$ qubits specified by these labels.

Just as in the EPR Protocol, the input on PP's system specified by $\mathcal{X}_1, \dots, \mathcal{X}_n$ is a quantum one-time pad of either $|\boldsymbol{x}\rangle$, $|0\rangle^{\otimes n}$, or $|+\rangle^{\otimes n}$, depending on the round type, with V holding the keys (determined by $\boldsymbol{e}$). Throughout the interaction, PP always maintains a one-time pad of the current state of the computation, with the verifier in possession of the one-time-pad keys. The verifier updates her keys as the computation is carried out, using the rules in Table 2.

From PP's perspective, the protocol works just as the EPR Protocol, except that he does not receive the bit z_i needed to implement the T gadget until *during* the T gadget, after he has sent V his measurement result c_i (see Figure 5).

To perform the i-th T gate on the j-th wire, PP performs the circuit shown in Figure 5. As Figure 5 shows, PV has already applied the observable specified by V to his half of the EPR pair. The T gadget requires interaction with the verifier, to compute the bit z_i, which depends on the measured c_i, the value W_i, and one-time-pad key a_j, however, this interaction can be done in parallel for T gates in the same layer.

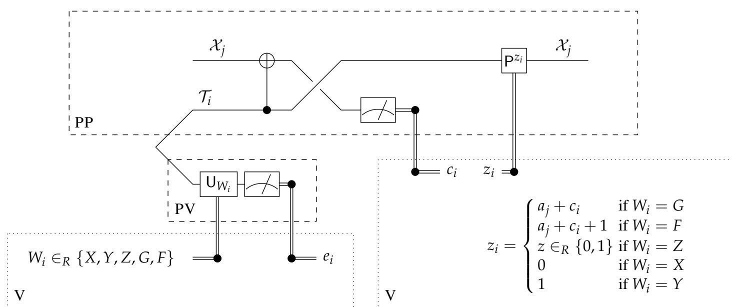


Fig. 5: The gadget for implementing the i-th T gate, on the j-th wire.

It is simple to check that the T gadget in Figure 5 is the same as the T gadget for the EPR Protocol shown in Figure 1. In the case of the leash protocol, W is chosen at random, and then z is chosen accordingly, whereas in the case of the EPR Protocol, z is chosen at random and then W is chosen accordingly.

	Computation Round	X-test Round	Z-test Round
N	$\{i \in A : W_i = Z\}$	$\{i \in A : W_i = Z\}$	$\{i \in A : W_i = X\}$
T_ℓ^0	$\{i \in B_\ell : W_i \in \{G,F\}\}$	$\{i \in B_\ell : W_i = Z\}$	$\{i \in B_\ell : W_i \in \{X,Y\}\}$
T_ℓ^1	$\{i \in B_\ell : W_i \in \{G,F\}\}$	$\{i \in B_\ell : W_i \in \{X,Y\}\}$	$\{i \in B_\ell : W_i = Z\}$

Table 4: How the verifier chooses index sets $T = T^0 \cup T^1$ and N for each type of round. These sets determine which systems are labeled by $\{\mathcal{T}_i\}_{i=1}^t$ and $\{\mathcal{X}_j\}_{j=1}^n$, respectively.

We now give the precise protocols for V (Figure 6) and honest provers PV (Figure 7) and PP (Figure 8).

Let $(Q, \boldsymbol{x})$ be the input to the verifier, where Q is compiled in the form described in Section 2.3. Let n be the size of the input to Q. Let d be the T-depth, and for $\ell \in \{1, \ldots, d\}$ let t_ℓ be the number of T gates in the ℓ-th layer.

1. The verifier selects $W \in_R \Sigma^m$. She partitions $\{1, \ldots, m\}$ arbitrarily into non-overlapping subsets A and $B_1, \ldots, B_d$ such that W_A contains at least n copies of each symbol in Σ, and for each $\ell \in \{1, \ldots, d\}$, W_{B_ℓ} contains at least t_ℓ copies of each symbol in Σ.
2. The verifier sends A, W_A to PV, who returns $\boldsymbol{e}_A \in \{0,1\}^A$. The verifier sequentially sends $(B_1, W_{B_1}), \ldots, (B_d, W_{B_d})$ to PV, each time receiving $\boldsymbol{e}_{B_\ell} \in \{0,1\}^{B_\ell}$ as answer.
3. The verifier selects a round type uniformly at random. She selects sets $N \subseteq A$ and $T_\ell \subseteq B_\ell$, for $\ell \in \{1, \ldots, d\}$, of sizes $|N| = n$ and $|T_\ell| = t_\ell$, as follows:
   Computation Round: N is chosen at random from $\{i \in A : W_i = Z\}$. T_ℓ is chosen at random from $\{i \in B_\ell : W_i \in \{G, F\}\}$. She sets $\boldsymbol{a} = \boldsymbol{e}_N + \boldsymbol{x}$ and $\boldsymbol{b} = 0^n$.
   X**-test Round:** N is chosen at random from $\{i \in A : W_i = Z\}$. $T_\ell = T_\ell^0 \cup T_\ell^1$, where T_ℓ^0 is of size $t_{\ell,0}$ chosen at random from $\{i \in B_\ell : W_i = Z\}$ and T_ℓ^1 is of size $t_{\ell,1}$ chosen at random from $\{i \in B_\ell : W_i \in \{X, Y\}\}$. She sets $\boldsymbol{a} = \boldsymbol{e}_N$ and $\boldsymbol{b} = 0^n$.
   Z**-test Round:** N is chosen at random from $\{i \in A : W_i = X\}$. $T_\ell = T_\ell^0 \cup T_\ell^1$, where T_ℓ^0 is of size $t_{\ell,0}$ chosen at random from $\{i \in B_\ell : W_i \in \{X, Y\}\}$ and T_ℓ^1 is of size $t_{\ell,1}$ chosen at random from $\{i \in B_\ell : W_i = Z\}$. She sets $\boldsymbol{a} = 0^n$ and $\boldsymbol{b} = \boldsymbol{e}_N$.
   The verifier sends the sets N and T_ℓ^0, T_ℓ^1, for all $\ell \in \{1, \ldots, d\}$, to PP.
4. For $\ell = 1, \ldots, d$,
   (a) For each Clifford gate in the ℓ-th layer, perform the appropriate key update (Table 2).
   (b) The verifier receives $\boldsymbol{c} = \{c_i\}_{i \in T_\ell}$ from PP. If it's an X-test round and $i \in T_\ell^0$, or it's a Z-test round and $i \in T_\ell^1$, reject if $c_i \neq a_j + e_i$, where j is the wire to which the i-th T gate is applied.
   (c) For each $i \in T_\ell$, the verifier computes $\boldsymbol{z} = \{z_i\}_{i \in T_\ell}$ as follows:
   Computation Round $z_i = a_j + 1_{W_i = F} + c_i$;
   X**-test Round** if $i \in T_\ell^0$, $z_i \in_R \{0,1\}$; else if $i \in T_\ell^1$, $z_i = 1_{W_i = Y}$;
   Z**-test Round** if $i \in T_\ell^0$, $z_i = 1_{W_i = Y}$; else if $i \in T_\ell^1$, $z_i \in_R \{0,1\}$.
   (d) The verifier sends $\boldsymbol{z}$ to PP and updates keys for each T gate applied (Table 2).
5. The verifier receives a bit c_f from PP. She outputs reject if it's a computation or X-test round and $c_f + a_f \neq 0$, where a_f is the final X-key on the output wire; and accept otherwise.

Fig. 6: The Delegation Game: Verifier's point of view.

1. For $\ell = 0, 1, \ldots, d$,
   (a) PV receives a string $W_S \in \Sigma^S$, for some subset S of $\{1, \ldots, m\}$, from V.
   (b) For $i \in S$, PV measures his half of the i-th EPR pair using the observable indicated by W_i, obtaining an outcome $e_i \in \{0,1\}$.
   (c) PV returns $\boldsymbol{e}_S$ to V.

Fig. 7: Honest strategy for PV

1. PP receives subsets N and T_ℓ^0, T_ℓ^1 of $\{1,\ldots,m\}$, for $\ell \in \{1,\ldots,d\}$, from the verifier.
2. For $\ell = 1,\ldots,d$,
   (a) PP does the Clifford computations in the ℓ-th layer.
   (b) For each $i \in T_\ell = T_\ell^0 \cup T_\ell^1$, PP applies a CNOT from $\mathcal{T}_i$ into the input register corresponding to the wire on which this T gate should be performed, $\mathcal{X}_j$, and measures this wire to get a value c_i. The register $\mathcal{T}_i$ is relabeled $\mathcal{X}_j$. He sends $\boldsymbol{c}_{T_\ell} = \{c_i\}_{i\in T_\ell}$ to V.
   (c) PP receives $\boldsymbol{z}_{T_\ell} = \{z_i\}_{i\in T_\ell}$ from V. For each $i \in T_\ell$, he applies P^{z_i} to the corresponding $\mathcal{X}_j$.
3. PP performs the final computations that occur after the d-th layer of T gates, measures the output qubit, $\mathcal{X}_1$, and sends the resulting bit, c_f, to V.

Fig. 8: Honest strategy for PP

Finally, we describe the sequential version of the game $\textsc{rigid}(\Sigma, m)$ in Figure 9. It is no different than $\textsc{rigid}(\Sigma, m)$, except for the fact that certain subsets of questions and answers are exchanged sequentially, but the acceptance condition is the same. As mentioned earlier, running the game sequentially only reduces the provers' ability to cheat. Hence the guarantees from $\textsc{rigid}(\Sigma, m)$ hold verbatim for the sequential version.

Let m, n, and $t_1,\ldots,t_d$ be parameters provided as input, such that $m = \Theta(n + t_1 + \cdots + t_d)$.

1. The verifier selects questions $W, W' \in \Sigma^m$, for the first and second player respectively, according to the distribution of questions in the game $\textsc{rigid}(\Sigma, m)$. She partitions $\{1,\ldots,m\}$ at random into subsets A and B_ℓ, for $\ell \in \{1,\ldots,d\}$, of size $|A| = \Theta(n)$ and $|B_\ell| = \Theta(t_\ell)$, exactly as in Step 1 of the Delegation Game.
2. The verifier sends $(A, W_A), (B_1, W_{B_1}), .., (B_d, W_{B_d})$ and $(A, W'_A), (B_1, W'_{B_1}), .., (B_d, W'_{B_d})$ in sequence to the first and second prover respectively. They sequentially return respectively $\boldsymbol{e}_A \in \{0,1\}^{|A|}$, $\boldsymbol{e}_{B_1} \in \{0,1\}^{|B_1|}, .., \boldsymbol{e}_{B_d} \in \{0,1\}^{|B_d|}$ and $\boldsymbol{e}'_A \in \{0,1\}^{|A|}$, $\boldsymbol{e}'_{B_1} \in \{0,1\}^{|B_1|}, .., \boldsymbol{e}'_{B_d} \in \{0,1\}^{|B_d|}$.
3. The verifier accepts if and only if $\boldsymbol{e}, \boldsymbol{e}'$ and W, W' satisfy the winning condition of $\textsc{rigid}(\Sigma, m)$.

Fig. 9: Sequential version of $\textsc{rigid}(\Sigma, m)$.

4.2 Completeness

Lemma 1. *Suppose the verifier executes the rigidity game with probability p_r and the delegation game with probability $p_d = 1 - p_r$, on an input $(Q, |\boldsymbol{x}\rangle)$ such that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for the provers which is accepted with probability at least $p_{\text{compl}} = p_r(1 - e^{-\Omega(n+t)}) + \frac{8}{9}p_d$.*

Proof. The provers PV and PP play the rigidity game according to the honest strategy, and the delegation game as described in Figures 7 and 8 respectively. Their success probability in the delegation game is the same as the honest strategy in the EPR Protocol, which is at least $\frac{2}{3} + \frac{2}{3}\frac{1}{3} = \frac{8}{9}$, by Theorem 2 and since in our protocol the verifier chooses each of the three types of rounds uniformly.

4.3 Soundness

We divide the soundness analysis into three parts. First we analyze the case of an honest PV, and a cheating PP (Lemma 2). Then we show that if PV and PP pass the rigidity game with almost optimal probability, then one can construct new provers PV$'$ and PP$'$, with PV$'$ honest, such that the probability that they are accepted in the delegation game is not changed by much (Lemma 3). In Lemma 4, we combine the previous to derive the desired constant soundness-completeness gap, where we exclude that the acceptance probability of the provers in the rigidity game is too low by picking a p_r large enough.

Lemma 2 (Soundness against PP). *Suppose the verifier executes the delegation game on input $(Q, |x\rangle)$ such that $\|\Pi_0 Q|x\rangle\|^2 \leq 1/3$ with provers $(\mathrm{PV}, \mathrm{PP}^*)$ such that* PV *plays the honest strategy. Then the verifier accepts with probability at most $7/9$.*

Proof. Let PP* be any prover. Assume that PV behaves honestly and applies the measurements specified by his query W on halves of EPR pairs shared with PP*. As a result the corresponding half-EPR pair at PP* is projected onto the post-measurement state associated with the outcome reported by PV to V.

From PP*, we define another prover, P^*, such that if P^* interacts with V_{EPR}, the honest verifer for the EPR Protocol (Figure 3a), then V_{EPR} rejects with the same probability that V would reject on interaction with PP*. The main idea of the proof can be seen by looking at Figure 5, and noticing that: (1) the combined action of V and PV is unchanged if instead of choosing the W_i-values at random and then choosing z_i as a function of these, the z_i are chosen uniformly at random, and then the W_i are chosen as a function of these; and (2) with this transformation, the combined action of V and PV is now the same as the action of V_{EPR} in the EPR Protocol.

We now define P^*. P^* acts on a system that includes $n + t$ qubits that, in an honest run of the EPR Protocol, are halves of EPR pairs shared with V_{EPR}. P^* receives $\{z_i\}_{i=1}^t$ from V_{EPR}. P^* creates $m - (n + t)$ half EPR pairs (i.e. single-qubit maximally mixed states) and randomly permutes these with his $n + t$ unmeasured qubits, n of which correspond to computation qubits on systems $\mathcal{X}_1, \ldots, \mathcal{X}_n$ — he sets N to be the indices of these qubits — and t of which correspond to T-auxiliary states — he sets T^0 and T^1 to be the indices of these qubits. P^* simulates PP* on these m qubits in the following way. First, P^* gives PP* the index sets N, T^0, and T^1. In the ℓ-th iteration of the loop (Step 2. in Figure 8), PP* returns some bits $\{c_i\}_{i \in T_\ell}$, and then expects inputs $\{z_i\}_{i \in T_\ell}$, which P^* provides, using the bits he received from V_{EPR}. Finally, at the end of the computation, PP* returns a bit c_f, and P^* outputs $\{c_i\}_{i \in T}$ and c_f.

This completes the description of P^*. To show the lemma we argue that for any input $(Q, |x\rangle)$ the probability that V outputs accept on interaction with PV and PP* is the same as the probability that V_{EPR} outputs accept on interaction with P^*, which is at most $\frac{2}{3}q_t + \frac{1}{3}q_c$ whenever $\|\Pi_0 Q|x\rangle\|^2 \leq 1/3$, by Theorem 3. Using $\delta = \frac{1}{3}$, Theorem

3 gives $q_c \leq \frac{5}{3} - \frac{4}{3}q_t$, which yields

$$\frac{2}{3}q_t + \frac{1}{3}q_c \leq \frac{5}{9} + \frac{2}{9}q_t \leq \frac{7}{9}.$$

There are two reasons that V_{EPR} might reject: (1) in a computation or X-test round, the output qubit decodes to 1; or (2) in an evaluation of the gadget in Figure 5 (either an X-test round for an even T gate, or a Z-test round for an odd T gate) the condition $c_i = a_j \oplus e_i$ fails.

We first consider case (1). This occurs exactly when $c_f \oplus a_f = 1$, where a_f is the final X key of the output wire, held by V_{EPR}. We note that a_f is exactly the final X key that V would hold in the Verifier-on-a-Leash Protocol, which follows from the fact that the update rules in both the EPR Protocol and the leash protocol are the same. Thus, the probability that V_{EPR} finds $v_f \oplus a_f = 1$ on interaction with P^* is exactly the probability that V finds $c_f \oplus a_f = 1$ in Step 5 of Figure 6.

Next, consider case (2). The condition $c_i \neq a_j \oplus e_i$ is exactly the condition in which a verifier interacting with P^* as in Figure 6 would reject (see Step 4.(b)).

Thus, the probability that V_{EPR} outputs reject upon interaction with P^* is exactly the probability that V outputs reject on interaction with PP^*, which, as discussed above, is at most $7/9$.

The following lemma shows soundness against cheating PV^*.

Lemma 3. *Suppose the verifier executes the leash protocol on input $(Q, |x\rangle)$ such that $\|\Pi_0 Q|x\rangle\|^2 \leq 1/3$ with provers $(\mathrm{PV}^*, \mathrm{PP}^*)$, such that the provers are accepted with probability $1-\varepsilon$, for some $\varepsilon > 0$, in the rigidity game, and with probability at least q in the delegation game. Then there exist provers PP' and PV' such that PV' applies the honest strategy and PP' and PV' are accepted with probability at least $q - \mathrm{poly}(\varepsilon)$ in the delegation game.*

Proof. By assumption, PP^* and PV^* are accepted in the rigidity game with probability at least $1-\varepsilon$. Let V_A, V_B be the local isometries guaranteed to exist by Theorem 4, and $\{\tau_\lambda\}$ the sub-normalized densities associated with PP^*'s Hilbert space (recall that playing the rigidity game sequentially leaves the guarantees from Theorem 4 unchanged, since it only reduces the provers' ability to cheat).

First define provers PV'' and PP'' as follows. PP'' and PV'' initially share the state

$$|\psi'\rangle_{\mathsf{AB}} = \otimes_{i=1}^{m} |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{AB}} \otimes \sum_{\lambda\in\{\pm\}} |\lambda\rangle\langle\lambda|_{\mathsf{A}'} \otimes |\lambda\rangle\langle\lambda|_{\mathsf{B}'} \otimes (\tau_\lambda)_{\mathsf{A}''} ,$$

with registers $\mathsf{AA'A''}$ in the possession of PP'' and $\mathsf{BB'}$ in the possession of PV''. Upon receiving a query $W \in \Sigma^m$, PV'' measures B' to obtain a $\lambda \in \{\pm\}$. If $\lambda = +$ he proceeds honestly, measuring his half-EPR pairs exactly as instructed. If $\lambda = -$ he proceeds honestly except that for every honest single-qubit observable specified by W, he instead measures the complex conjugate observable. Note that this strategy can be implemented irrespective of whether W is given at once, as in the game RIGID, or sequentially, as in the Delegation Game. PP'' simply acts like PP^*, just with the isometry V_A applied.

First note that by Theorem 4, the distribution of answers of PV'' to the verifier, as well as the subsequent interaction between the verifier and PP, generate (classical) transcripts that are within statistical distance $\mathrm{poly}(\varepsilon)$ from those generated by PV^* and PP^* with the same verifier.

Next we observe that taking the complex conjugate of both provers' actions does not change their acceptance probability in the delegation game, since the interaction with the verifier is completely classical. Define PP' as follows: PP' measures A' to obtain the same λ as PV'', and then executes PP'' or its complex conjugate depending on the value of λ. Define PV' to execute the honest behavior (he measures to obtain λ, but then discards it and does not take any complex conjugates).

Then PV' applies the honest strategy, and $(\mathrm{PV}', \mathrm{PP}')$ applies either the same strategy as $(\mathrm{PV}'', \mathrm{PP}'')$ (if $\lambda = +$) or its complex conjugate (if $\lambda = -$). Therefore they are accepted in the delegation game with exactly the same probability.

Combining Lemma 2 and Lemma 3 gives us the final soundness guarantee.

Lemma 4. *(Constant soundness-completeness gap) There exist constants $p_r, p_d = 1 - p_r$ and $\Delta > 0$ such that if the verifier executes the leash protocol with parameters (p_r, p_d) on input $(Q, |x\rangle)$ such that $\|\Pi_0 Q|x\rangle\|^2 \leq 1/3$, any provers $(\mathrm{PV}^*, \mathrm{PP}^*)$ are accepted with probability at most $p_{\mathrm{sound}} = p_{\mathrm{compl}} - \Delta$.*

Proof. Suppose provers PP^* and PV^* succeed in the delegation game with probability $\frac{7}{9} + w$ for some $w > 0$, and the testing game with probability $1 - \varepsilon_*(w)$, where $\varepsilon_*(w)$ will be specified below. By Lemma 3, this implies that there exist provers PP' and PV' such that PV' is honest and the provers succeed in the delegation game with probability at least $\frac{7}{9} + w - g(\varepsilon_*(w))$, where $g(\varepsilon) = \mathrm{poly}(\varepsilon)$ is the function from the guarantee of Lemma 3. Let $\varepsilon_*(w)$ be such that $g(\varepsilon_*(w)) \leq \frac{w}{2}$. In particular, $\frac{7}{9} + w - g(\varepsilon_*(w)) \geq \frac{7}{9} + \frac{w}{2} > \frac{7}{9}$. This contradicts Lemma 2.

Thus if provers PP and PV succeed in the delegation game with probability $\frac{7}{9} + w$ they must succeed in the rigidity game with probability less than $1 - \varepsilon_*(w)$. This implies that for any strategy of the provers, on any *no* instance, the probability that they are accepted is at most

$$\max\left\{p_r + (1 - p_r)\Big(\frac{7}{9} + \frac{1}{18}\Big),\ p_r\Big(1 - \varepsilon_*\Big(\frac{1}{18}\Big)\Big) + (1 - p_r) \cdot 1\right\}. \tag{4}$$

Since $\varepsilon_*(\frac{1}{18})$ is a positive constant, it is clear that one can pick p_r large enough so that

$$p_r\Big(1 - \varepsilon_*\Big(\frac{1}{18}\Big)\Big) + (1 - p_r) \cdot 1 < p_r + (1 - p_r)\Big(\frac{7}{9} + \frac{1}{18}\Big). \tag{5}$$

Select the smallest such p_r. Then the probability that the two provers are accepted is at most

$$p_{\mathrm{sound}} := p_r + (1 - p_r)\Big(\frac{7}{9} + \frac{1}{18}\Big) < p_r\big(1 - e^{-\Omega(n+t)}\big) + (1 - p_r)\frac{8}{9} = p_{\mathrm{compl}}\,,$$

which gives the desired constant completeness-soundness gap Δ.

4.4 Blindness

We now establish blindness of the Leash Protocol. In Lemma 5, we will prove that the protocol has the property that neither prover can learn anything about the input to the circuit, x, aside from its length. Thus, the protocol can be turned into a blind protocol, where Q is also hidden, by modifying any input (Q, x) where Q has g gates and acts on n qubits, to an input $(U_{g,n}, (Q, x))$, where $U_{g,n}$ is a universal circuit that takes as input a description of a g-gate circuit Q on n qubits, and a string x, and outputs $Q|x\rangle$. The universal circuit $U_{g,n}$ can be implemented in $O(g \log n)$ gates. By Lemma 5, running the Leash Protocol on $(U_{g,n}, (Q, x))$ reveals nothing about Q or x aside from g and n.

In the form presented in Figure 6, the verifier V interacts first with PV, sending him random questions that are independent from the input x, aside from the input length n. It is thus clear that the protocol is blind with respect to PV.

In contrast, the questions to PP depend on PV's answers and on the input, so it may a priori seem like the questions can leak information to PP. To show that the protocol is also blind with respect to PP, we show that there is an alternative formulation, in which the verifier first interacts with PP, sending him random messages, and then only with PV, with whom the interaction is now adaptive. We argue that, for an arbitrary strategy of the provers, the reduced state of all registers available to either prover, PP or PV, is exactly the same in both formulations of the protocol — the *original* and the *alternative* one. This establishes blindness for both provers. This technique for proving blindness is already used in [RUV13] to establish blindness of a two-prover protocol based on computation by teleportation.

Lemma 5 (Blindness of the Leash Protocol). *For any strategy of* PV^* *and* PP^**, the reduced state of* PV^* *(resp.* PP^**) at the end of the leash protocol is independent of the input* x*, aside from its length.*

Proof. Let PV^* and PP^* denote two arbitrary strategies for the provers in the leash protocol. Each of these strategies can be modeled as a super-operator

$$\mathcal{T}_{\mathrm{PV}} : \mathrm{L}(\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}) \to \mathrm{L}(\mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}),$$

$$\mathcal{T}_{\mathrm{PP},ad} : \mathrm{L}(\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{PP}}) \to \mathrm{L}(\mathcal{H}_{T'_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{PP}}).$$

Here $\mathcal{H}_{T_{\mathrm{PV}}}$ and $\mathcal{H}_{T'_{\mathrm{PV}}}$ (resp. $\mathcal{H}_{T_{\mathrm{PP}}}$ and $\mathcal{H}_{T'_{\mathrm{PP}}}$) are classical registers containing the inputs and outputs to and from PV^* (resp. PP^*), and $\mathcal{H}_{\mathrm{PV}}$ (resp. $\mathcal{H}_{\mathrm{PP}}$) is the private space of PV^* (resp. PP^*). Note that the interaction of each prover with the verifier is sequential, and we use $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$ to denote the combined action of the prover and the verifier across all rounds of interaction (formally these are sequences of superoperators).

Consider an alternative protocol, which proceeds as follows. The verifier first interacts with PP. From Figure 8 we see that the inputs required for PP are subsets N and $T_1, \ldots, T_d$, and values $\{z_i\}_{i \in T_\ell}$ for each $\ell \in \{1, \ldots, d\}$. To select the former, the verifier proceeds as in the first step of the Delegation Game. She selects the latter uniformly at random. The verifier collects values $\{c_i\}_{i \in T_\ell}$ from PP exactly as in the original Delegation Game.

Once the interaction with PP has been completed, the verifier interacts with PV. First, she selects a random string $W_N \in \Sigma^N$, conditioned on the event that W_N contains at least n copies of each symbol in Σ, and sends it to PV, collecting answers $\boldsymbol{e}_N$. The verifier then follows the same update rules as in the delegation game. We describe this explicitly for computation rounds. First, the verifier sets $\boldsymbol{a} = \boldsymbol{e}_N$. Depending on the values $\{c_i\}_{i\in T_1}$ and $\{z_i\}_{i\in T_1}$ obtained in the interaction with PP, using the equation $z_i = a_j + 1_{W_i=F} + c_i$ she deduces a value for $1_{W_i=F}$ for each $i \in T_1 \subseteq B_1$. She then selects a uniformly random $W_{B_1} \in \Sigma^{B_1}$, conditioned on the event that W_{B_1} contains at least t_1 copies of each symbol from Σ, and for $i \in T_1$ it holds that $W_i = F$ if and only if $z_i = a_j + 1 + c_i$. The important observation is that, if T_1 is a uniformly random, unknown subset, the marginal distribution on W_{B_1} induced by the distribution described above is independent of whether $z_i = a_j + 1 + c_i$ or $z_i = a_j + 0 + c_i$: precisely, it is uniform conditioned on the event that W_{B_1} contains at least t_1 copies of each symbol from Σ. The verifier receives outcomes $\boldsymbol{e}_{B_1} \in \{0,1\}^{B_1}$ from PV, and using these outcomes performs the appropriate key update rules; she then proceeds to the second layer of the circuit, until the end of the computation. Finally, the verifier accepts using the same rule as in the last step of the original delegation game.

We claim that both the original and alternative protocols generate the same joint final state:

$$\mathcal{T}_{\mathrm{PP},ad} \circ \mathcal{T}_{\mathrm{PV}}(\rho_{orig}) = \mathcal{T}_{\mathrm{PV},ad} \circ \mathcal{T}_{\mathrm{PP}}(\rho_{alt}) \in \mathcal{H}_{\mathrm{PP}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{V}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}, \quad (6)$$

where we use ρ_{orig} and ρ_{alt} to denote the joint initial state of the provers, as well as the verifier's initialization of her workspace, in the original and alternative protocols respectively, and $\mathcal{T}_{\mathrm{PV},ad}$ and $\mathcal{T}_{\mathrm{PP}}$ are the equivalent of $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$ for the reversed protocol (in particular they correspond to the same strategies PV* and PP* used to define $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$). Notice that $\mathcal{T}_{\mathrm{PV},ad}$ and $\mathcal{T}_{\mathrm{PP}}$ are well-defined since neither prover can distinguish an execution of the original from the alternative protocol.[6] To see that equality holds in (6), it is possible to re-write the final state of the protocol as the result of the following sequence of operations. First, the verifier initializes the message registers with PP* and PV* using half-EPR pairs, keeping the other halves in her private workspace. This simulates the generation of uniform random messages to both provers. Then, the superoperator $\mathcal{T}_{\mathrm{PV}} \otimes \mathcal{T}_{\mathrm{PP}}$ is executed. Finally, the verifier post-selects by applying a projection operator on $\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$ that projects onto valid transcripts for the original protocol (i.e. transcripts in which the adaptive questions are chosen correctly). This projection can be implemented in two equivalent ways: either the verifier first measures $\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}}$, and then $\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$; based on the outcomes she accepts a valid transcript for the original protocol or she rejects. Or, she first measures $\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$, and then $\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}}$; based on the outcomes she accepts a valid transcript for the alternative protocol or she rejects. Using the commutation of the provers' actions, conditioned on the transcript being accepted, the first gives rise to the first final state in (6), and the second to the second final state. The two are equivalent because the acceptance condition for a valid transcript is identical in the two versions of the protocol.

[6] One must ensure that a prover does not realize if the alternative protocol is executed instead of the original; this is easily enforced by only interacting with any of the provers at specific, publicly decided times.

Since in the first case the reduced state on $\mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}$ is independent of the input to the computation, x, and in the second the reduced state on $\mathcal{H}_{\mathrm{PP}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$ is independent of x, we deduce that the protocol hides the input from each of PV* and PP*.

Remark 1. In order to make a fair comparison between previous delegated computation protocols and ours (see Figure 1), one must analyze their resource requirements under the condition that they produce the correct outcome of the computation with a fixed, let us say 99%, probability. For most protocols, this is achieved by sequentially repeating the original version, in order to amplify the completeness-soundness gap. We present in Section C of supplemental material, a sequencial procedure that allows the verifier to obtain the correct output with a fixed probability (or abort whenever the provers are malicious).

5 Dog-Walker protocol

The Dog-Walker Protocol again involves a classical verifier V and two provers PV and PP. As in the leash protocol presented in Section 4, PP and PV take the roles of P_{EPR} and V_{EPR} from [Bro18] respectively. The main difference is that the Dog-Walker Protocol gives up blindness in order to reduce the number of rounds to two (one round of interaction with each prover, played sequentially). After one round of communication with PP, who returns a sequence of measurement outcomes, V communicates all of PP's outcomes, except for the one corresponding to the output bit of the computation, as well as the input x, to PV. With these, PV can perform the required adaptive measurements without the need to interact with V. It may seem risky to communicate bits sent by PP directly to PV — this seems to allow for communication between the two provers! Indeed, blindness is lost. However, if PP is honest, his outcomes $\{c_i\}_i$ in the computation round are the result of measurements he performs on half-EPR pairs, and are uniform random bits. If he is dishonest, and does not return the outcomes obtained by performing the right measurements, he will be caught in the test rounds. It is only in computation rounds that V sends the measurement results $\{c_i\}_i$ to PV.

We notice that PV has a much more important role in this protocol: he decides himself the measurements to perform according to previous measurements' outcomes as well as the input x. For this reason, we must augment the test discussed in Section 3 in order to test if PV remains honest with respect to these new tasks. For this reason, we introduce the Tomography test and prove a rigidity theorem that will allow us to prove the soundness of the Dog-walker protocol (see Figure 10 for a glimpse of the proof structure). Due to space limitations we present the Tomography Test in Section A.8 of the supplemental material, and in Section B we describe the Dog-walker protocol formally and prove its correctness.

Finally, the Dog-Walker Protocol can be easily extended to a classical-verifier two-prover protocol for all languages in QMA. Along the same lines of the proof that QMIP = MIP* from [RUV13], one of the provers plays the role of PP, running the QMA verification circuit, while the second prover creates and teleports the corresponding QMA witness. In our case, it is not hard to see that the second prover can be re-used as PV in the Dog-Walker Protocol, creating the necessary gadgets for the computation and

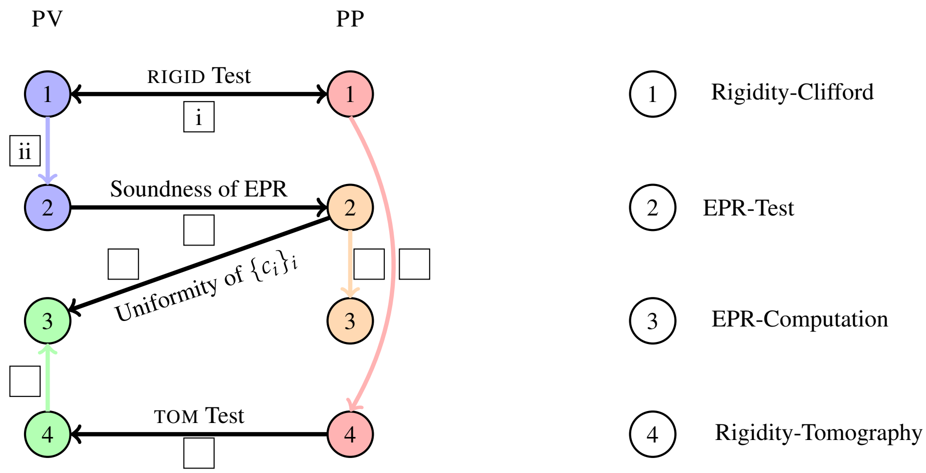


Fig. 10: Overview of the soundness of the Dog-Walker Protocol

allowing the Verifier to check the operations performed by the first prover. We describe this approach in more details in Section B.4 of the supplemental material.

References

AAV13. Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *SIGACT News*, (2):47–79, 2013.

ABE10. Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. In *Proceedings of the first Symposium on Innovations in Computer Science (ICS 2010)*, pages 453–469, 2010.

ADSS17. Gorjan Alagic, Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum fully homomorphic encryption with verification. *arXiv preprint arXiv:1708.09156*, 2017.

Bel64. John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

Bro18. Anne Broadbent. How to verify a quantum computation. *Theory of Computing*, 14(11):1–37, 2018. arXiv preprint `arXiv:1509.09180`.

BvCA18. Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Self-testing of Pauli observables for device-independent entanglement certification, 2018. arXiv:1801.10446.

Cas17. Davide Castelvecchi. IBM's quantum cloud computer goes commercial. *Nature News*, 543(7644), 6 March 2017.

CHSH69. John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

DSS16. Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum homomorphic encryption for polynomial-sized circuits. In *Advances in Cryptology – Proceedings of the 36th Annual International Cryptology Conference (CRYPTO 2016)*, pages 3–32, 2016. arXiv:1603.09717.

FH15. Joseph F. Fitzsimons and Michal Hajdušek. Post hoc verification of quantum computation, 2015. arXiv preprint `arXiv:1512.04375`.

FH17. Keisuke Fujii and Masahito Hayashi. Verifiable fault tolerance in measurement-based quantum computation. *Physical Review A*, 96:030301, Sep 2017.

Fit16. Joseph F. Fitzsimons. Private quantum computation: An introduction to blind quantum computing and related protocols, 2016. arXiv preprint `arXiv:1611.10107`.

FK17. Joseph F. Fitzsimons and Elham Kashefi. Unconditionally verifiable blind quantum computation. *Physical Review A*, 96(012303), 2017. arXiv preprint `arXiv:1203.5217`.

FV15. Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local Hamiltonian problem. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science (ITCS 2015)*, pages 103–112, 2015.

GH15. W. T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups, 2015. arXiv preprint `arXiv:1510.04085`.

GKW15. Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17, 2015.

Gri17. Alex B. Grilo. Relativistic verifiable delegation of quantum computation, 2017. arXiv preprint arXiv:1711.09585.

HH16. Masahito Hayashi and Michal Hajdušek. Self-guaranteed measurement-based quantum computation, 2016. arXiv preprint `arXiv:1603.02195`.

HM15. Masahito Hayashi and Tomoyuki Morimae. Verifiable measurement-only blind quantum computing with stabilizer testing. *Physical Review Letters*, 115:220502, Nov 2015.

HPDF15. Michal Hajdušek, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. Device-independent verifiable blind quantum computation, 2015. arXiv preprint `arXiv:1502.02563`.

HZM$^+$17. He-Liang Huang, Qi Zhao, Xiongfeng Ma, Chang Liu, Zu-En Su, Xi-Lin Wang, Li Li, Nai-Le Liu, Barry C. Sanders, Chao-Yang Lu, and Jian-Wei Pan. Experimental Blind Quantum Computing for a Classical Client. *Physical Review Letters*, 119:050503, Aug 2017.

Ji16. Zhengfeng Ji. Classical verification of quantum proofs. In *Proceedings of the Forty-eighth Annual ACM SIGACT Symposium on Theory of Computing (STOC 2016)*, pages 885–898, 2016.

Mah17. Urmila Mahadev. Classical homomorphic encryption for quantum circuits. *arXiv preprint arXiv:1708.02130*, 2017.

Mah18. Urmila Mahadev. Classical verification of quantum computations. *arXiv preprint arXiv:1804.01082*, 2018.

McK16. Matthew McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016. arXiv preprint `arXiv:1309.5675`.

Mer90. N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65:3373–3376, 1990.

MF16. Tomoyuki Morimae and Joseph F. Fitzsimons. Post hoc verification with a single prover, 2016. arXiv preprint `arXiv:1603.06046`.

Mon16. Ashely Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(15023), 2016.

Mor14. Tomoyuki Morimae. Verification for measurement-only blind quantum computing. *Physical Review A*, 89, 2014.

MTH17. Tomoyuki Morimae, Yuki Takeuchi, and Masahito Hayashi. Verified measurement-based quantum computing with hypergraph states, 2017. arXiv:1701.05688.

MY04. Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4:273–286, 2004.

NV17. Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the Forty-ninth Annual ACM SIGACT Symposium on Theory of Computing (STOC 2017)*, pages 1003–1015, 2017.

RUV12. Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games, 2012. arXiv preprint `arXiv:1209.0448`.

RUV13. Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496:456–460, 2013. Full version `arXiv:1209.0448`.

Slo16. William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games, 2016. arXiv preprint `arXiv:1606.03140`.

Vid17. Thomas Vidick. The Pauli braiding test. Available at https://mycqstate.wordpress.com/2017/06/28/pauli-braiding/, 2017.

WBMS16. Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93:062121, 2016.

Supplemental material

A Rigidity

The goal of this section is proving the Rigidity theorems used in our delegation protocols. We start by introducing the language required to formulate our testing results in Section A.1. We then present a series of elementary tests, for commutation, anti-commutation, etc., that are presented in Sections A.2 and A.3. We follow by giving a test for the conjugation of one observable to another by a unitary, the Conjugation Test, in Section A.4. In Section A.5, we apply the Conjugation Test to test the relations that dictate how an arbitrary m-qubit Clifford unitary acts by conjugation on the Pauli matrices. In Section A.6 we specialize the test to the case of unitaries that can be expressed as the m-fold tensor product of Clifford observables taken from the set Σ. In Sections A.7 and A.8, we decribe variants of the test from Section A.6, which are later employed in the Leash and Dog-Walker protocols.

A.1 Testing

In this section we recall the standard formalisms from self-testing, including state-dependent distance measure, local isometries, etc. We also introduce a framework of "tests for relations" that will be convenient to formulate our results.

Distance measures. Ultimately our goal is to test that a player implements a certain tensor product of single-qubit or two-qubit measurements defined by observables such as σ_X, σ_Y, or σ_G. Since it is impossible to detect whether a player applies a certain operation X on state $|\psi\rangle$, or $VXV^\dagger$ on state $V|\psi\rangle$, for any isometry $V : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ such that $V^\dagger V = \mathrm{Id}$, we will (as is standard in testing) focus on testing identity up to *local isometries*. Towards this, we introduce the following important piece of notation:

Definition 1. *For finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_{A'}$, $\delta > 0$, and operators $R \in \mathrm{L}(\mathcal{H}_A)$ and $S \in \mathrm{L}(\mathcal{H}_{A'})$ we say that R and S are δ-isometric with respect to $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and write $R \simeq_\delta S$, if there exists an isometry $V : \mathcal{H}_A \to \mathcal{H}_{A'}$ such that*

$$\left\|(R - V^\dagger S V) \otimes \mathrm{Id}_B |\psi\rangle\right\|^2 = O(\delta).$$

If V is the identity, then we further say that R and S are δ-equivalent, and write $R \approx_\delta S$ for $\|(R-S)\otimes \mathrm{Id}_B|\psi\rangle\|^2 = O(\delta)$.

The notation $R \simeq_\delta S$ carries some ambiguity, as it does not specify the state $|\psi\rangle$. The latter should always be clear from context: we will often simply write that R and S are δ-isometric, without explicitly specifying $|\psi\rangle$ or the isometry. The relation is transitive, but not reflexive: the operator on the right will always act on a space of dimension at least as large as that on which the operator on the left acts. The notion of δ-equivalence is both transitive (its square root obeys the triangle inequality) and reflexive, and we will use it as our main notion of distance.

Tests. We formulate our tests as two-player games in which both players are treated symmetrically. We often use the same symbol, a capital letter $X, Z, W, \ldots$, to denote a question in the game and the associated projective measurement $\{W^a\}$ applied by the player upon receipt of that question. To a projective measurement with outcomes in $\{0,1\}^n$ we associate a family of observables $W(u)$ parametrized by n-bit strings $u \in \{0,1\}^n$, defined by $W(u) = \sum_a (-1)^{u\cdot a} W^a$. If $n = 1$ we simply write $W = W(1) = W^0 - W^1$; note that $W(0) = \mathrm{Id}$.

With the exception of the Tomography Test TOM presented in Section A.8, all the games, or tests, we consider implicitly include a "consistency test" which is meant to enforce that whenever both players are sent identical questions, they produce matching answers. More precisely, let T be any of the two-player tests described in the paper. Let $\Pr_T(W, W')$ be the distribution on questions (W, W') to the players that is specified by T. Since the players are always treated symmetrically, $\Pr_T(\cdot,\cdot)$ is permutation-invariant. Let $\Pr_T(\cdot)$ denote the marginal on either player. Then, instead of executing the test T as described, the verifier performs the following:

(i) With probability $1/2$, execute T.
(ii) With probability $1/2$, select a random question W according to $\Pr_T(W)$. Send W to both players. Accept if and only if the players' answers are equal.

Then, success with probability at least $1-\varepsilon$ in the modified test implies success with probability at least $1-2\varepsilon$ in the original test, as well as in the consistency test. If $\{W_{\mathsf{A}}^a\}$ and $\{W_{\mathsf{B}}^b\}$ are the players' corresponding projective measurements, the latter condition implies

$$\begin{aligned}\sum_a \big\|(W_{\mathsf{A}}^a \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{\mathsf{B}}^a)|\psi\rangle_{\mathsf{AB}}\big\|^2 &= 2 - 2\sum_a \langle\psi| W_{\mathsf{A}}^a \otimes W_{\mathsf{B}}^a |\psi\rangle \\ &\leq 4\varepsilon, \end{aligned} \tag{7}$$

so that $W_{\mathsf{A}}^a \otimes \mathrm{Id} \approx_\varepsilon \mathrm{Id} \otimes W_{\mathsf{B}}^a$ (where the condition should be interpreted on average over the choice of a question W distributed as in the test). Similarly, if W_{A}, W_{B} are observables for the players that succeed in the consistency test with probability $1-2\varepsilon$ we obtain $W_{\mathsf{A}} \otimes \mathrm{Id} \approx_\varepsilon \mathrm{Id} \otimes W_{\mathsf{B}}$. We will often use both relations to "switch" operators from one player's space to the other's; as a result we will also often omit an explicit specification of which player's space an observable is applied to.

Strategies. Given a two-player game, or test, a strategy for the players consists of a bipartite entangled state $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ together with families of projective measurements $\{W_{\mathsf{A}}^a\}$ for Alice and $\{W_{\mathsf{B}}^a\}$ for Bob, one for each question W that can be sent to either player in the test. As already mentioned, for convenience we restrict our attention to pure-state strategies employing projective measurements. We will loosely refer to a strategy for the players as $(W, |\psi\rangle)$, with the symbol W referring to the complete set of projective measurements used by the players in the game; taking advantage of symmetry we often omit the subscript A or B, as all statements involving observables for one player hold verbatim with the other player's observables as well.

Relations. We use $\mathcal{R}$ to denote a set of relations over variables $X, Z, W, \dots$, such as

$$\mathcal{R} = \{XZXZ = -\mathrm{Id},\ HX = ZH,\ X, Z, H \in \mathrm{Obs}\}.$$

We only consider relations that can be brought in the form of one of the following equations

- $f(W) = (-1)^a W_1 \cdots W_k = \mathrm{Id}$, where the W_i are (not necessarily distinct) unitary variables and $a \in \mathbb{Z}_2$, or
- $f(W) = W_1 \cdot (\sum_a \omega_a W_2^a) = \mathrm{Id}$, where W_1 is a unitary variable, $\{W_2^a\}$ a projective measurement with s possible outcomes, and ω_a are (arbitrary) s-th roots of unity.

Definition 2 (Rigid self-test). *We say that a set of relations $\mathcal{R}$ is $(c, \delta(\varepsilon))$-testable, on average under the distribution $\mathcal{D} : \mathcal{R} \to [0,1]$, if there exists a game (or test) G with question set $\mathcal{Q}$ that includes (at least) a symbol for each variable in $\mathcal{R}$ that is either an observable or a POVM and such that:*

- *(*Completeness*) There exists a set of operators which exactly satisfy all relations in $\mathcal{R}$ and a strategy for the players which uses these operators (together possibly with others for the additional questions) that has success probability at least c;*
- *(*Soundness*) For any $\varepsilon > 0$ and any strategy $(W, |\psi\rangle_{AB})$ that succeeds in the game with probability at least $c - \varepsilon$, the associated measurement operators satisfy the relations in $\mathcal{R}$ up to $\delta(\varepsilon)$, in the state-dependent norm. More precisely, on average over the choice of a relation $f(W) = \mathrm{Id}$ from $\mathcal{R}$ chosen according to $\mathcal{D}$, it holds that $\|\mathrm{Id} \otimes (f(W) - \mathrm{Id})|\psi\rangle_{AB}\|^2 \le \delta(\varepsilon)$.*

If both conditions hold, we also say that the game G is a robust $(c, \delta(\varepsilon))$ self-test for the relations $\mathcal{R}$.

Most of the games we consider have perfect completeness, $c = 1$, in which case we omit explicitly mentioning the parameter. The distribution $\mathcal{D}$ will often be implicit from context, and we do not always specify it explicitly (e.g. in case we only measure $\delta(\varepsilon)$ up to multiplicative factors of order $|\mathcal{R}|$ the exact distribution $\mathcal{D}$ does not matter as long as it has complete support).

Definition 3 (Stable relations). *We say that a set of relations $\mathcal{R}$ is $\delta(\varepsilon)$-stable, on average under the distribution $\mathcal{D} : \mathcal{R} \to [0,1]$, if for any two families of operators $W_A \in \mathrm{L}(\mathcal{H}_A)$ and $W_B \in \mathrm{L}(\mathcal{H}_B)$ that are consistent on average, i.e.*

$$\mathop{\mathrm{E}}_{f\sim\mathcal{D}} \mathop{\mathrm{E}}_{W\in_U f} \big\|(\mathrm{Id} \otimes W_B - W_A \otimes \mathrm{Id})|\psi\rangle\big\|^2 \le \varepsilon,$$

where $W \in_U f$ is shorthand for W being a uniformly random operator among those appearing in the relation specified by f, and satisfy the relations on average, i.e.

$$\mathop{\mathrm{E}}_{\substack{f\sim\mathcal{D}:\\ f(W)=\mathrm{Id}\in\mathcal{R}}} \big\|(f(W_A) - \mathrm{Id}) \otimes \mathrm{Id}\,|\psi\rangle\big\|^2 \le \varepsilon,$$

there exists operators $\hat{W}$ which satisfy the same relations exactly and are $\delta(\varepsilon)$-isometric to the W with respect to $|\psi\rangle$, on average over the choice of a random relation in $\mathcal{R}$ and *a uniformly random W appearing in the relation, i.e. there exists an isometry V_A such that*

$$\mathop{\mathrm{E}}_{f\sim\mathcal{D}}\mathop{\mathrm{E}}_{W\in_U f}\big\|(\hat{W}_A - V_A^\dagger W_A V_A)\otimes \mathrm{Id}\,|\psi\rangle\big\|^2 = O(\delta(\varepsilon)).$$

A.2 Some simple tests

In this appendix we collect simple tests that will be used as building blocks. In Section A.2 and Section A.2 we review elementary tests whose analysis is either immediate or can be found in the literature. In Section A.2 we formulate a simple test for measurements in the Bell basis and the associated two-qubit SWAP observable.

The Magic Square game We use the Magic Square game [Mer90] as a building block, noting that it provides a robust self-test test for the two-qubit Weyl-Heisenberg group (see Section 2.1 for the definition). Questions in this game are specified by a triple of labels corresponding to the same row or column from the square pictured in Figure 11 (so a typical question could be (IZ, XI, XZ); there are 6 questions in total, each a triple). An answer is composed of three values in $\{\pm 1\}$, one for each of the labels making up the question. Answers from the prover should be entrywise consistent, and such that the product of the answers associated to any row or column except the last should be $+1$; for the last column it should be -1. The labels indicate the "honest" strategy for the game, which consists of each prover measuring two half-EPR pairs using the commuting Pauli observables indicated by the labels of his question.

IZ	ZI	ZZ
XI	IX	XX
XZ	ZX	YY

Fig. 11: Questions, and a strategy, for the Magic Square game

The following lemma states some properties of the Magic Square game, interpreted as a self-test (see e.g. [WBMS16]).

Lemma 6. *Suppose a strategy for the provers, using state $|\psi\rangle$ and observables W, succeeds with probability at least $1-\varepsilon$ in the Magic Square game. Then there exist isometries $V_D : \mathcal{H}_D \to (\mathbb{C}^2\otimes\mathbb{C}^2)_{D'}\otimes\mathcal{H}_{\hat{D}}$, for $D\in\{A,B\}$ and a state $|\mathrm{AUX}\rangle_{\hat{A}\hat{B}} \in \mathcal{H}_{\hat{A}}\otimes\mathcal{H}_{\hat{B}}$ such that*

$$\big\|(V_A\otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle_{A'B'}^{\otimes 2}|\mathrm{AUX}\rangle_{\hat{A}\hat{B}}\big\|^2 = O(\sqrt{\varepsilon}),$$

and for $W\in\{I,X,Z\}^2\cup\{YY\}$,

$$\big\|\big(W - V_A^\dagger \sigma_W V_A\big)\otimes \mathrm{Id}_B\,|\psi\rangle\big\|^2 = O(\sqrt{\varepsilon}).$$

Elementary tests Figure 12 summarizes some elementary tests. For each test, "Inputs" refers to a subset of designated questions in the test; "Relation" indicates a relation that the test aims to certify (in the sense of Section A.1); "Test" describes the certification protocol. (Recall that all our protocols implicitly include a "consistency" test in which a question is chosen uniformly at random from the marginal distribution and sent to both provers, whose answers are accepted if and only if they are equal.)

Test $\textsc{id}(A,B)$:

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $A = B$.
- Test: Send $W \in \{A,B\}$ and $W' \in \{A,B\}$, chosen uniformly at random, to the first and second prover respectively. Receive an answer in $\{\pm 1\}$ from each prover. Accept if and only if the answers are equal whenever the questions are identical.

Test $\textsc{ac}(X,Z)$:

- Inputs: X, Z two observables on the same space $\mathcal{H}$.
- Relation: $XZ = -ZX$.
- Test: Execute the Magic Square game, using the label "X" for the "XI" query, and "Z" for the "ZI" query.

Test $\textsc{com}(A,B)$:

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $AB = BA$.
- Test: Send $W \in \{A,B\}$ chosen uniformly at random to the first prover. Send (A,B) to the second prover. Receive a bit $c \in \{\pm 1\}$ from the first prover, and two bits $(a',b') \in \{\pm 1\}^2$ from the second. Accept if and only if $c = a'$ if $W = A$, and $c = b'$ if $W = B$.

Test $\textsc{prod}(A,B,C)$:

- Inputs: A, B and C three observables on the same space $\mathcal{H}$.
- Relations: $AB = BA = C$.
- Test: Similar to the commutation game, but use C to label the question (A,B).

Fig. 12: Some elementary tests.

Lemma 7. *Each of the tests described in Figure 12 is a robust $(1,\delta)$ self-test for the indicated relation(s), for some $\delta = O(\varepsilon^{1/2})$.*

Proof. The proof for each test is similar. As an example we give it for the commutation test $\textsc{com}(A,B)$.

First we verify completeness. Let A,B be two commuting observables on $\mathcal{H}_\mathsf{A} = \mathcal{H}_\mathsf{B} = \mathcal{H}$, and $|\text{EPR}\rangle_{\mathsf{AB}}$ the maximally entangled state in $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. Upon receiving question A or B, the prover measures the corresponding observable. If the question is (A,B), he jointly measures A and B. This strategy succeeds with probability 1 in the test.

Next we establish soundness. Let $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ be a state shared by the provers, A, B their observables on questions A, B, and $\{C^{a,b}\}$ the four-outcome PVM applied on question (A,B). Assume the strategy succeeds with probability at least $1-\varepsilon$. Recall that this includes both the test described in Figure 12, and the automatic consistency test. Let $C_A = \sum_{a,b}(-1)^a C^{a,b}$ and $C_B = \sum_{a,b}(-1)^b C^{a,b}$. Then C_A and C_B commute. Thus

$$\begin{aligned} A_{\mathsf{A}} B_{\mathsf{A}} \otimes \mathrm{Id}_{\mathsf{B}} &\approx_{\sqrt{\varepsilon}} A_{\mathsf{A}} \otimes (C_B)_{\mathsf{B}} \\ &\approx_{\sqrt{\varepsilon}} \mathrm{Id}_{\mathsf{A}} \otimes (C_B)_{\mathsf{B}} (C_A)_{\mathsf{B}} \\ &= \mathrm{Id}_{\mathsf{A}} \otimes (C_A)_{\mathsf{B}} (C_B)_{\mathsf{B}} \\ &\approx_{\sqrt{\varepsilon}} B_{\mathsf{A}} \otimes (C_A)_{\mathsf{B}} \\ &\approx_{\sqrt{\varepsilon}} B_{\mathsf{A}} A_{\mathsf{A}} \otimes \mathrm{Id}_{\mathsf{B}}\,. \end{aligned}$$

Here each approximation uses the consistency condition provided by the test, as explained in (7). Thus $[A,B] = (AB - BA) \approx_{\sqrt{\varepsilon}} 0$, as desired.

We will often make use of the following simple lemma, which expresses an application of the above tests.

Lemma 8. *Let $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ and A, X observables on $\mathcal{H}_{\mathsf{A}}$ such that there exists an isometry $\mathcal{H}_{\mathsf{A}} \simeq \mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*[7]

(i) There exists an observable A' on $\mathcal{H}_{\mathsf{B}}$ such that $A \otimes \mathrm{Id} \approx_{\delta_1} \mathrm{Id} \otimes A'$;
(ii) $|\psi\rangle \simeq_{\delta_1} |\mathrm{EPR}\rangle|\textsc{aux}\rangle$ and $X \simeq_{\delta_1} \sigma_X \otimes \mathrm{Id}$;
(iii) $[A,X] \approx_{\delta_2} 0$;
(iv) $\{A,X\} \approx_{\delta_3} 0$.

Then there exist Hermitian A_I, A_X, A_Y, A_Z on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that $A \simeq_{\delta_1+\delta_2} \mathrm{Id} \otimes A_I + \sigma_X \otimes A_X$ and $A \simeq_{\delta_1+\delta_3} \sigma_Y \otimes A_Y + \sigma_Z \otimes A_Z$. (A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $\mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P\in\{I,X,Y,Z\}} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. We can compute

$$[\tilde{A}, \sigma_X \otimes \mathrm{Id}] = -2i\,\sigma_Z \otimes A_Y + 2i\,\sigma_Y \otimes A_Z, \tag{8}$$

$$\{\tilde{A}, \sigma_X \otimes \mathrm{Id}\} = 2\,\sigma_X \otimes A_I + 2\,\sigma_I \otimes A_X. \tag{9}$$

Assumptions (i) and (ii) imply $[A,X] \simeq_{\delta_1} [\tilde{A}, \sigma_X \otimes \mathrm{Id}]$, so by (iii) and (8) we get $\|A_Y|\textsc{aux}\rangle\|^2 + \|A_Z|\textsc{aux}\rangle\|^2 = O(\delta_1+\delta_2)$. Similarly, (iv) and (9) give $\|A_I|\textsc{aux}\rangle\|^2 + \|A_X|\textsc{aux}\rangle\|^2 = O(\delta_1+\delta_3)$.

[7] Note that we allow either δ_i to equal 1, leading to a vacuous condition.

The Bell basis Given two commuting pairs of anti-commuting observables $\{X_1, Z_1\}$ and $\{X_2, Z_2\}$ we provide a test for a four-outcome projective measurement in the Bell basis specified by these observables, i.e. the joint eigenbasis of X_1X_2 and Z_1Z_2. The same test can be extended to test the "SW" observable,

$$\mathrm{SW} \;=\; \frac{1}{2}\big(\,\mathrm{Id} + X_1X_2 + Z_1Z_2 - (X_1Z_1)(X_2Z_2)\big), \tag{10}$$

which exchanges the qubits specified by each pair of observables. The Bell measurement test described in Figure 13 tests for both.

Test $\text{BELL}(X_1, X_2, Z_1, Z_2)$:

- Inputs: For $i \in \{1,2\}$, $\{X_i, Z_i\}$ observables, $\{\Phi^{ab}\}_{a,b\in\{0,1\}}$ a four-outcome projective measurement, and SW an observable, all acting on the same space $\mathcal{H}$.
- Relations: for all $a,b \in \{0,1\}$, $\Phi^{ab} = \frac{1}{4}\big(\,\mathrm{Id} + (-1)^a Z_1Z_2\big)\big(\,\mathrm{Id} + (-1)^b X_1X_2\big)$, and $\mathrm{SW} = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}$.
- Test: execute each of the following with equal probability:
  (a) Execute the Magic Square game, labeling each entry of the square from Figure 11 (except entry $(3,3)$, labeled as Y_1Y_2) using the observables X_1, Z_1 and X_2, Z_2.
  (b) Send Φ to one prover and the labels (X_1X_2, Z_1Z_2, Y_1Y_2) associated with the third column of the Magic Square to the other. The first prover replies with $a,b \in \{0,1\}$, and the second with $c,d,e \in \{\pm 1\}$. The referee checks the provers' answers for the obvious consistency conditions. For example, if the first prover reports the outcome $(0,0)$, then the referee rejects if $(c,d) \neq (+1,+1)$.
  (c) Send Φ to one prover and SW to the other. The first prover replies with $a,b \in \{0,1\}$, and the second with $c \in \{\pm 1\}$. Accept if and only $c = (-1)^{ab}$.

Fig. 13: The Bell measurement test.

Lemma 9. *The test* $\text{BELL}(X_1, X_2, Z_1, Z_2)$ *is a robust* $(1,\delta)$ *self-test for*

$$\begin{aligned}\mathcal{R} = \Big\{&\{\Phi^{ab}\}_{a,b\in\{0,1\}} \in \text{Proj},\ \mathrm{SW} \in \text{Obs}\Big\}\\ &\cup \Big\{\Phi^{ab} = \frac{1}{4}\big(1 + (-1)^a Z_1Z_2\big)\big(1 + (-1)^b X_1X_2\big)\Big\}\\ &\cup \big\{\mathrm{SW} = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}\big\},\end{aligned}$$

for some $\delta(\varepsilon) = O(\sqrt{\varepsilon})$.

Proof. Completeness is clear: the provers can play the honest strategy for the Magic Square game, use a measurement in the Bell basis on their two qubits for Φ, and measure the observable in (10) for SW.

For soundness, let $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, $\{W_1W_2' :\ W, W' \in \{I, X, Z\}\}$, $\{\Phi^{ab}\}$ and SW denote a state and operators for a strategy that succeeds with probability at least $1-\varepsilon$ in the test. From the analysis of the Magic Square game (Lemma 6) it follows that the provers' observables X_1X_2 and Z_1Z_2 associated to questions with those labels approximately commute, and are each the product of two commuting observables X_1I, IX_2 and Z_1I, IZ_2 respectively, such that X_1I and Z_1I, and IX_2 and IZ_2, anti-commute; all approximate identities hold up to error $O(\sqrt{\varepsilon})$.

Since X_1X_2 and Z_1Z_2 appear together in the same question (the last column of the Magic Square, Figure 11), each prover has a four-outcome projective measurement $\{W^{c,d}\}_{c,d\in\{0,1\}}$ such that $\sum_d(-1)^cW^{c,d} = X_1X_2$ and $\sum_c(-1)^dW^{c,d} = Z_1Z_2$, from which it follows that $W^{c,d} = (1/4)(1+(-1)^cZ_1Z_2)(1+(-1)^dX_1X_2)$.

The prover's success probability in part (b) of the test is then

$$\sum_{a,b}\langle\psi|\Phi^{ab}\otimes W^{a,b}|\psi\rangle = \sum_{a,b}\langle\psi|\Phi^{ab}\otimes\frac{1}{4}\big(1+(-1)^aZ_1Z_2\big)\big(1+(-1)^bX_1X_2\big)|\psi\rangle.$$

Using that, by assumption, $\{\Phi^{ab}\}$ is a projective measurement, the condition that this expression be at least $1-O(\varepsilon)$ implies

$$\Phi^{ab}\otimes\mathrm{Id}\approx_{\sqrt{\varepsilon}}\mathrm{Id}\otimes\frac{1}{4}\big(1+(-1)^aZ_1Z_2\big)\big(1+(-1)^bX_1X_2\big).$$

Combining this with the implicit consistency test yields the first relation. The last is guaranteed by part (c) of the test, which checks for the correct relationship between SW and Φ; the analysis is similar.

A.3 The m-qubit Pauli group

In this section we formulate a robust self-test for the m-qubit Pauli group. The result is a slight extension of the results from [NV17] to allow testing of σ_Y observables.

The m-qubit Weyl-Heisenberg group We start by giving a self-test for tensor products of σ_X and σ_Z observables acting on m qubits, i.e. the m-qubit Weyl-Heisenberg group $\mathcal{H}^{(m)}$ (see Section 2.1). Let $\mathcal{P}^{(m)}$ denote the relations

$$\begin{aligned}\mathcal{P}^{(m)}\{X,Z\} = &\Big\{W(a)\in\mathrm{Obs},\ W\in\prod_{i=1}^m\{X_i,Z_i\},\ a\in\{0,1\}^m\Big\}\\ &\cup\Big\{W(a)W'(a') = (-1)^{|\{i:\,W_i\neq W'_i\wedge a_ia'_i=1\}|}W'(a')W(a),\ \forall a,a'\in\{0,1\}^m\Big\}\\ &\cup\Big\{W(a)W(a') = W(a+a'),\ \forall a,a'\in\{0,1\}^m\Big\}.\end{aligned}$$

Recall the notation $W(a)$ for the string that is W_i when $a_i = 1$ and I otherwise. The first set of relations expresses the canonical anti-commutation relations. The second set of relations expresses the obvious relations $\sigma_W\,\mathrm{Id} = \mathrm{Id}\,\sigma_W$ and $\sigma_W^2 = \mathrm{Id}$, for $W\in\{X,Z\}$, coordinate-wise. It is easy to verify that $\mathcal{P}^{(m)}$ forms a defining set of relations for $\mathcal{H}^{(m)}$. Our choice of relations is suggested by the Pauli braiding test introduced in [NV17], which shows that the relations are testable with a robustness parameter $\delta(\varepsilon)$ that is independent of m. The underlying test is called the Pauli braiding test, and denoted $\textsc{pbt}(X, Z)$. For convenience here we use a slight variant of the test, which includes more questions; the test is summarized in Figure 14.

Test $\textsc{pbt}(X, Z)$:

- Inputs: (W, a), for $W \in \prod_{i=1}^{n} \{X_i, Z_i\}$ and $a \in \{0,1\}^m$.
- Relations: $\mathcal{P}^{(m)}\{X, Z\}$.
- Test: Perform the following with probability $1/2$ each:
  (a) Select $W, W' \in \prod_i \{X_i, Z_i\}$, and $a, a' \in \{0,1\}^m$, uniformly at random. If $\{i : W_i \neq W'_i \wedge a_i = a'_i = 1\}$ has even cardinality then execute test $\textsc{com}(W(a), W'(a'))$. Otherwise, execute test $\textsc{ac}(W(a), W'(a'))$.
  (b) Select $(a, a') \in \{0,1\}^m$ and $W \in \prod_{i=1}^{m} \{X_i, Z_i\}$ uniformly at random. Execute test $\textsc{prod}(W(a), W(a'), W(a + a'))$.

Fig. 14: The Pauli braiding test, $\textsc{pbt}(X, Z)$.

The following lemma follows immediately from the definition of $\mathcal{P}^{(m)}\{X, Z\}$ and the analysis of the tests COM, PROD and AC given in Section A.2.

Lemma 10 (Theorem 13 [NV17]). *The test $\textsc{pbt}(X, Z)$ is a robust $(1, \delta)$ self-test for $\mathcal{P}^{(m)}\{X, Z\}$, for some $\delta(\varepsilon) = O(\varepsilon^{1/2})$.*

In addition we need the following lemma, which states that observables approximately satisfying the relations $\mathcal{P}^{(m)}\{X, Z\}$ are close to operators which, up to a local isometry, behave exactly as a tensor product of Pauli σ_X and σ_Z observables.

Lemma 11 (Theorem 14 [NV17]). *The set of relations $\mathcal{P}^{(n)}$ is δ-stable, with $\delta(\varepsilon) = O(\varepsilon)$.*

Lemma 11 is proved in [NV17] with a polynomial dependence of δ on ε. The linear dependence can be established by adapting the results of [GH15] to the present setting; we omit the details (see [Vid17]).

The following lemma is an extension of Lemma 8 to the case of multi-qubit Pauli observables; the lemma avoids any dependence of the error on the number of qubits, as would follow from a sequential application of Lemma 8.

Lemma 12. *Let n be an integer, $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ and A and $X(a)$, for $a \in \{0,1\}^m$, observables on $\mathcal{H}_{\mathsf{A}}$ such that there exists an isometry $\mathcal{H}_{\mathsf{A}} \simeq (\mathbb{C}^2)^{\otimes m} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*

(i) There exists an observable A' on $\mathcal{H}_{\mathsf{B}}$ such that $A \otimes \mathrm{Id} \approx_{\delta_1} \mathrm{Id} \otimes A'$;
(ii) $|\psi\rangle \simeq_{\delta_1} |\mathrm{EPR}\rangle^{\otimes m} |\textsc{aux}\rangle$, and $X(a) \simeq_{\delta_1} \sigma_X(a) \otimes \mathrm{Id}$;
(iii) $[A, X(a)] \simeq_{\delta_2} 0$;
(iv) For some $c \in \{0,1\}^m$ and $a \cdot c = 1$, $\{A, X(a)\} \simeq_{\delta_3} 0$;

where the first two conditions are meant on average over a uniformly random $a \in \{0,1\}^m$, and the last over a uniformly random a such that $a \cdot c = 1$. For some $P \in \{I, X, Y, Z\}^m$ let $x_P \in \{0,1\}^m$ be such that $(x_P)_i = 1$ if and only if $P_i \in \{Y, Z\}$. Then there exists Hermitian A_P, for $P \in \{I, X, Y, Z\}^m$, on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that

$$A \simeq_{\delta_1+\delta_2} \sum_{P\in\{I,X\}^n} \sigma_P \otimes A_P, \qquad \textit{and} \qquad A \simeq_{\delta_1+\delta_3} \sum_{\substack{P\in\{I,X,Y,Z\}^m: \\ c_i=1 \implies P_i\in\{Y,Z\} \\ c_i=0 \implies P_i\in\{I,X\}}} \sigma_P \otimes A_P.$$

(A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $(\mathbb{C}^2)^{\otimes m} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P\in\{I,X,Y,Z\}^m} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. Then the analogue of (8) is

$$[\tilde{A}, \sigma_X(a) \otimes \mathrm{Id}] = 2 \sum_{P:\, a\cdot x_P=1} \sigma_P \sigma_X(a) \otimes A_P.$$

Using that any string x_P which is not the 0^m string satisfies $a \cdot x_P = 1$ with probability almost $1/2$ for a uniform choice of a, orthogonality of the $\sigma_P \sigma_X(a)$ for distinct P lets us conclude the proof of the first relation as in Lemma 8. Similarly, the analogue of (9) gives

$$\{\tilde{A}, \sigma_X(a) \otimes \mathrm{Id}\} = 2 \sum_{P:\, a\cdot x_P=0} \sigma_P \sigma_X(a) \otimes A_P.$$

Using that any string x_P which is not c satisfies $a \cdot x_P = 0$ with probability almost $1/2$ for a uniform choice of a such that $a \cdot c = 1$, orthogonality of the $\sigma_P \sigma_X(a)$ for distinct P lets us conclude the proof of the second relation.

The m-qubit Pauli group We will use an extended version of the Pauli braiding test introduced in Section A.3 which allows to test for a third observable, Y_i, on each system. Ideally we would like to enforce the relation $Y_i = \sqrt{-1} X_i Z_i$. Unfortunately, the complex phase cannot be tested from classical correlations alone: complex conjugation leaves correlations invariant, but does not correspond to a unitary change of basis (see [RUV12, Appendix A] for a discussion of this issue).

We represent the "choice" of complex phase, $\sqrt{-1}$ or its conjugate $-\sqrt{-1}$, by an observable Δ that the prover measures on a system that is in a tensor product with all other systems on which the prover acts. Informally, the outcome obtained when measuring Δ tells the prover to use $Y = iXZ$ or $Y = -iXZ$.

We first introduce Y and test that the triple $\{X, Y, Z\}$ pairwise anticommute at each site. This corresponds to the following set of relations:

$$\begin{aligned}
\mathcal{P}^{(m)}\{X,Y,Z\} = &\Big\{ W(a) \in \mathrm{Obs},\ W \in \{X,Y,Z\}^n,\ a \in \{0,1\}^n \Big\} \\
&\cup \Big\{ W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|} W'(a')W(a),\ \forall a, a' \in \{0,1\}^n \Big\} \\
&\cup \Big\{ W(a)W(a') = W(a+a'),\ \forall a, a' \in \{0,1\}^n \Big\}.
\end{aligned}$$

Test $\textsc{pbt}(X,Y,Z)$:

- Inputs: $W \in \prod_{i=1}^m \{X,Y,Z\}$
- Relations: $\mathcal{P}^{(m)}\{X,Y,Z\}$.
- Test: Perform the following with equal probability:
  (a) Execute test $\textsc{pbt}(X^m,Z^m)$.
  (b) Execute test $\textsc{pbt}(Y^m,X^m)$ or test $\textsc{pbt}(Y^m,Z^m)$, chosen with probability $1/2$ each.
  (c) Select a random permutation $\sigma \in \mathfrak{S}_{m/2}$, and $W \in \{I,Y\}^m$ uniformly at random. Write $W = W_1W_2$, where $W_1,W_2 \in \{I,Y\}^{m/2}$. Let W_1^σ be the string W_1 with its entries permuted according to σ. Do the following with equal probability:
    (i) Send one prover $W_1W_1^\sigma$ and the other either W_1W_2 or $W_2W_1^\sigma$ (chosen with probability $1/2$), and check consistency of the first or second half of the provers' answer bits.
    (ii) Send one prover $W_1W_1^\sigma$, and the other $\prod_i \Phi_{i,\sigma(i)}$, where each $\Phi_{i,\sigma(i)}$ designates a measurement in the Bell basis for the $(i,m/2+\sigma(i))$ pair of qubits. The first prover replies with $a \in \{\pm1\}^m$, and the second with $b \in \{00,01,10,11\}^{m/2}$. For each $i \in \{1,\ldots,m/2\}$ such that $b_i = 00$, check that $a_i = a_{m/2+\sigma(i)}$.
    (iii) Execute $m/2$ copies of test BELL (in parallel), for qubit pairs $(i,m/2+\sigma(i))$, for $i \in \{1,\ldots,m/2\}$.

Fig. 15: The extended Pauli braiding test, $\textsc{pbt}(X,Y,Z)$.

The test is described in Figure 15. It has three components. Part (a) of the test executes test $\textsc{pbt}(X^m,Z^m)$, which gives us multi-qubit Pauli X and Z observales. Part (b) of the test introduces observables labeled $Y(c)$, and uses tests $\textsc{pbt}(Y^m,X^m)$ and $\textsc{pbt}(Y^m,Z^m)$ to enforce appropriate anti-commutation relations with the Pauli X and Z observables obtained in part (a). Using Lemma 12, this part of the test will establish that the $Y(c)$ observables approximately respect the same n-qubit tensor product structure as $X(a)$ and $Z(b)$.

Part (c) of the test is meant to control the "phase" ambiguity in the definition of $Y(c)$ that remains after the analysis of part (b). Indeed, from that part it will follow that $Y(c) \simeq \sigma_Y(c)\otimes\Delta(c)$, where $\Delta(c)$ is an arbitrary observable acting on the ancilla system produced by the isometry obtained in part (a). We would like to impose $\Delta(c) \approx \Delta_Y^{|c|}$ for a fixed observable Δ_Y which represents the irreducible phase degree of freedom in the definition of Y, as discussed above. To obtain this, part (c) of the test performs a form of SWAP test between different $Y(c)$ observables, enforcing that e.g. $Y(1,0,1)$ is consistent with $Y(0,1,1)$ after an appropriate Bell measurement has "connected" registers 1 and 2. The swapping is defined using Pauli σ_X and σ_Z, which leave the ancilla register invariant; consistency will then imply $\Delta(1,0,1) \approx \Delta(0,1,1)$.

Lemma 13. *Suppose $|\psi\rangle \in \mathcal{H}_A\otimes\mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, for $W \in \{X,Y,Z\}^m$ and $a \in \{0,1\}^m$, specify a strategy for the players that has success probability at least $1-\varepsilon$ in the extended Pauli braiding test $\textsc{pbt}(X,Y,Z)$ described in Figure 15. Then there exist isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes m})_{D'}\otimes\hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A,B\}$, such that*

$$\big\|(V_A\otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle_{A'B'}^{\otimes n}|\textsc{aux}\rangle_{\hat{A}\hat{B}}\big\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X,Y,Z\}^m$,

$$\mathop{\mathrm{E}}_{a\in\{0,1\}^m} \big\| \big(W(a) - V_A^\dagger(\sigma_W(a)\otimes\Lambda_W(a))V_A\big)\otimes \mathrm{Id}_B\,|\psi\rangle \big\|^2 = O(\sqrt{\varepsilon}), \qquad (11)$$

where $\Lambda_W(a) = \prod_i \Lambda_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{\mathsf{A}}})$ *are observables with* $\Delta_X = \Delta_Z = \mathrm{Id}$ *and* Δ_Y *an arbitrary observable on* $\hat{\mathcal{H}}$ *such that*

$$\big\|\Delta_Y\otimes\Delta_Y|\textsc{aux}\rangle - |\textsc{aux}\rangle\big\|^2 = O(\sqrt{\varepsilon}).$$

Proof (Proof sketch). The existence of the isometries V_A and V_B follows from part (a) of the test and the combination of Lemma 10 and Lemma 11; see e.g. [NV17] for an explicit construction. Under this isometry we have $X(a) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)$ and $Z(b) \simeq_{\sqrt{\varepsilon}} \sigma_Z(b)$, on average over $a,b \in \{0,1\}^m$. Applying the second part of Lemma 12, the anti-commutation relations between $Y(c)$ and $X(a)$ and $Z(b)$ verified in part (b) of the test imply that under the same isometry,

$$Y(c) \simeq \sigma_Y(c)\otimes\Delta(c),$$

for some observable $\Delta(c)$ on $\mathcal{H}_{\hat{\mathsf{A}}}$. Using the linearity relations that are verified in the PBT test, we may in addition express $\Delta(c) = \prod_i \Delta_i^{c_i}$ for (perfectly) commuting observables Δ_i. Using Claim A.3 below, success at least $1-O(\varepsilon)$ in part (c) of the test then implies that on average over a random permutation $\sigma\in\mathcal{S}_{n/2}$,

$$\mathop{\mathrm{E}}_{\sigma}\mathop{\mathrm{E}}_{c\in\{0,1\}^{m/2}} 2^{-m}\mathrm{Tr}\big(\sigma_Y(c,c^\sigma)\big)\,\langle\textsc{aux}|\Big(\prod_{i=1}^{m/2}\big(\Delta_i\Delta_{m/2+\sigma(i)}\big)^{c_i}\Big)|\textsc{aux}\rangle = 1-O(\sqrt{\varepsilon}), \qquad (12)$$

where we wrote (c,c^σ) for the m-bit string $(c_1,\ldots,c_{m/2},c_{\sigma(1)},\ldots,c_{\sigma(m/2)})$. Defining

$$\Delta_Y \;=\; \mathop{\mathrm{E}}_{i\in\{\frac{m}{2}+1,\ldots,m\}} \frac{\Delta_i}{|\,\mathrm{E}_i\,\Delta_i|}, \qquad (13)$$

Eq. (12) readily implies that $\Delta(c) \approx_{\sqrt{\varepsilon}} \Delta_Y^{|c|}$. In slightly more detail, we first observe that

$$\mathop{\mathrm{E}}_{c\in\{0,1\}^{m/2}}\Big\|\Big(\Delta(c) - \big(\mathop{\mathrm{E}}_{i\in\{\frac{m}{2}+1,\ldots,m\}}\Delta_i\big)^{|c|}\Big)|\textsc{aux}\rangle\Big\|^2 \qquad (14)$$

$$\le \mathop{\mathrm{E}}_{c}\mathop{\mathrm{E}}_{g:\{1,\ldots,\frac{m}{2}\}\to\{\frac{m}{2}+1,\ldots,m\}}\Big\|\Big(\Delta(c) - \prod_i \Delta_{g(i)}^{c_i}\Big)|\textsc{aux}\rangle\Big\|^2. \qquad (15)$$

where the first inequality is by convexity, with the expectation taken over a random function g. We would like to relate this last term to the expectation over a random permutation $\sigma\in\mathcal{S}_{m/2}$. One way to do this is to observe that with probability $1-O(1/m)$ over the choice of a uniformly random g it is possible to write

$$\prod_i \Delta_{g(i)}^{c_i} = \Big(\prod_i \Delta_{m/2+\tau'(i)}^{c_i'}\Big)\Big(\prod_i \Delta_{m/2+\tau''(i)}^{c_i''}\Big),$$

where $c'_i + c''_i = c_i$ for all i, τ', τ'' are permutations such that $m/2 + \tau'(i) = g(i)$ if $c'_i = c_i$, and $m/2 + \tau''(i) = g(i)$ if $c''_i = c_i$; this is possible because g might have two-element collisions, but is unlikely to have any three-element collisions. Moreover, for uniformly random c and g we can ensure that the marginal distribution on (c', τ') and (c', τ'') is uniform. This allows us to use (12) twice to bound the right-hand side of (15) by $O(\sqrt{\varepsilon})$ (after having expanded the square). As a consequence, $\mathrm{E}_i\, \Delta_i$ is close to an observable, and it is then routine to show that Δ_Y defined in (13) satisfies $\Delta(c) \approx_{\sqrt{\varepsilon}} \Delta_Y^{|c|}$, on average over a uniformly random c.

The last condition in the lemma follows from the consistency relations, which imply that $X(a) \otimes X(a)$, $Z(b) \otimes Z(b)$ and $Y(c) \otimes Y(c)$ all approximately stabilize $|\psi\rangle$; then $\Delta_Y^{|a|} \otimes \Delta_Y^{|a|} \approx X(a)Z(a)Y(a) \otimes X(a)Z(a)Y(a)$ also does.

Claim. Let $A \in \mathrm{Obs}(\mathbb{C}^2_{\mathsf{A}_1} \otimes \cdots \otimes \mathbb{C}^2_{\mathsf{A}_k} \otimes \mathcal{H})$ and $B \in \mathrm{Obs}(\mathbb{C}^2_{\mathsf{B}_1} \otimes \cdots \otimes \mathbb{C}^2_{\mathsf{B}_k} \otimes \mathcal{H})$ be k-qubit observables acting on distinct registers A_j, B_j, as well as a common space $\mathcal{H}$, and $\Phi_{\mathsf{A'B'}} = \prod_{j=1}^k |\mathrm{EPR}\rangle\langle \mathrm{EPR}|_{\mathsf{A'}_j,\mathsf{B'}_j}$ the the projector on k EPR pairs across registers $\mathsf{A'}_j$ and $\mathsf{B'}_j$. Then

$$\Big(\bigotimes_j \langle \mathrm{EPR}|_{\mathsf{A}_j\mathsf{A'}_j} \langle \mathrm{EPR}|_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathrm{Id}_{\mathcal{H}}\Big)\Big(\big(A_{\mathsf{A}\mathcal{H}} \otimes \mathrm{Id}_{\mathsf{B}}\big)\big(\mathrm{Id}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}\big) \otimes \Phi_{\mathsf{A'B'}}\Big)\Big(\bigotimes_j |\mathrm{EPR}\rangle_{\mathsf{A}_j\mathsf{A'}_j} |\mathrm{EPR}\rangle_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathrm{Id}_{\mathcal{H}}\Big)$$

$$= \frac{1}{2^{2k}} \sum_i \mathrm{Tr}\big(A_i B_i\big) A'_i B'_i, \tag{16}$$

where we write $A = \sum_i A_i \otimes A'_i$ and $B = \sum_i B_i \otimes B'_i$, for A_i on $\mathcal{H}_{\mathsf{A}}$, B_i on $\mathcal{H}_{\mathsf{B}}$, and A'_i, B'_i on $\mathcal{H}$.

Proof. We do the proof for $k = 1$, as the general case is similar. Using that for any operators X_{AB} and $Y_{\mathsf{A'B'}}$,

$$\langle \mathrm{EPR}|_{\mathsf{AA'}} \langle \mathrm{EPR}|_{\mathsf{BB'}} \big(X_{\mathsf{AB}} \otimes Y_{\mathsf{A'B'}}\big) |\mathrm{EPR}\rangle_{\mathsf{AA'}} |\mathrm{EPR}\rangle_{\mathsf{BB'}} = \frac{1}{4} \mathrm{Tr}(XY^T),$$

the left-hand side of (16) evaluates to

$$4^{-1} \mathrm{Tr}_{\mathsf{AB}}\Big(\big(A_{\mathsf{A}\mathcal{H}} \otimes \mathrm{Id}_{\mathsf{B}}\big)\big(\mathrm{Id}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}\big)\big(\Phi^T_{\mathsf{A'B'}} \otimes \mathrm{Id}_{\mathcal{H}}\big)\Big),$$

which using the same identity again gives the right-hand side of (16).

A.4 The conjugation test

We give a test which certifies that a unitary (not necessarily an observable) conjugates one observable to another. More precisely, let A, B be observables, and R a unitary, acting on the same space $\mathcal{H}$. The test $\textsc{conj}(A, B, R)$, given in Figure 16, certifies that the players implement observables of the form

$$X_R = \begin{pmatrix} 0 & R^\dagger \\ R & 0 \end{pmatrix} \qquad \text{and} \qquad C = C_{A,B} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \tag{17}$$

such that X_R and C commute. The fact that X_R is an observable implies that R is unitary,[8] while the commutation condition is equivalent to the relation $RAR^\dagger = B$. The test thus tests for the relations

$$\mathcal{C}\{R,C\} = \big\{X_R, C, X, Z \in \mathrm{Obs}\big\} \cup \big\{XZ = -ZX\big\} \cup \big\{X_R C = C X_R,\ X_R Z = -Z X_R,\ CZ = ZC\big\}.$$

Here the anti-commuting observables X and Z are used to specify a basis in which X_R and C can be block-diagonalized. The anti-commutation and commutation relations with Z enforce that X_R and C respectively have the form described in (17). These relations are enforced using simple commutation and anti-commutation tests that are standard in the literature on self-testing. For convenience, we state those tests, COM and AC, in Appendix A.2. The conjugation test, which uses them as sub-tests, is given in Figure 16. Here, "Inputs" refers to a subset of designated questions in the test; "Relation" indicates a relation that the test aims to certify; "Test" describes the certification protocol. (Recall that all our protocols implicitly include a "consistency" test in which a question is chosen uniformly at random from the marginal distribution and sent to both players, whose answers are accepted if and only if they are equal.)

Test CONJ(A,B,R)

- Inputs: A and B observables on the same space $\mathcal{H}$, and X and Z observables on $\mathcal{H}'$. X_R and C observables on $\mathcal{H} \otimes \mathcal{H}'$.
- Relations: $\mathcal{C}\{R,C\}$, with R defined from X_R, and C related to A and B, as in (17).
- Test: execute each of the following with equal probability
  (a) With probability $1/8$ each, execute tests AC(X,Z), COM(C,Z), COM(X_R,C), AC(X_R,Z) and COM(A,X), COM(B,X), COM(A,Z), COM(B,Z).
  (b) Ask one player to measure A, B, C or Z (with probability $1/4$ each), and the other to jointly measure A or B (with probability $1/2$ each) and Z. The first player returns one bit, and the second two bits. Reject if either:
    - The first player was asked C, the second player was asked (A,Z), his second answer bit is 0, and his first answer bit does not match the first player's;
    - The first player was asked C, the second player was asked (B,Z), his second answer bit is 1, and his first answer bit does not match the first player's.
    - The first player was asked A, B, or Z and his answer bit does not match the corresponding answer from the second player.

Fig. 16: The conjugation test, CONJ(A,B,R).

Lemma 14. *The test* CONJ(A,B,R) *is a* $(1,\delta)$ *self-test for the set of relations* $\mathcal{C}\{R,C\}$*, for some* $\delta = O(\sqrt{\varepsilon})$*. Moreover, for any strategy that succeeds with probability at least* $1-\varepsilon$ *in the test it holds that* $C \approx_\delta A(\mathrm{Id}+Z)/2 + B(\mathrm{Id}-Z)/2$*, where* A, B, C *and* Z *are the observables applied by the prover on receipt of a question with the same label.*

[8] Note that R will not be directly accessed in the test, since by itself it does not necessarily correspond to a measurement.

Proof. Completeness is clear, as players making measurements on a maximally entangled state on $\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$, tensored with an EPR pair on $\mathbb{C}^2 \otimes \mathbb{C}^2$ for the X and Z observables, and using X_R and C defined in (17) (with the blocks specified by the space associated with each player's half-EPR pair) succeed in each test with probability 1.

We now consider soundness. Success in $\text{AC}(X,Z)$ in part (a) of the test implies the existence of local isometries V_A, V_B such that $V_A : \mathcal{H}_{\mathsf{A}} \to \mathcal{H}_{\hat{\mathsf{A}}} \otimes \mathbb{C}^2_{\mathsf{A}'}$, with $X \simeq_{\sqrt{\varepsilon}} \mathrm{Id}_{\hat{\mathsf{A}}} \otimes \sigma_X$ and $Z \simeq_{\sqrt{\varepsilon}} \mathrm{Id}_{\hat{\mathsf{A}}} \otimes \sigma_Z$. By Lemma 8, approximate commutation with both X and Z implies that under the same isometry, $A \simeq_{\sqrt{\varepsilon}} A_I \otimes \mathrm{Id}$ and $B \simeq_{\sqrt{\varepsilon}} B_I \otimes \mathrm{Id}$, for observables A_I, B_I on $\mathcal{H}_{\hat{\mathsf{A}}}$. Similarly, the parts of the test involving C and X_R imply that they each have the block decomposition specified in (17). In particular, anti-commutation of X_R with Z certifies that X_R has a decomposition of the form $X_R \simeq R_X \otimes \sigma_X + R_Y \otimes \sigma_Y$. Using that X_R is an observable, we deduce that there exists a unitary R on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that $R \approx R_X + iR_Y$. Similarly, commutation of C with Z implies that $C \simeq C_I \otimes I + C_Z \otimes \sigma_Z$, for Hermitian C_I, C_Z such that $C_I \pm C_Z$ are observables.

Next we analyze part (b) of the test. Let $\{W_{AZ}^{a,z}\}$ be the projective measurement applied by the second player upon query (A,Z). Success with probability $1 - O(\varepsilon)$ in the first item ensures that

$$\big|\langle\psi| C \otimes (W_{AZ}^{00} - W_{AZ}^{10})|\psi\rangle\big| \,=\, O(\varepsilon),$$

and a similar condition holds from the second item, with W_{BZ} instead of W_{AZ}. Success with probability $1 - O(\varepsilon)$ in the third item ensures consistency of $\{W_{AZ}^{a,z}\}$ (resp. $\{W_{BZ}^{a,z}\}$) with the observable A (resp. B) when marginalizing over the second outcome, and Z when marginalizing over the first outcome. Using the decompositions for A, B and C derived earlier, we obtain $C_I \approx (A+B)/2$ and $C_Z \approx (A-B)/2$, giving the "Moreover" part of the lemma.

Finally, success in test $\text{COM}(X_R, C)$ certifies the approximate commutation relation $[X_R, C] \approx_{\sqrt{\varepsilon}} 0$, which, given the decomposition of X_R and C obtained so far, implies $RA \approx BR$, as desired.

A.5 Testing Clifford unitaries

Let $m \geq 1$ be an integer, and R an m-qubit Clifford unitary. R is characterized, up to phase, by its action by conjugation on the m-qubit Weyl-Heisenberg group. This action is described by linear functions $h_S : \{0,1\}^m \times \{0,1\}^m \to \mathbb{Z}_4$ and $h_X, h_Z : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^m$ such that

$$R\sigma_X(a)\sigma_Z(b)R^\dagger = (-1)^{h_S(a,b)}\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)), \qquad \forall a,b \in \{0,1\}^m. \tag{18}$$

Using that $(\sigma_X(a)\sigma_Z(b))^\dagger \,=\, (-1)^{a\cdot b}\sigma_X(a)\sigma_Z(b)$, the same condition must hold of the right-hand side of (18), thus $h_X(a,b) \cdot h_Z(a,b) = a \cdot b \mod 2$. To any family of observables $\{X(a), Z(b),\, a,b \in \{0,1\}^m\}$ we associate, for $a,b \in \{0,1\}^m$,

$$A(a,b) = i^{a\cdot b}X(a)Z(b), \qquad B(a,b) = i^{a\cdot b}X(h_X(a,b))Z(h_Z(a,b)), \tag{19}$$

where the phase $i^{a\cdot b}$ is introduced to ensure that $A(a,b)$ and $B(a,b)$ are observables. Define $C(a,b)$ in terms of $A(a,b)$ and $B(a,b)$ as in (17). The Clifford conjugation test aims to test for the conjugation relation $RA(a,b)R^\dagger = B(a,b)$, for all (in fact, on average over a randomly chosen) (a,b). For this, we first need a test that ensures $A(a,b)$ and $B(a,b)$ themselves have the correct form, in terms of a tensor product of Pauli observables. Such a test was introduced in [NV17], where it is called "Pauli braiding test". The test certifies the Pauli relations

$$\begin{aligned}
&\mathcal{P}^{(m)}\{X,Y,Z\} = \Big\{W(a) \in \mathrm{Obs},\ W \in \{X,Y,Z\}^m,\ a \in \{0,1\}^m\Big\} \\
&\quad \cup \Big\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|} W'(a')W(a),\ \forall W, W' \in \{X,Y,Z\}^n,\ \forall a, a' \in \{0,1\}^m\Big\} \\
&\quad \cup \Big\{W(a)W(a') = W(a+a'),\ \forall a, a' \in \{0,1\}^m\Big\}.
\end{aligned}$$

The Pauli braiding test is recalled in Appendix A.3, and we refer to the test as $\mathrm{PBT}(X,Y,Z)$. The original test from [NV17] only allows to test for tensor products of σ_X and σ_Z Pauli observables, and we extend the test to include Pauli σ_Y. This requires us to provide a means to accommodate the phase ambiguity discussed earlier. The result is described in the following lemma; we refer to Appendix A.3 for the proof. (In some cases a simpler variant of the test, which does not attempt to test for the Y observable, will suffice. This is essentially the original test from [NV17], which we call $\mathrm{PBT}(X,Z)$ and is introduced in Appendix A.3.)

Lemma 15. *Suppose $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_{\mathsf{A}})$, for $W \in \{X,Y,Z\}^m$ and $a \in \{0,1\}^m$, specify a strategy for the players that has success probability at least $1-\varepsilon$ in the extended Pauli braiding test $\mathrm{PBT}(X,Y,Z)$ described in Figure 15. Then there exist a state $|\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}}$ and isometries $V_D : \mathcal{H}_{\mathsf{D}} \to ((\mathbb{C}^2)^{\otimes m})_{\mathsf{D}'} \otimes \hat{\mathcal{H}}_{\hat{\mathsf{D}}}$, for $D \in \{A,B\}$, such that*

$$\big\|(V_A \otimes V_B)|\psi\rangle_{\mathsf{AB}} - |\mathrm{EPR}\rangle^{\otimes m}_{\mathsf{A}'\mathsf{B}'}|\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}}\big\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X,Y,Z\}^m$,

$$\mathop{\mathrm{E}}_{a \in \{0,1\}^m} \big\|\big(W(a) - V_A^\dagger(\sigma_W(a) \otimes \Delta_W(a))V_A\big) \otimes \mathrm{Id}_B\,|\psi\rangle\big\|^2 = O(\sqrt{\varepsilon}), \tag{20}$$

where $\Delta_W(a) = \prod_i \Delta_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{\mathsf{A}}})$ are observables with $\Delta_X = \Delta_Z = \mathrm{Id}$ and Δ_Y an arbitrary observable on $\hat{\mathcal{H}}$ such that

$$\big\|\Delta_Y \otimes \Delta_Y|\mathrm{AUX}\rangle - |\mathrm{AUX}\rangle\big\|^2 = O(\sqrt{\varepsilon}).$$

Building on the Pauli braiding test and the conjugation test from the previous section, the Clifford conjugation test $\mathrm{CONJ\text{-}CLIFF}(R)$ described in Figure 17 provides a test for the set of relations

$$\begin{aligned}
\mathcal{J}_{h_S,h_X,h_Z}\{R\} = \mathcal{P}^{(m)}&\{X,Y,Z\} \cup \{R \in \mathrm{U}\} \cup \{\Delta_Y \in \mathrm{Obs}\} \\
&\cup \big\{RX(a)Z(b)R^\dagger = \Delta_Y^{h_S(a,b)} X(h_X(a,b))Z(h_Z(a,b)),\ \forall a,b \in \{0,1\}^m\big\} \\
&\cup \big\{\Delta_Y X(a) = X(a)\Delta_Y,\ \Delta_Y Z(b) = Z(b)\Delta_Y,\ \forall a,b \in \{0,1\}^m\big\}.
\end{aligned} \tag{21}$$

Note the presence of the observable Δ_Y, which arises from the conjugation ambiguity in the definition of Y (see Lemma 15).

Test CONJ-CLIFF(R):

- Input: R an m-qubit Clifford unitary. Let h_S, h_X, h_Z be such that (18) holds, and $A(a,b), B(a,b)$ the observables defined in (19).
- Relations: $\mathcal{J}_{h_S,h_X,h_Z}\{R\}$ defined in (21).
- Test: execute each of the following with equal probability
  (a) Execute test PBT(X,Y,Z) on $(m+1)$ qubits, where the last qubit is called the "control" qubit;
  (b) Select $a,b \in \{0,1\}^m$ uniformly at random. Let $C(a,b)$ be the observable defined from $A(a,b)$ and $B(a,b)$ in (17), with the block structure specified by the control qubit. Execute test CONJ$\{A(a,b), B(a,b), R\}$. In the test, to specify query $A(a,b)$ or $B(a,b)$, represent each as a string in $\{I,X,Y,Z\}^m$ and use the same label as for the same query when it is used in part (a).

Fig. 17: The Clifford conjugation test, CONJ-CLIFF(R).

Lemma 16. *Let R be an m-qubit Clifford unitary and h_S, h_X, h_Z such that* (18) *holds. Suppose a strategy for the players succeeds with probability at least $1-\varepsilon$ in test* CONJ-CLIFF(R). *Let $V_A : \mathcal{H}_{\mathsf{A}} \to ((\mathbb{C}^2)^{\otimes(m+1)})_{\mathsf{A}'} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ be the isometry whose existence follows from part (a) of the test, and Δ_Y the observable on $\mathcal{H}_{\hat{\mathsf{A}}'}$ that represents the phase ambiguity (see Lemma 15). Then there exists a unitary Λ_R on $\mathcal{H}_{\hat{\mathsf{A}}}$, commuting with Δ_Y, such that*

$$\big\|\Lambda_R \otimes \Lambda_R|\mathrm{AUX}\rangle - |\mathrm{AUX}\rangle\big\|^2 = O(\mathrm{poly}(\varepsilon)). \tag{22}$$

Moreover, let $\hat{\tau}_R$ be any m-qubit Clifford unitary, acting on the space $(\mathbb{C}^2)^{\otimes m}$ into which the isometry V_A maps, which satisfies the relations specified in (21)*, where for any location $i \in \{1,\ldots,m\}$ such that $a_i = b_i = 1$ we replace $\sigma_X\sigma_Z$ by $\tau_Y = \sigma_Y \otimes (i\Delta_Y)$. Then, letting $\tau_R = \hat{\tau}_R(\mathrm{Id}_{\mathsf{A}'} \otimes \Lambda_R)$ we have that under the same isometry,*

$$R \simeq_{\mathrm{poly}(\varepsilon)} \tau_R.$$

Note that $\hat{\tau}_R$ is only defined up to phase in the lemma. Any representative will do, as the phase ambiguity can be absorbed in Λ_R. As an example, in this notation we have

$$\hat{\tau}_F = \frac{1}{\sqrt{2}}\big(-\sigma_X + \sigma_Y \otimes \Delta_Y\big), \qquad \hat{\tau}_G = \frac{1}{\sqrt{2}}\big(\sigma_X + \sigma_Y \otimes \Delta_Y\big), \tag{23}$$

where the "honest" single-qubit Clifford observables σ_F and σ_G are defined in (2).

Completeness of the test is clear, as players making measurements on $(m+1)$ shared EPR pairs using standard Pauli observables, R, and $C(a,b)$ defined in (17) with $A(a,b)$ and $B(a,b)$ as in (19) will pass all tests with probability 1.

Proof (Proof sketch.). For $D \in \{A, B\}$ let V_D be the isometries that follow from part (a) of the test and Lemma 15. According to (19), $A(a,b)$ and $B(a,b)$ can each be expressed (up to phase) as a tensor product of X, Y, Z operators, where the number of occurrences of Y modulo 2 is $a \cdot b$ for $A(a,b)$ and $h_X(a,b) \cdot h_Z(a,b) = a \cdot b \mod 2$ for $B(a,b)$. Thus the labels used to specify the observables in $A(a,b)$ and $B(a,b)$ in part (b), together with the analysis of part (a) and Lemma 15, imply that

$$A(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)\sigma_Z(b) \otimes (i\Delta_Y)^{a\cdot b} \text{ and } B(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes (i\Delta_Y)^{a\cdot b+h_S(a,b)},$$

under the same isometry. Applying the analysis of the conjugation test given in Lemma 14 shows that X_R must have the form in (17), for some R that approximately conjugates $A(a,b)$ to $B(a,b)$, on average over uniformly random $a, b \in \{0,1\}^m$.

Let $\hat{\tau}_R$ be as defined in the paragraph preceding the lemma. Note that $\hat{\tau}_R$ acts on $\mathcal{H}_{\mathsf{A}'}$ and $\mathcal{H}_{\hat{\mathsf{A}}}$. After application of the isometry, R has an expansion

$$R \simeq \hat{\tau}_R \cdot \Big(\sum_{a,b} \sigma_X(a)\sigma_Z(b) \otimes \Lambda_R(a,b) \Big), \tag{24}$$

for arbitrary $\Lambda_R(a,b)$ on $\mathcal{H}_{\hat{\mathsf{A}}}$; since $\hat{\tau}_R$ is invertible such an expansion exists for any operator. Using the approximate version of (18) certified by the conjugation test (Lemma 14),

$$RV_A^\dagger\big(\sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b}\big)V_A \approx V_A^\dagger\big(\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b+h_S(a,b)}\big)V_A R,$$

where the approximation holds on average over a uniformly random choice of (a,b) and up to error that is polynomial in ε but independent of m. Expanding out R and using the consistency relations between the two provers,

$$\begin{aligned}\sum_{c,d} \hat{\tau}_R \Big(\sigma_X(c)\sigma_Z(d) \otimes \Lambda_R(c,d)\Big) \otimes \Big((-1)^{a\cdot b}\sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b}\Big) \\ \approx \sum_{c,d} \Big(\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b+h_S(a,b)}\Big)\, \hat{\tau}_R \,\Big(\sigma_X(c)\sigma_Z(d) \otimes \Lambda_R(c,d)\Big) \otimes \mathrm{Id}\,,\end{aligned} \tag{25}$$

where the factor $(-1)^{a\cdot b}$ comes from using

$$\big(\sigma_X(a)\sigma_Z(b) \otimes \mathrm{Id}\,\big)|\mathrm{EPR}\rangle^{\otimes m} \;=\; \big(\,\mathrm{Id} \otimes \big(\sigma_X(a)\sigma_Z(b)\big)^T\big)|\mathrm{EPR}\rangle^{\otimes m}\,.$$

Using the conjugation relations satisfied, by definition, by $\hat{\tau}_R$, the right-hand side of (25) simplifies to

$$\sum_{c,d} \hat{\tau}_R \Big(\sigma_X(a)\sigma_Z(b)\sigma_X(c)\sigma_Z(d) \otimes \Delta_Y^{a\cdot b}\Lambda_R(c,d)\Big) \otimes \mathrm{Id}\,. \tag{26}$$

Next using the fact that the state on which the approximations are measured is maximally entangled across registers A and B, together with the Pauli (anti-)commutation relations, to simplify the left-hand side of (25), together with (26) we arrive at the approximation

$$\sum_{c,d}\Big((-1)^{a\cdot d+b\cdot c}\sigma_X(a+c)\sigma_Z(b+d)\otimes\Lambda_R(c,d)\Big)\otimes\Big(\mathrm{Id}\otimes\Delta_Y^{a\cdot b}\Big)$$
$$\approx\sum_{c,d}\Big(\sigma_X(a+c)\sigma_Z(b+d)\otimes\Delta_Y^{a\cdot b}\Lambda_R(c,d)\Big)\otimes\mathrm{Id}\,.$$

If $(c,d)\neq(0,0)$ a fraction about half of all (a,b) such that $a\cdot b=0$ satisfy $a\cdot d+b\cdot c=1$. Using that $\{\sigma_X(a)\sigma_Z(b)\otimes\mathrm{Id}\,|\mathrm{EPR}\rangle\}$ are orthogonal for different (a,b), the above then implies that $\Lambda_R(c,d)\approx-\Lambda_R(c,d)$, on average over $(c,d)\neq(0,0)$. Hence $\Lambda_R(c,d)\approx 0$, on average over $(c,d)\neq(0,0)$. Considering (a,b) such that $a\cdot b=1$ implies that $\Lambda_R(0,0)$ approximately commutes with Δ_Y. Finally, the relation (22) follows from self-consistency of X_R implicitly enforced in the test.

A.6 Tensor products of single-qubit Clifford observables

We turn to testing observables in the m-fold direct product of the Clifford group. Although the test can be formulated more generally, for our purposes it will be sufficient to specialize it to the case where each element in the direct product is an observable taken from the set $\Sigma=\{X,Y,Z,F,G\}$ associated with the single-qubit Pauli observables defined in Section 2.1. Recall that the associated operators satisfy the conjugation relation $\sigma_Y\sigma_F\sigma_Y=\sigma_G$, which will be tested as part of our procedures (specifically, item (c) in Figure 18).

Test $\textsc{cliff}(\Sigma, m)$:

- Input: An integer m and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: Select $W \in \Sigma^m$ uniformly at random. Execute each of the following with equal probability:
  (a) Execute the test $\textsc{conj-cliff}(W)$;
  (b) Send one player either the query W, or X_W and the other $(W, X(e_{m+1}))$, where e_{m+1} indicates the control qubit used for part (a). Receive one bit from the first player, and two from the second. If the query to the first player was W, check that the first player's answer is consistent with the second player's first answer bit. If the query to the first player was X_W, then: If the second player's second bit is 0, check that his first bit is consistent with the first player's; If the second player's second bit is 1, check that his first bit is different than the first player's.
  (c) Let S and T be subsets of the positions in which $W_i = F$ and $W_i = G$ respectively, chosen uniformly at random. Let W' equal W except $W'_i = G$ for $i \in S$, and $W'_i = F$ for $i \in T$. Let $R = Y(\sum_{i \in S \cup T} e_i)$. Execute test $\textsc{conj}(W, W', R)$.
  (d) Set $W'_i = X$ (resp. Y) whenever $W_i = Y$ (resp. X), $W'_i = F$ (resp. G_i) whenever $W_i = G$ (resp. F), and $W'_i = X$ whenever $W_i = Z$. Execute test $\textsc{pbt}(W, W')$ on m qubits.
  (e) Let S and T be subsets of (non-overlapping) pairs of positions in which $W_i = F$ and $W_i = G$ respectively, chosen uniformly at random. Send one player the query W, with entries $(i, j) \in S \cup T$ removed and replaced by $\Phi_{i,j}$ (indicating a measurement in the Bell basis).
    - With probability $1/2$, send the other player the query W. Check consistency of outcomes associated with positions not in $S \cup T$. For outcomes in $S \cup T$, check the natural consistency as well: e.g. if the Bell measurement indicated the outcome Φ_{00}, then the two outcomes reported by the other player at those locations should be identical.
    - With probability $1/2$, execute an independent copy of the Bell measurement test BELL (Figure 13) between the first and second players in each of the pair of qubits in $S \cup T$.

Fig. 18: The m-qubit Clifford test, $\textsc{cliff}(\Sigma, m)$.

The test is described in Figure 18. It is divided in five parts. Part (a) of the test executes $\textsc{conj-cliff}(W)$ to verify that an observable $W \in \Sigma^m$ satisfies the appropriate Pauli conjugation relations (18). Note that a priori test $\textsc{conj-cliff}(W)$ only tests for the observable X_W obtained from W in blocks as X_R from R in (17) (indeed, in that test W need not be an observable). Thus part (b) of the test is introduced to verify that $X_W \approx WX(e_{m+1})$, where the $(m+1)$-st qubit is the one used to specify the block decomposition relating X_W to W. The result of parts (a) and (b) is that, under the same isometry as used to specify the Pauli X and Z, $W \simeq \hat{\tau}_W \cdot (\mathrm{Id} \otimes \Lambda_W)$, according to the same decomposition as shown in Lemma 16. The goal of the remaining three parts of the test is to verify that $\Lambda_W = \Lambda_F^{|\{i: W_i \in \{F,G\}\}|}$, for a single observable Λ_F. For this, part (c) of the test verifies that Λ_W only depends on the locations at which $W_i \in \{F, G\}$, but not on the specific observables at those locations. Part (d) verifies that $\Lambda_W \approx \prod_{i:W_i\in\{F,G\}} \Lambda_i$ for commuting observables Λ_i. Finally, part (e) checks that Λ_i is (approximately) independent of i.

Theorem 6. *Suppose a strategy for the players succeeds in test* $\textsc{cliff}(\Sigma, m)$ *(Figure 18) with probability at least* $1-\varepsilon$*. Then for* $D \in \{A, B\}$ *there exists an isometry*

$$V_D : \mathcal{H}_{\mathsf{D}} \to (\mathbb{C}^2)^{\otimes m}_{\mathsf{D}'} \otimes \mathcal{H}_{\hat{\mathsf{D}}}$$

such that

$$\big\|(V_A \otimes V_B)|\psi\rangle_{\mathsf{AB}} - |\mathrm{EPR}\rangle^{\otimes m}_{\mathsf{A}'\mathsf{B}'}|\textsc{aux}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}}\big\|^2 = O(\sqrt{\varepsilon}), \tag{27}$$

and

$$\mathop{\mathrm{E}}_{W\in\Sigma^m,\, c\in\{0,1\}^m} \big\|\,\mathrm{Id}_A \otimes \big(V_B W(c) - \tau_W(c) V_B\big)|\psi\rangle_{\mathsf{AB}}\big\|^2 = O(\mathrm{poly}(\varepsilon)). \tag{28}$$

Here τ_W *is defined from* W *as in Lemma 16, with* $\Lambda_{W_i} = \mathrm{Id}$ *if* $W_i \in \{X, Y, Z\}$ *and* $\Lambda_{W_i} = \Lambda_F$ *if* $W_i \in \{F, G\}$*, where* Λ_F *is an observable on* $\mathcal{H}_{\hat{\mathsf{B}}}$ *that commutes with* Δ_Y.

Proof (Proof sketch). The existence of the isometry, as well as (27) and (28) for $W \in \{I, X, Y, Z\}^m$, follows from the test $\textsc{pbt}(X, Y, Z)$, executed as part of the Clifford conjugation test from part (a), and Lemma 15. Using part (a) of the test and Lemma 16 it follows that every $W \in \Sigma^m$ is mapped under the same isometry to

$$W \simeq_{\sqrt{\varepsilon}} \tau_W = \hat{\tau}_W(\mathrm{Id} \otimes \Lambda_W), \tag{29}$$

where $\hat{\tau}_W$ is as defined in the lemma and Λ_W is an observable on $\mathcal{H}_{\hat{\mathsf{A}}}$ which may depend on the whole string W; here we also use the consistency check in part (b) to relate the observable X_W used in the Clifford conjugation test with the observable W used in part (c). Note that from the definition we can write $\hat{\tau}_W = \otimes_i \hat{\tau}_{W_i}$, where in particular $\hat{\tau}_X = \sigma_X$, $\hat{\tau}_Z = \sigma_Z$ and $\hat{\tau}_Y = \sigma_Y \otimes \Delta_Y$.

The analysis of the conjugation test given in Lemma 14 shows that success with probability $1 - O(\varepsilon)$ in part (c) of the test implies the relations

$$\begin{aligned}\hat{\tau}_W \tau_R(\mathrm{Id} \otimes \Lambda_W) &= \tau_R \hat{\tau}_W(\mathrm{Id} \otimes \Lambda_W)\\ &\approx_{\sqrt{\varepsilon}} \hat{\tau}_{W'} \tau_R(\mathrm{Id} \otimes \Lambda_{W'}),\end{aligned}$$

where the first equality is by definition of R, and uses that $\tau_Y = \sigma_Y \otimes \Delta_Y$ and Δ_Y commutes with Λ_W; the approximation holds as a consequence of the conjugation test and should be understood on average over a uniformly random choice of $W \in \Sigma^m$. Thus Λ_W depends only on the locations at which $W_i \in \{F, G\}$, but not on the particular values of the observables at those locations.

Part (d) of the test and Lemma 15 imply that the observables $W(a)$ satisfy approximate linearity conditions $W(a)W(a') \approx W(a + a')$, on average over a uniformly random choice of $W \in \Sigma^n$ and $a, a' \in \{0, 1\}^n$. Using the form (29) for W and the fact that the $\hat{\tau}_W(a)$ satisfy the linearity relations by definition, we deduce that $\Lambda_{W(a)}\Lambda_{W(a')} \approx \Lambda_{W(a+a')}$ as well. Using the analysis of the Pauli braiding test (Lemma 15), this implies that for each i and W_i there is an observable Λ_{i,W_i} such that the Λ_{i,W_i} pairwise commute and $\Lambda_W \approx \prod_i \Lambda_{i,W_i}$. Using the preceding observations, $\Lambda_{i,W_i} \approx \Lambda_i$ if $W_i \in \{F,G\}$, and $\Lambda_{i,W_i} \approx \mathrm{Id}$ if $W_i \in \{X,Y,Z\}$.

Success in part (e) of the test implies the condition $\mathrm{E}_W \langle \psi | W \otimes W_\Phi | \psi \rangle \geq 1 - O(\varepsilon)$, where W is distributed as in the test, and W_Φ is the observable applied by the second player upon a query W, with some locations, indexed by pairs in S and T, have been replaced by the Φ symbol (as described in the test). Let U be the set of i such that $W_i \in \{F,G\}$. Since Δ_Y commutes with all observables in play, for clarity let us assume in the following that $\Delta_Y = \mathrm{Id}$. From the decomposition of the observables W obtained so far and the analysis of the test BELL given in Lemma 9 it follows that

$$W \simeq \Big(\otimes_i \hat{\tau}_{W_i}\Big) \otimes \Big(\prod_{i\in U} \Lambda_i\Big), \quad \text{and} \quad W_\Phi \simeq \Big(\otimes_{i\notin S\cup T} \hat{\tau}_{W_i}\Big) \otimes \Big(\otimes_{(i,j)\in S\cup T} \mathrm{SW}_{i,j}\Big) \otimes \Big(\prod_{i\in U\setminus S\cup T} \Lambda_i\Big),$$

where the ordering of tensor products does not respect the ordering of qubits, but it should be clear which registers each operator acts on. Using that for any operators A, B and Δ,

$$\langle \mathrm{EPR}|^{\otimes 2}\big(A \otimes B \otimes |\Phi_{00}\rangle\langle\Phi_{00}|\big)|\mathrm{EPR}\rangle^{\otimes 2} \;=\; \frac{1}{8}\,\mathrm{Tr}\big(AB^T\big),$$

the above conditions imply

$$\mathop{\mathrm{E}}_{S=\{(s_i,s_i')\}}\;\mathop{\mathrm{E}}_{T=\{(t_i,t_i')\}} \Lambda_{s_i}\Lambda_{s_i'}\Lambda_{t_i}\Lambda_{t_i'} \;\approx\; \mathrm{Id},$$

where the expectation is taken over sets S and T specified as in part (e), for a given W, and on average over the choice of W. Let $\Lambda = \mathrm{E}_i \Lambda_i$. By an averaging argument it follows that for U the set of locations such that $W_i \in \{F,G\}$, $\prod_{i\in U} \Lambda_i \approx \Lambda^{|S|}$, again on average over the choice of W. To conclude we let $\Lambda_F = \Lambda/|\Lambda|$, which is an observable and satisfies the required conditions.

A.7 Post-measurement states

We give a first corollary of Theorem 6 which expresses its conclusion (28) in terms of the post-measurement state of the first player. This corollary will be used in the analysis of the leash protocol from Section 4. To obtain a useful result we would like to "lift" the phase ambiguity Λ_W which remains in the statement of Theorem 6 (in contrast to the ambiguity Δ_Y, which itself cannot be lifted solely by examining correlations). This ambiguity means that the provers have the liberty of choosing to report opposite outcomes whenever they apply an F or G observable, but they have to be consistent between themselves and across all of their qubits in doing so. To verify that the provers use the "right" labeling for their outcomes we incorporate a small tomography test in the test, described in Figure 19. Note that an inconvenience of the tomography is that the test no longer achieves perfect completeness (although completeness remains exponentially close to 1).

Test $\textsc{rigid}(\Sigma, m)$:

- Input: An integer m and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: execute each of the following with equal probability:
  (a) Execute the test $\textsc{cliff}(\Sigma, m)$;
  (b) Send each player a uniformly random query $W, W' \in \Sigma^m$. Let $T \subseteq \{1, \dots, m\}$ be the subset of positions i such that $W_i \in \{X, Y\}$ and $W'_i \in \{F, G\}$. Reject if the fraction of answers (a_i, b_i), for $i \in T$, from the provers that satisfy the CHSH correlations (i.e. $a_i \neq b_i$ if and only if $(W_i, W'_i) = (X, F)$) is not at least $\cos^2 \frac{\pi}{8} - 0.1$.

Fig. 19: The n-qubit rigidity test, $\textsc{rigid}(\Sigma, m)$.

For an observable $W \in \Sigma$, let $\sigma_W = \sigma_W^{+1} - \sigma_W^{-1}$ be its eigendecomposition, where σ_W are the "honest" Pauli matrices defined in (1) and (2). For $u \in \{\pm 1\}$ let $\sigma_{W,+} = \sigma_W^u$ for $W \in \Sigma$, and

$$\sigma^u_{X,-} = \sigma^u_X, \quad \sigma^u_{Z,-} = \sigma^u_Z, \quad \sigma^u_{Y,-} = \sigma^{-u}_Y, \quad \sigma^u_{F,-} = \sigma^{-u}_G, \quad \sigma^u_{G,-} = \sigma^{-u}_F.$$

Corollary 1. *Let $\varepsilon > 0$ and m an integer. Suppose a strategy for the players succeeds with probability $1 - \varepsilon$ in test $\textsc{rigid}(\Sigma, m)$. Then for $D \in \{A, B\}$ there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)^{\otimes m}_{D'} \otimes \mathcal{H}_{\hat{D}}$$

such that

$$\big\| (V_A \otimes V_B) |\psi\rangle_{AB} - |\mathrm{EPR}\rangle^{\otimes m} \otimes |\textsc{aux}\rangle_{\hat{A}\hat{B}} \big\|^2 = O(\sqrt{\varepsilon}), \tag{30}$$

and positive semidefinite matrices τ_λ on $\hat{A}$ with orthogonal support, for $\lambda \in \{+, -\}$, such that $\mathrm{Tr}(\tau_+) + \mathrm{Tr}(\tau_-) = 1$ and

$$\mathop{\mathrm{E}}_{W \in \Sigma^m} \sum_{u \in \{\pm 1\}^m} \Big\| V_A \mathrm{Tr}_B\big((\mathrm{Id}_A \otimes W^u_B) |\psi\rangle\langle\psi|_{AB} (\mathrm{Id}_A \otimes W^u_B)^\dagger \big) V_A^\dagger - \sum_{\lambda \in \{\pm\}} \Big(\bigotimes_{i=1}^m \frac{\sigma^{u_i}_{W_i,\lambda}}{2} \Big) \otimes \tau_\lambda \Big\|_1 \tag{31}$$
$$= O(\mathrm{poly}(\varepsilon)).$$

Moreover, players employing the honest strategy succeed with probability $1 - e^{-\Omega(m)}$ in the test.

Proof. From Theorem 6 we get isometries V_A, V_B and commuting observables Δ_Y, Λ_F on $\mathcal{H}_{\hat{A}}$ such that the conclusions of the theorem hold. Write the eigendecomposition $\Delta_Y = \Delta_Y^+ - \Delta_Y^-$ and $\Lambda_F = \Lambda_F^+ - \Lambda_F^-$. For $\lambda \in \{+, -\}^2$ let

$$\tau_\lambda = \mathrm{Tr}_{\hat{B}}\big(\big(\mathrm{Id}_{\hat{A}} \otimes \Delta_Y^{\lambda_1} \Lambda_F^{\lambda_2} \big) |\textsc{aux}\rangle\langle\textsc{aux}| \big(\mathrm{Id}_{\hat{A}} \otimes \Delta_Y^{\lambda_1} \Lambda_F^{\lambda_2} \big) \big).$$

Using that Δ_Y and Λ_F commute and satisfy

$$\Delta_Y \otimes \Delta_Y |\textsc{aux}\rangle \approx \Lambda_F \otimes \Lambda_F |\textsc{aux}\rangle \approx |\textsc{aux}\rangle$$

it follows that the (sub-normalized) densities τ_λ have (approximately) orthogonal support. In particular the provers' strategy in part (b) of the test is well-approximated by a mixture of four strategies, labeled by $(\lambda_Y, \lambda_F) \in \{\pm 1\}^2$, such that the strategy with label (λ_Y, λ_F) uses the observables

$$(X, Z, Y, F, G) \;=\; \Big(\sigma_X,\, \sigma_Z,\, \lambda_Y \sigma_Y,\, \frac{1}{\sqrt{2}}\lambda_F\big(-\sigma_X + \lambda_Y \sigma_Y\big),\, \frac{1}{\sqrt{2}}\lambda_F\big(\sigma_X + \lambda_Y \sigma_Y\big)\Big).$$

Among these four strategies, the two with $\lambda_F = -1$ fail part (b) of the test with probability exponentially close to 1. Success in both parts of the test with probability at least $1 - 2\varepsilon$ each thus implies

$$\mathrm{Tr}\big(\tau_{+-}\big) + \mathrm{Tr}\big(\tau_{--}\big) \;=\; \mathrm{poly}(\varepsilon). \tag{32}$$

For $W \in \Sigma^m$ and $c \in \{0,1\}^m$ the observable $W(c) = \otimes_i W_i^{c_i}$ can be expanded in terms of a 2^m-outcome projective measurement $\{W^u\}$ as

$$W(c) = \sum_{u \in \{0,1\}^m} (-1)^{u\cdot c}\, W^u.$$

Similarly, by definition the projective measurement associated with the commuting Pauli observables $\tau_W(c) = \otimes_i \tau_{W_i}^{c_i}$, $c \in \{0,1\}^m$, is

$$\tau_W^u = \bigotimes_i \Big(\mathop{\mathrm{E}}_{c \in \{0,1\}^m} (-1)^{u\cdot c} \tau_W(c)\Big).$$

Thus,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{c \in \{0,1\}^m} \big\| \mathrm{Id}_A \otimes \big(W(c) - V_B^\dagger \tau_W(c) V_B\big) |\psi\rangle_{\mathsf{AB}} \big\|^2 \\
&\quad= \mathop{\mathrm{E}}_{c \in \{0,1\}^m} \Big\| \sum_u (-1)^{u\cdot c}\, \mathrm{Id}_A \otimes \big(W^u - V_B^\dagger \tau_W^u V_B\big) |\psi\rangle_{\mathsf{AB}} \Big\|^2 \\
&\quad= \sum_{u \in \{0,1\}^m} \big\| \mathrm{Id}_A \otimes \big(W^u - V_B^\dagger \tau_W^u V_B\big) |\psi\rangle_{\mathsf{AB}} \big\|^2,
\end{aligned} \tag{33}$$

where the third line is obtained by expanding the square and using $\mathrm{E}_{c \in \{0,1\}^m} (-1)^{v\cdot c} = 1$ if $v = 0^m$, and 0 otherwise. Using (28), the expression in (33), when averaged over all $W \in \Sigma^m$, is bounded by $O(\mathrm{poly}(\varepsilon))$. Using the Fuchs-van de Graaf inequality and the fact that trace distance cannot increase under tracing out, we get that the following is $O(\mathrm{poly}(\varepsilon))$:

$$\mathop{\mathrm{E}}_{W \in \Sigma^m} \sum_u \Big\| V_A \mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}} \otimes W^u)|\psi\rangle\langle\psi|(\mathrm{Id}_{\mathsf{A}} \otimes W^u)^\dagger\big) V_A^\dagger - \mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}} \otimes \tau_W^u)|\psi\rangle\langle\psi|(\mathrm{Id}_{\mathsf{A}} \otimes \tau_W^u)^\dagger\big) \Big\|_1. \tag{34}$$

Using that $\tau_X = \sigma_X$, $\tau_Z = \sigma_Z$, and $\tau_Y = \sigma_Y \Delta_Y$, we deduce the post-measurement states for $u \in \{\pm 1\}$

$$\tau_X^u = \sigma_X^u, \qquad \tau_Z^u = \sigma_Z^u, \qquad \tau_Y^u = \sigma_Y^u \otimes (\tau_{++} + \tau_{+-}) + \sigma_Y^{-u} \otimes (\tau_{-+} + \tau_{--}).$$

Similarly, from $\tau_F = (-\tau_X + \tau_Y)\Lambda_F$ and $\tau_G = (\tau_X + \tau_Y)\Lambda_F$ we get that e.g. the $+1$ eigenspace of τ_F is the combination of:

- The simultaneous $+1$ eigenspace of $\sigma_F = (-\sigma_X + \sigma_Y)/\sqrt{2}$, $+1$ eigenspace of Δ_Y, and $+1$ eigenspace of Λ_F;
- The simultaneous -1 eigenspace of σ_F, $+1$ eigenspace of Δ_Y, and -1 eigenspace of Λ_F;
- The simultaneous -1 eigenspace of $\sigma_G = -(-\sigma_X - \sigma_Y)/\sqrt{2}$, -1 eigenspace of Δ_Y, and $+1$ eigenspace of Λ_F;
- The simultaneous $+1$ eigenspace of σ_G, -1 eigenspace of Δ_Y, and -1 eigenspace of Λ_F.

Proceeding similarly with τ_G, we obtain

$$\tau_F^u = \sigma_F^u \otimes \tau_{++} + \sigma_F^{-u} \otimes \tau_{+-} + \sigma_G^{-u} \otimes \tau_{-+} + \sigma_G^u \otimes \tau_{--},$$
$$\tau_G^u = \sigma_G^u \otimes \tau_{++} + \sigma_G^{-u} \otimes \tau_{+-} + \sigma_F^{-u} \otimes \tau_{-+} + \sigma_F^u \otimes \tau_{--}.$$

Starting from (34) and using (27) we obtain

$$\mathop{\mathrm{E}}_{W\in\Sigma^m} \sum_u \Big\| V_A \mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}} \otimes W^u)|\psi\rangle\langle\psi|(\mathrm{Id}_{\mathsf{A}} \otimes W^u)^\dagger\big) V_A^\dagger - \mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}} \otimes \tau_W^u)|\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes m} \otimes |\textsc{aux}\rangle\langle\textsc{aux}|_{\hat{\mathsf{A}}\hat{\mathsf{B}}}(\mathrm{Id}_{\mathsf{A}} \otimes \tau_W^u)^\dagger\big)\Big\|_1 = O(\mathrm{poly}(\varepsilon)).$$

Since $\mathrm{Tr}_{\mathsf{B}}(\mathrm{Id} \otimes B|\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{AB}}\,\mathrm{Id} \otimes B^\dagger) = (B^\dagger B)^T/2$ for any single-qubit operator B, to conclude the bound claimed in the theorem it only remains to apply the calculations above and use (32) to eliminate the contribution of τ_{+-} and τ_{--}; the factor $\frac{1}{2}$ comes from the reduced density matrix of an EPR pair.

A.8 Tomography

Theorem 6 and Corollary 1 show that success in test $\textsc{rigid}(\Sigma, m)$ gives us control over the players' observables and post-measurement states in the test. This allows us to use one of the players to perform some kind of limited tomography (limited to post-measurement states obtained from measurements in Σ), that will be useful for our analysis of the Dog-Walker Protocol from Section B.

Let $1 \le m' \le m$ and consider the test $\textsc{tom}(\Sigma, m', m)$ described in Figure 20. In this test, one player is sent a question $W \in \Sigma^m$ chosen uniformly at random. Assuming the players are also successful in the test $\textsc{rigid}(\Sigma, m)$ (which can be checked independently, with some probability), using that the input distribution μ in $\textsc{rigid}(\Sigma, m)$ assigns weight at least $|\Sigma|^{-m}/2$ to any $W' \in \Sigma^m$, from Corollary 1 it follows that the second player's post-measurement state is close to a state consistent with the first player's reported outcomes. Now suppose the second player is sent a random subset $S \subseteq [m]$ of size $|S| = m'$, and is allowed to report an arbitrary string $W' \in \Sigma^{m'}$, together with outcomes u. Suppose also that for each $i \in S$, we require that $u_i = a_i$ whenever $W'_i = W_i$. Since the latter condition is satisfied by a constant fraction of $i \in \{1, \ldots, m'\}$, irrespective of W', with very high probability, it follows that the only possibility for the second player to satisfy the condition is to actually measure his qubits precisely in the basis that he indicates. This allows us to check that a player performs the measurement that he claims, even if the player has the choice of which measurement to report.

Tomography Test $\textsc{tom}(\Sigma, m', m)$:

- Input: Integer $1 \le m' \le m$ and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: Let $S \subseteq [m]$ be chosen uniformly at random among all sets of size $|S| = m'$. Select $W \in \Sigma^m$ uniformly at random. Send W to the first player, and the set S to the second. Receive a from the first player, and $W' \in \Sigma^{m'}$ and u from the second. Accept only if $a_i = u_i$ whenever $i \in S$ and $W_i = W'_i$.

Fig. 20: The m-qubit tomography test $\textsc{tom}(\Sigma, m', m)$.

Corollary 2. *Let $\varepsilon > 0$ and $1 \le m' \le m$ integer. Suppose a strategy for the players succeeds with probability $1-\varepsilon$ in both tests $\textsc{rigid}(\Sigma, m)$ (Figure 19) and $\textsc{tom}(\Sigma, m', m)$ (Figure 20). Let V_A, V_B be the isometries specified in Corollary 1. Let $\{Q^{W',u}\}$ be the projective measurement applied by the second player in $\textsc{tom}(\Sigma, m', m)$. Then there exists a distribution q on $\Sigma^{m'} \times \{\pm\}$ such that*

$$\sum_{W' \in \Sigma^{m'}} \sum_{u \in \{\pm 1\}^{m'}} \Big\| \mathrm{Tr}_{\mathsf{A}\hat{\mathsf{B}}}\big((\mathrm{Id}_A \otimes V_B Q^{W',u})|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_A \otimes V_B Q^{W',u})^\dagger\big) - \sum_{\lambda \in \{\pm\}} q(W', \lambda)\Big(\bigotimes_{i=1}^{m'} \frac{1}{2}\sigma^{u_i}_{W'_i,\lambda}\Big)\Big\|_1 = O(\mathrm{poly}(\varepsilon)),$$

where the notation is the same as in Corollary 1.

Moreover, players employing the honest strategy succeed with probability 1 in tomography part of the test.

Proof. Success in $\textsc{rigid}(\Sigma, m)$ allows us to apply Corollary 1. For any (W', u) let $\rho^{W',u}_{\mathsf{A'},\lambda}$ be the post-measurement state on the first player's space, conditioned on the second player's answer in test $\textsc{tom}(\Sigma, m', m)$ being (W', u), after application of the isometry V_A, and conditioned on $\mathcal{H}_{\hat{\mathsf{A}}}$ being in a state that lies in the support of τ_λ (note this makes sense since τ_+, τ_- have orthogonal support). Using that for any $i \in S$, $W_i = W'_i$ with constant probability $|\Sigma|^{-1}$, it follows from (30) and (31) in Corollary 1 that success in $\textsc{tom}(\Sigma, m)$ implies the condition

$$\mathop{\mathrm{E}}_{\substack{S \subseteq \{1,\dots,m\} \\ |S| = m'}} \sum_{W',\lambda,u} \mathrm{Tr}(\tau_\lambda)\,\mathrm{Tr}\Big(\Big(\frac{|\Sigma|-1}{|\Sigma|}\,\mathrm{Id} + \frac{1}{|\Sigma|} \otimes_{i\in S} \sigma^{u_i}_{W'_i,\lambda}\Big)\rho^{W',u}_{\mathsf{A'},\lambda}\Big) = 1 - O(\mathrm{poly}(\varepsilon)). \tag{35}$$

Eq (35) concludes the proof, for some distribution $q(W', \lambda) \approx \sum_u \mathrm{Tr}(\rho^{W',u}_{\mathsf{A'},\lambda})\mathrm{Tr}(\tau_\lambda)$ (the approximation is due to the fact that the latter expression only specifies a distribution up to error $O(\mathrm{poly}(\varepsilon))$.

B The Dog-Walker Protocol

B.1 Protocol and statement of results

Throughout this section we let $\Sigma = \{X, Y, Z, F, G\}$, and let $m = \Theta(n+t)$ be chosen large enough so that each symbol in Σ appears at least $n+t$ times in a uniform random $W \in \Sigma^m$, with probability close to 1. Let $\mu(W)$ denote the probability that a player receives input W while playing $\text{RIGID}(\Sigma, m)$ (recall that both players have the same marginals in RIGID). Let $\mu(W'|W)$ denote the probability that one player receives W' given that the other player receives W.

The full protocols are presented in Figure 21 (verifier's point of view), Figure 23 (PV's point of view) and Figure 22 (PP's point of view). The protocol has two types of rounds: EPR and Rigidity. Within an EPR round are three types of sub-rounds: Computation sub-round, X-test sub-round, and Z-test sub-round. We will generally think of X- and Z-test sub-rounds as one sub-round type (Test sub-round). Within a Rigidity round are two types of sub-rounds: Tomography sub-round, which should be thought of as the Rigidity version of the EPR-Computation round; and Clifford sub-round, which should be thought of as the Rigidity version of the EPR-Test round. With some probability p_1, V runs a Rigidity round, Clifford sub-round; with some probability p_2, V runs an EPR round, Test sub-round; with some probability p_3, V runs an EPR round, Computation sub-round; and with probability $p_4 = 1 - p_1 - p_2 - p_3$, V runs a Rigidity round, Tomography sub-round. We call this the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4).

The following theorem states the guarantees of the Dog-Walker Protocol.

Theorem 7. *There exist constants p_1, p_2, p_3, $p_4 = 1 - p_1 - p_2 - p_3$, and $\Delta > 0$ such that the following hold of the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4), when executed on input $(Q, |\boldsymbol{x}\rangle)$.*

- *(Completeness:) Suppose that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for* PV *and* PP *that is accepted with probability at least $p_{\text{compl}} = p_1(1 - e^{-\Omega(n+t)}) + p_2 + \frac{2}{3}p_3 + p_4$.*
- *(Soundness:) Suppose that $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \leq 1/3$. Then any strategy for* PV *and* PP *is accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

The proof of completeness is given in Lemma 17, and proof of soundness is given in Lemma 22.

1. Select a round type **EPR** or **Rigidity**, and disjoint sets $N, T^0, T^1 \subset \{1, \ldots, m\}$ of sizes n, t_0 and $t - t_0$.

EPR Choose $\boldsymbol{z}$ uniformly at random from $\{0,1\}^t$ and send it, along with N, T^0 and T^1, to PP. Receive measurement outcomes $\boldsymbol{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ from PP.

Rigidity Choose W' according to $\mu(\cdot)$ and send it to PP. Receive $\boldsymbol{e}' \in \{0,1\}^m$ from PP.

2. Select a sub-round type at random from **Computation**, **X Test** or **Z Test**.

Computation Based on whether it's an EPR or a Rigidity Round:

EPR (i) Send $\boldsymbol{x}$, $\boldsymbol{z}$, $\boldsymbol{c}$ and sets N, T^0 and T^1 to PV, and receive measurement outcomes $\boldsymbol{a}, \boldsymbol{b} \in \{0,1\}^n$ and $\boldsymbol{e} \in \{0,1\}^t$.

(ii) Apply the update rules from Table 2 gate-by-gate to obtain the final X key for the output wire a'_f. If $c_f + a'_f \neq 0$, reject.

Rigidity (Tomography) (i) Choose uniform random strings $\boldsymbol{c}, \boldsymbol{z} \in \{0,1\}^t$, $\boldsymbol{x} \in \{0,1\}^n$ to send to PV, along with N and T, and receive measurement outcomes $\boldsymbol{d} \in \{0,1\}^n$ and $\boldsymbol{e} \in \{0,1\}^t$.

(ii) From $\boldsymbol{x}$, $\boldsymbol{c}$, $\boldsymbol{z}$, $\boldsymbol{d}$, and $\boldsymbol{e}$, determine the adaptive measurements $W \in \Sigma^{n+t}$ that V^0_{EPR} would have performed (based on Figure 3b), and reject if the input-output pairs $(W', \boldsymbol{e}')$ and $(N \cup T, (W, \boldsymbol{e}))$ do not satisfy the winning criterion for $\textsc{tom}(\Sigma, n+t, m)$.

X**-Test** Based on whether it's an EPR or a Rigidity Round:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = Z$ for all $i \in N$; $W_i = Z$ for all $i \in T^0$; and $W_i \in \{X, Y\}$ for all $i \in T^1$. Send W to PV and receive measurement results $\boldsymbol{e} \in \{0,1\}^m$. Let $(\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{e}_N, 0^n)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$ the X key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $\exists i$ s.t. the i-th T gate is even and $c_i \neq a'_i + e_i$, reject. If $c_f + a'_f \neq 0$, reject.

Rigidity (Clifford) Choose W according to the marginal conditioned on W', $\mu(\cdot|W')$. Send W to PV and receive $\boldsymbol{e} \in \{0,1\}^m$. Reject if $(W', \boldsymbol{e}', W, \boldsymbol{e})$ doesn't win $\textsc{rigid}(\Sigma, m)$.

Z**-Test** Based on whether it's an EPR or a Rigidity Round:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = X$ for all $i \in N$; $W_i \in \{X, Y\}$ for all $i \in T^0$; and $W_i = Z$ for all $i \in T^1$. Send W to PV and receive measurement results $\boldsymbol{e} \in \{0,1\}^m$. Let $(\boldsymbol{a}, \boldsymbol{b}) = (0^n, \boldsymbol{e}_N)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$, the X key before the i-th T gate is applied, a'_i. If $\exists i$ s.t. the i-th T gate is odd and $c_i \neq a'_i + e_i$, reject.

Rigidity (Clifford) Identical to X-Test case.

Fig. 21: The Dog-Walker Protocol: Verifier's point of view.

1. If PP receives a question W' from V (he is playing TOM or RIGID):
   Measure the m qubits in the observable indicated by W' — for example, if $W' \in \Sigma^m$, for $i \in \{1,\dots,m\}$, measure the i-th qubit in the basis indicated by W'_i — and report the outcomes $\boldsymbol{e}'$ to V.
2. If PP receives $\boldsymbol{z}$, and sets N, T^0 and T^1 from V (he is playing the role of P_{EPR} from the EPR Protocol):
   Run the prover P_{EPR} from Figure 3c on input $\boldsymbol{z}$, the n qubits in N, and the t qubits in $T^0 \cup T^1$. Report the outputs $\boldsymbol{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ of P_{EPR} to V.

Fig. 22: The Dog-Walker Protocol: Honest strategy for PP.

1. If PV receives a question W from V (he is playing RIGID or an X- or Z-Test Round):
   Measure the m qubits in the observable indicated by W — for example, if $W \in \Sigma^m$, for $i \in \{1,\dots,m\}$, measure the i-th qubit in the basis indicated by W_i — and report the outcomes $\boldsymbol{e}$ to V.
2. If PV receives $\boldsymbol{x}$, $\boldsymbol{z}$, $\boldsymbol{c}$ and sets N, T^0 and T^1 from V (he is playing TOM or a Computation Round):
   Run the procedure V^0_{EPR} from Figure 3b on input $\boldsymbol{x}$, $\boldsymbol{c}$, $\boldsymbol{z}$, the n qubits in N, and the t qubits in $T^0 \cup T^1$. Report the outputs $\boldsymbol{d}$ and $\boldsymbol{e}$ of V^0_{EPR} to V.

Fig. 23: The Dog-Walker Protocol: Honest strategy for PV.

B.2 Completeness

Lemma 17. *Suppose* V *executes the Dog-Walker Protocol with parameters* (p_1, p_2, p_3, p_4). *There is a strategy for the provers such that, on any input* $(Q, |\boldsymbol{x}\rangle)$ *such that* $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \geq \frac{2}{3}$, V *accepts with probability at least* $p_{\text{compl}} = p_1(1-\delta_c) + p_2 + \frac{2}{3}p_3 + p_4$, *for some* $\delta_c = e^{-\Omega(n+t)}$.

Proof. The provers PV and PP play the strategy described in Figures 23 and 22 respectively. In the Rigidity-Tomography round, the verification performed by V amounts to playing TOM$(\Sigma, n+t, m)$ with the provers (with an extra constraint on the output W of PV that is always satisfied by the honest strategy). This game has perfect completeness, which makes the V accept with probability 1 in the Rigidity-Tomography round. In the Rigidity-Clifford round, V plays RIGID(Σ, m) with the provers. The game has completeness at least $1-\delta_c$ for some $\delta_c = e^{-\Omega(n+t)}$, since $m = \Omega(n+t)$, therefore their success probability in this round is at least $1-\delta_c$.

In the EPR round, the provers are exactly carrying out the EPR Protocol, with V using PV to run V^r_{EPR}, and PP playing the role of P_{EPR}. Thus, test rounds result in acceptance with probability 1, and the computation round results in acceptance with probability $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2$, by Theorem 2.

B.3 Soundness

Figure 10 summarizes the high-level structure of the soundness analysis. Intuitively, our ultimate goal is to argue that both provers either apply the correct operations in EPR-Computation rounds, or are rejected with constant probability. This will be achieved by employing a form of "hybrid argument" whereby it is argued that the provers, if they are not caught, must be using the honest strategies described in Figure 22 and Figure 23 in the different types of rounds considered in the protocol. Towards this, we divide the round types into the following four scenarios:

1. Rigidity-Clifford: The round type is **Rigidity** and the sub-round type is either X**-Test** or Z**-Test**. (When the provers are honest) PV behaves as in Item 1 of Figure 23, and PP behaves as in Item 1 of Figure 22.
2. EPR-Test: The round type is **EPR** and the sub-round type is either X**-Test** or Z**-Test**. PV behaves as in Item 1 of Figure 23, and PP behaves as in Item 2 of Figure 22.
3. EPR-Computation: The round type is **EPR** and the sub-round type is **Computation**. PV behaves as in Item 2 of Figure 23, and PP behaves as in Item 2 of Figure 22.
4. Rigidity-Tomography: The round type is **Rigidity** and the sub-round type is **Computation**. PV behaves as in Item 2 of Figure 23, and PP behaves as in Item 1 of Figure 22.

Examining Figure 21, we can see the following. In the Rigidity-Clifford scenario, the verifier is precisely playing the game RIGID with the provers, as the provers receive questions W' and W distributed according to $\mu(\cdot,\cdot)$, the distribution of questions for RIGID(Σ, m); their answers are tested against the winning conditions of RIGID(Σ, m). In the Rigidity-Tomography scenario, the verifier plays a variant of the game TOM with the provers, in which PV's choice of observable W is uniquely determined by his inputs $\boldsymbol{x}$, $\boldsymbol{c}$ and $\boldsymbol{z}$: it should match the observable implemented by V_{EPR}^{0} on these inputs. In EPR rounds, PV plays the part of V_{EPR}^{r} from the EPR Protocol, and PP play the part of P_{EPR}. The EPR-Test scenario corresponds to X- and Z-tests from the EPR Protocol, whereas the EPR-Computation scenario corresponds to computation rounds from the EPR Protocol.

The structure of the proof is as follows (see also Figure 10):

(i) By the game RIGID, in the Rigidity-Clifford rounds, both PP and PV must be honest, or they would lose the game.
(ii) Since PV can't distinguish between Rigidity-Clifford and EPR-Test (both are Figure 23 Item 1 from his perspective, and the input distributions, while not identical, are within constant total variation distance), PV must be honest in the EPR-Test rounds, by (i).
(iii) Since PP can't distinguish between Rigidity-Clifford and Rigidity-Tomography (both are Figure 22 Item 1 from his perspective), PP must be honest in the Rigidity-Tomography rounds, by (i).
(iv) Since PV is honest in EPR-Test rounds by (ii), PP must be honest in EPR-Test rounds or he will get caught, but in particular, he must output values $\{c_i\}_{i\in[t]}$ that

are uniform random and independent of z. Since PP can't distinguish between EPR-Test and EPR-Computation rounds, this is also true in EPR-Computation rounds, when the verifier sends the values $\{c_i\}_i$ to PV.

(v) PV must be honest in Rigidity-Tomography rounds, or the provers would lose the game TOM.

(vi) Since PV can't distinguish between Rigidity-Tomography rounds and EPR-Computation rounds (both are Figure 23 Item 2 from his perspective), PV must be honest in EPR-Computation rounds, by (v), and his input distribution to both rounds is within constant total variation distance, by (iv).

(vii) Since PV is honest in EPR-Test rounds by (ii), and EPR-Computation rounds by (vi), the combined behavior of V and PV in the EPR rounds is that of V_{EPR} in the EPR Protocol, so by the soundness of the EPR Protocol, PP must be honest in EPR-Computation rounds, or get caught in the EPR-Test rounds with high probability.

The following lemma establishes (i), (ii) and (iii).

Lemma 18. *Suppose the verifier executes the Dog-Walker Protocol with provers* $(\mathrm{PV}^*, \mathrm{PP}^*)$ *such that the provers are accepted with probability* $q_1 \geq 1 - \varepsilon$ *in the Rigidity-Clifford Round,* q_2 *in the EPR-Test Round,* q_3 *in the EPR-Computation Round, and* q_4 *in the Rigidity-Tomography Round. Then there exist provers* $(\mathrm{PV}', \mathrm{PP}')$ *such that:*

- PV' *and* PP' *both apply the honest strategy in the Rigidity-Clifford rounds,* PV' *applies the honest strategy in the EPR-Test rounds, and* PP' *applies the honest strategy in the Rigidity-Tomography rounds; in particular, the state shared by the provers at the beginning of the protocol is a tensor product of the honest state consisting of* m *shared EPR pairs and an arbitrary shared ancilla;*
- *The provers are accepted with probability* $q_2' = q_2 - O(\mathrm{poly}(\varepsilon))$ *in the EPR-Test Round,* $q_3' = q_3$ *in the EPR-Computation Round, and* $q_4' = q_4 - O(\mathrm{poly}(\varepsilon))$ *in the Rigidity-Tomography Round.*

Proof. Using a similar argument as in Lemma 3, the strategy of PV^* in Rigidity-Clifford rounds, which is also his strategy in EPR-Test rounds (Figure 23 Item 1); and the strategy of PP^* in Rigidity-Clifford rounds, which is also his strategy in Rigidity-Tomography rounds (Figure 22 Item 1); can both be replaced with the honest strategies. Since the distribution of inputs to PP^* in the Rigidity-Tomography rounds and Rigidity-Clifford rounds is the same, the success probability in the Rigidity-Tomography rounds is changed by at most $O(\mathrm{poly}(\varepsilon))$ by using the honest strategy. On the other hand, PV^*'s input distribution in EPR-Test rounds is uniform on Σ^m, whereas his distribution in Rigidity-Clifford rounds is given by μ. However, from the description of the test RIGID it is clear that for all $W \in \Sigma^m$, $\mu(W) \geq \frac{1}{c|\Sigma|^m}$ for some constant $c > 1$, thus the total variation distance between the two distributions is at most $1 - \frac{1}{c}$. Thus, replacing PV^* with the honest strategy in the EPR-Test rounds will change the success probability by at most $O(\mathrm{poly}(\varepsilon))$.

Finally, since the provers' strategy in the EPR-Computation round has not changed, the acceptance probability in it remains unchanged.

Next, we will show that whenever PV^* is honest in the EPR-Test rounds this forces PP^* to output (close to) uniformly random $\{c_i\}_{i\in[t]}$ that are independent of the round type, even given $\boldsymbol{z}$. This will allow us to verify that PP* is unable to signal to PV* whether the round is an EPR Round in the EPR-Computation round, when PV* is sent $\boldsymbol{z}$ and $\boldsymbol{c}$. This establishes (iv).

Lemma 19. *Suppose the verifier executes the Dog-Walker Protocol with provers* $(\mathrm{PV}^*, \mathrm{PP}^*)$ *such that the initial shared state of the provers consists of* m *shared EPR pairs, together with an arbitrary shared auxiliary state;* PV* *plays the honest strategy in the EPR-Test rounds; the provers are accepted with probability* q_1 *in the Rigidity-Clifford Round,* $q_2 = 1 - \varepsilon'$ *in the EPR-Test Round,* q_3 *in the EPR-Computation Round, and* q_4 *in the Rigidity-Tomography Round. Then the input* $(\boldsymbol{c}, \boldsymbol{z})$ *given by the verifier to* PV* *in the EPR-Computation rounds has a distribution that is within* $O(\varepsilon')$ *total variation distance of uniform on* $\{0,1\}^t \times \{0,1\}^t$.

Proof. Let a'_i denote the X key of the wire to which the i-th T gate is applied, just before the i-th T is applied, and let D_i be a random variable defined as follows. If the i-th T gate is even, let $D_i = e_i + a'_i$, where we interpret e_i and a'_i as the random variables representing the measurement result and key V would get if she chooses to execute an X-Test round. If the i-th T gate is odd, let $D_i = e_i + a'_i$, where we interpret e_i and a'_i as the measurement result and key V would get if she chooses to execute an Z-Test round. Since PV* is assumed to play honestly in EPR-Test rounds, $\boldsymbol{D}$ is uniformly distributed in $\{0,1\}^t$. In particular, we have, for any $\boldsymbol{d}, \boldsymbol{z} \in \{0,1\}^t$,

$$\Pr[\boldsymbol{D} = \boldsymbol{d}, \boldsymbol{Z} = \boldsymbol{z}] = \frac{1}{4^t}. \tag{36}$$

Let C_i be the random variable that corresponds to the measurement output of the i-th T gadget by PP* in X-Test round if the i-th T gate is even, or the measurement output of the i-th T gadget by PP* in Z-Test round if the i-th T gate is odd.

Let $T^0 \subset [t]$ be the set of even T gates and $T^1 \subset [t]$ the set of odd T gates. In an X-Test Round, the provers are rejected whenever $i \in T^0$ and $c_i \neq d_i$, and in a Z-Test Round, they are rejected whenever $i \in T^1$ and $c_i \neq d_i$. An EPR-Test Round consists of running one of these two rounds with equal probability, so:

$$\Pr[\boldsymbol{C} \neq \boldsymbol{D}] \leq 2\varepsilon'. \tag{37}$$

We can express (37) as

$$\Pr[(\boldsymbol{C}, \boldsymbol{Z}) \neq (\boldsymbol{D}, \boldsymbol{Z})] \leq 2\varepsilon'.$$

We conclude by using the easily verifiable fact that for any random variables X and Y such that $\Pr[X = Y] \geq 1 - 2\varepsilon'$, the total variation distance between the marginal distributions on X and Y is at most $2\varepsilon'$.

Next, we can use the tomography test TOM to establish (v), and then the fact that by Lemma 19 the input to PV is not very different in EPR-Computation and Rigidity-Tomography rounds to establish (vi):

Lemma 20. *Suppose the verifier executes the Dog-Walker Protocol with provers* $(\mathrm{PV}^*, \mathrm{PP}^*)$ *such that:* PV* *applies the honest strategy in EPR-Test rounds;* PP* *applies the honest* *strategy in the Rigidity-Tomography rounds; and the provers are accepted with probability q_1 in the Rigidity-Clifford Round, $q_2 = 1-\varepsilon'$ in the EPR-Test Round, q_3 in the EPR-Computation Round, and $q_4 = 1-\varepsilon$ in the Rigidity-Tomography Round. Then there exist provers $(\mathrm{PV}', \mathrm{PP}')$ such that PV' applies the honest strategy in the Rigidity-Tomography rounds and EPR-Computation rounds, PP' applies the honest strategy in Rigidity-Tomography rounds, and the provers are accepted with probability q_1 in the Rigidity-Clifford Round, $q_2 = 1-\varepsilon'$ in the EPR-Test Round and $q_3 - \mathrm{poly}(\varepsilon) - O(\varepsilon')$ in the EPR-Computation round.*

Proof. The Rigidity-Tomography rounds can be seen as V playing the Tomography Game with the provers, except that whereas PV* gets no non-trivial input in the Tomography Game, in the Rigidity-Tomography round, he gets random values $\boldsymbol{c}$ and $\boldsymbol{z}$ on which his strategy can depend. Fix $\boldsymbol{x}$, and let $\{Q^u_{\boldsymbol{c},\boldsymbol{z}}\}_u$ be the projective measurement that PV* applies upon receiving $\boldsymbol{c}, \boldsymbol{z}, \boldsymbol{x}$, where $u = (\boldsymbol{d}, \boldsymbol{e})$ is the string of outcomes obtained by PV on the $n+t$ single-qubit measurements he is to perform according to Step 2 in Figure 23.

By Corollary 2, since the provers win the Rigidity-Tomography round with probability $1-\varepsilon$, for every $\boldsymbol{c}, \boldsymbol{z} \in \{0,1\}^t$, there exist distributions $q_{\boldsymbol{c},\boldsymbol{z}}$ on $\Sigma^m \times \{\pm\}$ such that the following is $O(\mathrm{poly}(\varepsilon))$:

$$\mathop{\mathrm{E}}_{\boldsymbol{c},\boldsymbol{z}} \sum_{u\in\{0,1\}^m} \left\| \mathrm{Tr}_{\mathsf{A},\hat{\mathsf{B}}} \Big((\mathrm{Id}_{\mathsf{A}} \otimes V_{\mathsf{B}} Q^u_{\boldsymbol{c},\boldsymbol{z}}) |\psi\rangle\langle\psi|_{\mathsf{AB}} (\mathrm{Id}_{\mathsf{A}} \otimes V_{\mathsf{B}} Q^u_{\boldsymbol{c},\boldsymbol{z}})^\dagger \Big) - \sum_{\lambda\in\{\pm\}} q_{\boldsymbol{c},\boldsymbol{z}}(W', \lambda) \left(\bigotimes_{i=1}^m \frac{\sigma^{u_i}_{W'_i,\lambda}}{2} \right) \right\|_1 . \tag{38}$$

Here we use the notation from Corollary 1 and 2. The string $W' = W(\boldsymbol{c}, \boldsymbol{z}, \boldsymbol{u}) \in \Sigma^m$ is uniquely determined by $\boldsymbol{c}, \boldsymbol{z}$, and the outcomes u reported by PV*; indeed it is using this string that PV*'s answers are checked against the measurement outcomes obtained by PP*, who by assumption applies the honest strategy. For any fixed (W', λ) the distribution on outcomes u obtained in the "honest" strategy represented by the right-hand side in (38) is uniform. Thus the outcomes u reported by PV* are within $\mathrm{poly}(\varepsilon)$ of uniform. From this it follows that the joint distribution on transcripts $(\boldsymbol{c}, \boldsymbol{z}, u, W' = W(\boldsymbol{c}, \boldsymbol{z}, u))$ that results from an interaction with PV* is within statistical distance $\mathrm{poly}(\varepsilon)$ of the distribution generated by an interaction with the honest PV; furthermore, by (38) the resulting post-measurement states on PP* are also $\mathrm{poly}(\varepsilon)$ close to the honest ones, on average over this distribution.

We can now consider two provers PV$'$ and PP$'$ who, in Rigidity-Tomography rounds, first apply the isometries V_A, V_B from Corollary 2, then measure their auxiliary systems $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ using Δ_Y, obtaining a shared outcome $\lambda \in \{\pm\}$, and finally apply the honest strategy shown in Item 2 of Figure 23 ($\lambda = +$) or its conjugate ($\lambda = -$). Furthermore, conjugating the honest strategy produces exactly the same statistics as the honest strategy itself, so we may in fact assume that PV$'$ and PP$'$ both apply the honest strategy in Rigidity-Tomography rounds.

A consequence of PV$'$ applying the honest strategy in Figure 23 Item 2 is that PV$'$ also plays the honest strategy in EPR-Computation rounds. Since PV$'$ is still honest in the EPR-Test round and $q_2 = 1-\varepsilon'$, Lemma 19 implies that the distribution of the input to PV$'$ in EPR-Computation rounds is within $\mathrm{poly}(\varepsilon) + O(\varepsilon')$ total variation distance of his input in Rigidity-Tomography rounds, therefore the provers' success probability in EPR-Computation rounds changes at most by $\mathrm{poly}(\varepsilon) + O(\varepsilon')$.

Finally, we show that if PV is honest, PP must be honest in EPR computation rounds, or the acceptance probability would be low, establishing (vii):

Lemma 21. *Suppose* V *executes the Dog-Walker Protocol on an input* $(Q, |\boldsymbol{x}\rangle)$ *such that* $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \leq 1/3$*, with provers* $(\mathrm{PV}, \mathrm{PP})$ *such that* PV *plays the honest strategy. Let* q_2 *be the provers' acceptance probability in EPR-Test rounds. Then the verifier accepts with probability at most* $p_1(1-\delta_c) + p_2 q_2 + p_3(5/3 - 4q_2/3) + p_4$.

Proof. With probability $p_2 + p_3$, V executes an EPR round, in which case, he executes EPR-Computation with probability $\frac{p_3}{p_2+p_3}$ and EPR-Test with probability $\frac{p_2}{p_2+p_3}$. In the former case, since PV is honest, he is executing V^0_{EPR}. In fact, the behavior of an honest PV in the EPR-Test rounds is also that of V^r_{EPR}. Thus, the combined behavior of V and PV is that of V_{EPR}. Then the result follows from Theorem 3.

We can now combine Lemmas 18, 20, and 21 to get the main result of this section, the "soundness" part of Theorem 7.

Lemma 22 (Constant soundness-completeness gap). *There exist constants* p_1*,* p_2*,* p_3*,* $p_4 = 1 - p_1 - p_2 - p_3$ *and* $\Delta > 0$ *such that if the verifier executes the Dog-Walker Protocol with parameters* (p_1, p_2, p_3, p_4) *on input* $(Q, |\boldsymbol{x}\rangle)$ *such that* $\|\Pi_0 Q|\boldsymbol{x}\rangle\|^2 \leq 1/3$*, then any provers* $(\mathrm{PV}^*, \mathrm{PP}^*)$ *are accepted with probability at most* $p_{\mathrm{sound}} = p_{\mathrm{compl}} - \Delta$.

Proof. Suppose the provers PV^* and PP^* are such that the lowest acceptance probability in either the Rigidity-Clifford round or the Rigidity-Tomography round is $1 - \varepsilon$, and they are accepted with probability $1 - \varepsilon'$ in the EPR-Test round, and with probability $1/3 + w$ in the Computation Round. Applying Lemma 18 and Lemma 20 in sequence, we deduce the existence of provers $(\mathrm{PV}', \mathrm{PP}')$ for which

$$\begin{aligned}
q_1' &= 1 - O(\delta_c), \\
q_2' &= 1 - \varepsilon' - \mathrm{poly}(\varepsilon), \\
q_3' &= \frac{1}{3} + w - \mathrm{poly}(\varepsilon) - O(\varepsilon'), \\
q_4' &= 1,
\end{aligned}$$

where q_1', q_2', q_3' and q_4' are their success probabilities in the four types of rounds, and $1 - \delta_c$ is the completeness of the RIGID test; from Corollary 1 we have $\delta_c = 2^{-\Omega(n+t)}$. Moreover PV' applies the honest strategy in all rounds, while PP' applies the honest strategy in the Rigidity-Clifford and Rigidity-Tomography rounds. Applying Lemma 21, it follows that

$$w \;\leq\; O(\varepsilon') + \mathrm{poly}(\varepsilon) + p_1 \cdot O(\delta_c).$$

Therefore the prover's overall success probability is at most

$$\begin{aligned}&\min(p_1, p_4)(1-\varepsilon) + \max(p_1, p_4) + p_2(1-\varepsilon') + p_3\left(\frac{1}{3} + w\right)\\ \le & p_{\text{compl}} - \left(\frac{p_3}{3} + \varepsilon' p_2 + \varepsilon \min(p_1, p_4)\right) + p_3\left(O(\varepsilon') + \text{poly}(\varepsilon)\right) + (p_1 + p_3 p_1)\cdot O(\delta_c),\end{aligned}$$

where recall from Lemma 17 that $p_{\text{compl}} = p_1(1-\delta_c) + p_2 + p_4 + \frac{2}{3}p_3$. Fixing p_2 to be a large enough multiple of p_1 and of p_3 we can ensure that the net contribution of the terms involving ε' and δ_c on the right-hand side is always non-positive. Choosing $p_1 = p_4$ and p_3 so that the ratio p_3/p_1 is small enough we can ensure that the right-hand side is less than $p_{\text{compl}} - \Delta$, for some universal constant $\Delta > 0$ and all $\varepsilon, \varepsilon' \geq 0$.

B.4 Multi-prover game for QMA

In this section we propose a new multi-prover game for QMA, which is based on the Dog-Walker protocol. Recently, there has been an effort to devise such games [FV15,Ji16,NV17], due to their connections to the quantum PCP conjecture [AAV13].

A promise problem L is in QMA if there is a uniform family of quantum circuits $\{V_x\}_{x\in L}$ such that if x is a yes-instance, then there exists a quantum state $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n_w}$, such that V_x accepts on input $|\psi\rangle|0\rangle^{\otimes n_a}$ with probability at least $\frac{2}{3}$, while for a no-instance x and all states $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n_w}$, V_x rejects on input $|\psi\rangle|0\rangle^{\otimes n_a}$ with probability at least $\frac{2}{3}$. The run-time of the circuit V_x and the values n_w and n_a are polynomially bounded in $|x|$.

In a multi-prover game for a promise problem L, an instance $x \in L$ is reduced to ja game G_x such that if x is a yes-instance, then the maximum acceptance probability in the game is at least c, whereas if x is a no-instance, then the maximum acceptance probability in the game is at most s, for $c > s$.

Here, we are interested in multi-prover games where the verifier is classical, the honest provers run a polynomially bounded quantum computation on copies of an accepting witness and the completeness-soundness gap $c - s$ is constant. Using the Dog-Walker protocol, we are able to construct, to the best of our knowledge, the first two-prover game for QMA with these parameters. In our protocol the Verifier and provers exchange messages of polynomial size in two rounds of communication, one with each prover.

Our protocol consists in the Verifier running the Dog-Walker protocol, with the following changes:

- On X-Test rounds (resp. Z Test-rounds), the Verifier randomly selects positions where PV has measured in the Z basis (resp. X basis) and sends them to PP. PP uses the EPR pair halves in these positions as the witness register when he executes the circuit V_x.
- On Rigidity-Computation rounds, the Verifier informs PV of the halves of EPR pairs that should be used to teleport the witness state to PP, and PV reports the outcomes of the teleportation measurements along with the answers for the original Dog-Walker protocol. The Verifier ignores the measurements corresponding to the teleportation and uses the remaining bits to perform the same checks as in the original Dog-Walker protocol.

– On EPR-Computation rounds, the Verifier informs PP of the EPR pair halves that should be used as the witness when he performs the circuit V_x. The Verifier also informs PV of these positions, who should use them to teleport the witness state to PP. The outcomes of the teleportation measurements are reported to the Verifier along with the answers for the original Dog-Walker protocol, in order that the Verifier can decrypt the output of the computation.

The full description of the protocol is presented in Figures 24, 25 and 26, where the differences to the original Dog-Walker protocol are underlined. We state the result and sketch its proof.

Let x be an instance of a language $L \in$ QMA and V_x the associated verification circuit. V_x takes as input an n_w-qubit witness register and an n_a-qubit ancilla register. It has t T gates, t_0 of which are even and $t - t_0$ are odd (see Section 2.3 for the definition of even and odd T gates).

1. Select a round type **EPR** or **Rigidity**, and disjoint sets $N^w, N^a, T^0, T^1 \subset \{1, \ldots, m\}$ of sizes n_w, n_a, t_0 and $t - t_0$ respectively.

EPR Choose $\boldsymbol{z}$ uniformly at random from $\{0,1\}^t$ and send it, along with $\boldsymbol{x}$, N^w, N^a, T^0 and T^1, to PP. Receive measurement outcomes $\boldsymbol{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ from PP.

Rigidity Choose W' according to $\mu(\cdot)$ and send it to PP. Receive $\boldsymbol{e}' \in \{0,1\}^m$ from PP.

2. Select a sub-round type at random from **Computation**, **X-Test** or **Z-Test**.

Computation Based on whether it's an EPR or a Rigidity Round:

EPR (i) Send $\boldsymbol{x}$, $\boldsymbol{z}$, $\boldsymbol{c}$ and sets $\underline{N^w}$, N^a, T^0 and T^1 to PV, and receive measurement outcomes $\boldsymbol{a}, \boldsymbol{b} \in \{0,1\}^{n_w+n_a}$ and $\boldsymbol{e} \in \{0,1\}^t$.

(ii) Apply the update rules from Table 2 gate-by-gate to obtain the final X key for the output wire a'_f. If $c_f + a'_f \neq 0$, reject.

Rigidity (Tomography) (i) Choose uniform random strings $\boldsymbol{c}, \boldsymbol{z} \in \{0,1\}^t$, $\boldsymbol{x} \in \{0,1\}^n$ to send to PV, along with $\underline{N^w}$, N^a and T, and receive measurement outcomes $\boldsymbol{a}, \boldsymbol{b} \in \{0,1\}^{n_w+n_a}$ and $\boldsymbol{e} \in \{0,1\}^t$.

(ii) From $\boldsymbol{x}$, $\boldsymbol{c}$, $\boldsymbol{z}$, $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{e}$, determine the adaptive measurements $W \in \Sigma^{n+t}$ that V^0_{EPR} would have performed (based on Figure 3b), and reject if the input-output pairs $(W', \boldsymbol{e}')$ and $(N \cup T, (W, \boldsymbol{e}))$ do not satisfy the winning criterion for $\textsc{tom}(\Sigma, n+t, m)$.

X-**Test** Based on whether it's an EPR or a Rigidity Round:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = Z$ for all $i \in \underline{N^w} \cup N^a$; $W_i = Z$ for all $i \in T^0$; and $W_i \in \{X, Y\}$ for all $i \in T^1$. Send W to PV and receive measurement results $\boldsymbol{e} \in \{0,1\}^m$. Let $(\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{e}_N, 0^n)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$ the X key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $\exists i$ s.t. the i-th T gate is even and $c_i \neq a'_i + e_i$, reject. If $c_f + a'_f \neq 0$, reject.

Rigidity (Clifford) Choose W according to the marginal conditioned on W', $\mu(\cdot|W')$. Send W to PV and receive $\boldsymbol{e} \in \{0,1\}^m$. Reject if $(W', \boldsymbol{e}', W, \boldsymbol{e})$ doesn't win $\textsc{rigid}(\Sigma, m)$.

Z-**Test** Based on whether it's an EPR or a Rigidity Round:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = X$ for all $i \in \underline{N^w} \cup N^a$; $W_i \in \{X, Y\}$ for all $i \in T^0$; and $W_i = Z$ for all $i \in T^1$. Send W to PV and receive measurement results $\boldsymbol{e} \in \{0,1\}^m$. Let $(\boldsymbol{a}, \boldsymbol{b}) = (0^n, \boldsymbol{e}_N)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$, the X key before the i-th T gate is applied, a'_i. If $\exists i$ s.t. the i-th T gate is odd and $c_i \neq a'_i + e_i$, reject.

Rigidity (Clifford) Identical to X-Test case.

Fig. 24: QMA Protocol: Verifier's point of view.

1. If PP receives a question W' from V (he is playing TOM or RIGID):
   Measure the m qubits in the observable indicated by W' — for example, if $W' \in \Sigma^m$, for $i \in \{1,\dots,m\}$, measure the i-th qubit in the basis indicated by W'_i — and report the outcomes $\boldsymbol{e}'$ to V.
2. If PP receives $\boldsymbol{x},\boldsymbol{z}$, and sets N^w,N^a, T^0 and T^1 from V (he is playing the role of P_{EPR} from the EPR Protocol):
   Run prover P_{EPR} from Figure 3c with the V_x as the circuit Q, on input $\boldsymbol{z}$, the n_w qubits in N^w as the witness, the n_a qubits in N^a as the ancilla, and the t qubits in $T^0 \cup T^1$ for T gadgets. Report the outputs $\boldsymbol{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ of P_{EPR} to V.

Fig. 25: QMA Protocol: Honest strategy for PP.

1. If PV receives a question W from V (he is playing RIGID or an X- or Z-Test Round):
   Measure the m qubits in the observable indicated by W — for example, if $W \in \Sigma^m$, for $i \in \{1,\dots,m\}$, measure the i-th qubit in the basis indicated by W_i — and report the outcomes $\boldsymbol{e}$ to V.
2. If PV receives $\boldsymbol{x}$, $\boldsymbol{z}$, $\boldsymbol{c}$ and sets N^w, N^a, T^0 and T^1 from V (he is playing TOM or a Computation Round):
   Using the EPR pairs in N^w, teleports the witness state $|\psi\rangle$ that makes V_x accept with high probability. Let $(\boldsymbol{a}_{N^w},\boldsymbol{b}_{N^w})$ be the corresponding outcomes of the teleportation measurements.
   Measure each qubit in N^a in the Z basis with outcomes $\boldsymbol{d}$ and let $(\boldsymbol{a}_{N^a},\boldsymbol{b}_{N^a}) = (\boldsymbol{d},\boldsymbol{0})$
   Run the second step of procedure V^0_{EPR} from Figure 3b with V_x as the circuit Q, and the values $\boldsymbol{c}$, $\boldsymbol{z}$, the n_w qubits in N^w as the witness, the n_a qubits in N^a as the ancilla, and the t qubits in $T^0 \cup T^1$ for T gadgets. Report the outputs $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{e}$ of V^0_{EPR} to V.

Fig. 26: QMA Protocol: Honest strategy for PV.

Lemma 23. *There exists universal constants $0 \le p_{compl} \le 1$ and $\Delta > 0$ such that the following holds. Let L be a language in QMA and x an instance of L such that $n = |x|$. Let V_x be the verification circuit for this instance and g the number of gates in V_x (in the compiled form as described in Section 2). Then there exists a two-round interactive protocol between a classical verifier and two entangled provers where the Verifier sends $O(n+g)$-bit questions to the provers, the provers answer with $O(n+g)$ bits and the protocol satisfies the following properties.*

Completeness: *If x is a yes-instance, then there is a strategy for the provers such that the Verifier accepts with probability at least p_{compl}.*

Soundness: *If x is a no-instance, then for all strategies of the provers, the Verifier accepts with probability at most $p_{sound} = p_{compl} - \Delta$.*

Proof (Proof sketch). The Verifier performs the operations described in Figure 24.

The completeness of the protocol is straightforward: if PP and PV use the strategy in Figures 25 and 26, respectively, then the Verifier accepts with high probability.

The soundness of the protocol follows from the combination of the soundness of the Dog-Walker protocol and the soundness of the QMA verification circuit. Along the same lines as Lemmas 18, 19 and 20, we can show that if the acceptance probability in Rigidity-Test, Rigidity-Computation and EPR-Test rounds is sufficiently high, then there is a strategy where the provers follow the honest strategy and the acceptance probability in EPR-Computation round is only slightly changed. In the case where the provers are honest in the Rigidity-Test, Rigidity-Computation and EPR-Test rounds, no matter which state is held by PP as witness state, V_x rejects with high probability in the EPR-Computation round, by the soundness of the QMA verification circuit. The proof of soundness can be completed by repeating the arguments in Lemma 22.

C Running our protocols in sequence

In this section, we describe a sequential procedure that, starting from our protocols in Sections 4 and B, ensures that either the verifier aborts, or she obtains the correct outcome of the computation with probability 99%. Moreover, for honest provers, the probability that the procedure aborts is exponentially small in the number of sequential repetitions. Our sequential procedure has a number of rounds which depends on the desired soundness. As long as one only requires amplification of an arbitrarily small, but constant, soundness, to a fixed constant, the number of sequential repetitions remains constant.

To emphasize the importance of having such a sequential procedure, we note that, firstly, the current completeness-soundness gap between acceptance probability on *yes* and *no* instances, for both the leash and the Dog-Walker protocol, is a very small constant. Secondly, if a classical client wishes to employ our protocols to delegate a computation, we need to specify what the client interprets, at the end of the protocol, as the outcome of the delegated computation. The natural approach is to have the verifier interpret accept as a *yes* outcome and reject as a *no* outcome. However, this is not enough, as our security model based on the constant gap between acceptance probability for *yes* and *no* instances means that, while the provers have a low probability of making the verifier accept a *no* instance as a *yes*, they can always make the verifier accept a *yes* instance as a *no*, simply by behaving so that they are rejected.

The first point is addressed by running copies of the original protocol in sequence to amplify the completeness-soundness gap. The second point is addressed by having the verifier run the protocol twice: once for the circuit Q, and once for the circuit Q' defined by appending an X gate to the output wire of Q. If $f : X \to \{0,1\}$ for some $X \subseteq \{0,1\}^n$ is defined by $f(x) = 1$ if $\|\Pi_0 Q|x\rangle\|^2 \geq 2/3$, and $f(x) = 0$ if $\|\Pi_0 Q|x\rangle\|^2 \leq 1/3$, i.e. Q decides f with bounded error $1/3$, then it is easy to see that Q' decides $1 - f$ with bounded error $1/3$. Thus, the verifier will accept x as a *yes* instance of f if the protocol outputs accept when running Q on x and outputs reject when running Q' on x. The verifier accepts x as a *no* instance of f if the protocol outputs reject when running Q on x and outputs accept when running Q' on x. The verifier aborts if she sees accept-accept or reject-reject.

C.1 Sequential version of our protocols

Let P denote either the Verifier-on-a-leash or the Dog-Walker protocol from Sections 4 and B respectively, and let c and Δ denote the completeness and completeness-soundness gap. Let κ be a security parameter.

Protocol Seq(P, c, Δ, κ): Let (Q, x) be the verifier's input.

1. The verifier runs κ copies of protocol P in sequence on input (Q, x) with PP and PV. Then she runs κ copies in sequence on input (Q', x).
2. Let $\boldsymbol{o}, \tilde{\boldsymbol{o}} \in \{0,1\}^\kappa$ be such that $o_i = 1$ iff the i-th copy on input (Q, x) accepts, and $\tilde{o}_i = 1$ iff the i-th copy on input (Q', x) accepts. Let $wt(\boldsymbol{o})$ and $wt(\tilde{\boldsymbol{o}})$ be their Hamming weights. Then, the verifier accepts 1 as the outcome of the delegated computation if $wt(\boldsymbol{o}) \geq (c - \frac{\Delta}{2}) \cdot \kappa$ and $wt(\tilde{\boldsymbol{o}}) < (c - \frac{\Delta}{2}) \cdot \kappa$, and she accepts 0 as the outcome of the computation if $wt(\boldsymbol{o}) < (c - \frac{\Delta}{2}) \cdot \kappa$ and $wt(\tilde{\boldsymbol{o}}) \geq (c - \frac{\Delta}{2}) \cdot \kappa$. Otherwise the verifier aborts.

Fig. 27: Sequential version of our protocols

We state and prove completeness and soundness for the sequential protocol.

Theorem 8. *Let c and Δ be respectively the completeness and completeness-soundness gap of protocol P. On input (Q, x):*

- *If the provers are honest,*

$$\Pr\left(Seq(P, c, \Delta, \kappa) \textit{ outputs } f(x)\right) \geq 1 - 2\exp\left(-\frac{\Delta^2 \kappa}{2}\right).$$

- *For any cheating provers,*

$$\Pr\left(Seq(P, c, \Delta, \kappa) \textit{ outputs } 1 - f(x)\right) \leq \exp\left(-\frac{\Delta^2 \kappa}{8}\right).$$

Proof. We first show completeness. Let $s = c - \Delta$ be the soundness of protocol P. Suppose $f(x) = 1$ (the case $f(x) = 0$ is analogous). If the provers are honest, then the probability that the verifier outputs 1 is:

$$\begin{aligned}
\Pr(\text{Verifier outputs } 1) &= \Pr\left(wt(\boldsymbol{o}) \geq \left(c - \frac{\Delta}{2}\right) \cdot \kappa \ \wedge \ wt(\tilde{\boldsymbol{o}}) < \left(c - \frac{\Delta}{2}\right) \cdot \kappa\right) \\
&\geq 1 - \Pr\left(wt(\boldsymbol{o}) < \left(c - \frac{\Delta}{2}\right) \cdot \kappa\right) - \Pr\left(wt(\tilde{\boldsymbol{o}}) \geq \left(c - \frac{\Delta}{2}\right) \cdot \kappa\right) \\
&\geq 1 - 2\exp\left(-\frac{\Delta^2 \kappa}{2}\right)
\end{aligned}$$

by Hoeffding's inequality.

Next we show soundness. Again suppose $f(x) = 1$ (the case $f(x) = 0$ is analogous). Let W_j be an indicator random variable for the event $\tilde{o}_j = 1$, and let $F_j = W_j - s$. Define $X_l = \sum_{j=1}^{l} F_j$, for $l = 1, .., \kappa$. The F_j define a submartingale with $|F_j| \leq 1\ \forall j$. Hence, by Azuma's inequality, for any $\kappa \geq 1$, $\Pr(X_\kappa \geq t) \leq \exp(-\frac{t^2}{2\kappa})$. This implies that

$$\Pr\left(\sum_{j=1}^{\kappa} W_j - \kappa \cdot s \geq t\right) = \Pr\left(\sum_{j=1}^{\kappa} F_j \geq t\right) = \Pr\left(X_\kappa \geq t\right) \leq \exp\left(-\frac{t^2}{2\kappa}\right).$$

Then, for any provers PP and PV,

$$\begin{aligned}
\Pr(\text{Verifier outputs } 0) &\leq \Pr\left(wt(\tilde{\boldsymbol{o}}) \geq (c - \frac{\Delta}{2}) \cdot \kappa\right) \\
&= \Pr\left(\sum_{j=1}^{\kappa} W_j \geq (c - \frac{\Delta}{2}) \cdot \kappa\right) \\
&= \Pr\left(\sum_{j=1}^{\kappa} W_j - \kappa \cdot s \geq \kappa \cdot \frac{\Delta}{2}\right) \\
&\leq \exp\left(-\frac{\Delta^2 \kappa}{8}\right).
\end{aligned}$$