Practical parallel self-testing of Bell states via magic rectangles

Sean A. Adamson [*] and Petros Wallden [†]
School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom

(Received 6 August 2021; accepted 14 March 2022; published 31 March 2022)

Self-testing is a method to verify that one has a particular quantum state from purely classical statistics. For practical applications, such as device-independent delegated verifiable quantum computation, it is crucial that one self-tests multiple Bell states in parallel while keeping the quantum capabilities required of one side to a minimum. In this work, we use the $3\times n$ magic rectangle games (generalizations of the magic square game) to obtain a self-test for n Bell states where the one side needs only to measure single-qubit Pauli observables. The protocol requires small input sizes [constant for Alice and $O(\log_2 n)$ bits for Bob] and is robust with robustness $O(n^{5/2}\sqrt{\varepsilon})$, where ε is the closeness of the ideal (perfect) correlations to those observed. To achieve the desired self-test, we introduce a one-side-local quantum strategy for the magic square game that wins with certainty, we generalize this strategy to the family of $3\times n$ magic rectangle games, and we supplement these nonlocal games with extra check rounds (of single and pairs of observables).

DOI: 10.1103/PhysRevA.105.032456

I. INTRODUCTION

One of the most profound properties of quantum theory—one that defies our classical intuition—is that it exhibits nonlocality [1]. This distinct characteristic enables us to deduce that certain results we gather in an experimental setting cannot be explained with classical notions, and that there is necessarily some underlying quantumness at work. Even more interestingly, nonlocality makes it possible to deduce the exact quantum state of a real experimental system based on purely classical statistics. This property is known as self-testing. Beyond the foundational importance of being able to verify the quantum state of a totally untrusted black-box experimental setup, self-testing has many practical uses due to the higher levels of security it is able to offer. While the standard notions of nonlocality lead to device-independent cryptography (see, for example, Refs. [2,3]), self-testing enables such applications as device-independent secure delegated (verifiable) quantum computation [4–7] among other device-independent protocols that involve quantum *computation*. The crucial point is that, to enable device-independent quantum computation, one needs to test the quantum state itself (that is, one must perform self-testing); simple observation of nonlocal correlations does not suffice.

Delegated verifiable blind quantum computation [8,9] is arguably one of the most important applications of self-testing. Here, a client wishes to delegate some computation to a server (which has a quantum computer) such that the privacy of their input/output and computation is preserved, and in a way that allows the client to verify the validity of the answer that they receive. This is a setting with increasing practical relevancy, since quantum hardware companies already offer their services in the cloud. Protecting the privacy of client data and giving reassurances that the computation was performed as desired are crucial to making this model work. In this setting, since one side (the server) has access to a universal quantum computer, having extra quantum operations being performed on this side as part of a self-test comes with almost no further practical limitations. On the other hand, the client is assumed to have minimal quantum capabilities. Moreover, the client and server should self-test multiple maximally entangled Bell states in parallel. This is required in order to perform any interesting quantum computation (otherwise the client could simply perform the computation classically on their side). It follows that any natural self-test for such an application will have minimal experimental requirements on one side (the client) while also being required to test for many Bell states in parallel. This is precisely the nature of the self-test we obtain in this work.

A further observation is that self-tests of quantum states typically arise as the observation of an optimal quantum strategy for a certain nonlocal game. Conversely, exploring how different nonlocal games that appear elsewhere in the literature can be used for self-testing and what (if any) advantages these offer over other self-tests is, in its own right, an interesting endeavor. Here we examine the recently introduced generalization of the magic square game to rectangular dimensions [10], and we obtain a family of self-tests that compare favorably to other self-tests.

It is worth mentioning that one can compare self-tests with respect to a number of different figures of merit, with the importance of each depending on the application for which one wishes to use the self-test. We consider several different qualities, and in Sec. VI analyze what our proposed self-tests achieve and how they compare to other works. The first is the experimental complexity required by our self-test. This depends on the honest strategy and determines the quantum devices and resources required by each party. The second is that of communication complexity (required input and output sizes for the parties involved). Its most important ingredient is that of input question size, as this determines the amount of randomness that must be consumed per round of interaction

[*] sean.adamson@ed.ac.uk
[†] petros.wallden@ed.ac.uk

of the protocol. This can also play an important role in other aspects, e.g., in how much randomness can be generated in possible applications to private randomness expansion. Finally, the third figure of merit that self-tests can be compared upon is their robustness, i.e., how close to the ideal behavior the observed correlations need to be in order to ensure that the tested quantum state is sufficiently close to the desired reference state. Given that experiments have intrinsic imperfections and correlations cannot be perfectly saturated in a real setting, achieving good robustness is crucial for practical uses of self-testing. While many self-testing protocols are designed to perform well with respect to few particular figures of merit, it is key for the application at hand that a protocol achieves appropriate levels of performance simultaneously across all relevant areas. This is a major consideration in the self-test we present here.

A. Our contributions

We aim to obtain an improved self-test of multiple Bell states (with respect to different figures of merit). The nonlocal games at the core of our approach belong to the set of magic rectangle games. Our contributions may be summarized specifically as follows:

(i) We provide a quantum strategy to win the magic square game with certainty. This strategy involves three Bell pairs and, importantly, one side (say Alice) need only ever make local (single-qubit) Pauli measurements [11]. We say this strategy has the "one-side-local" property.

(ii) Based on this quantum strategy, we present a one-side-local self-test of three Bell states. This requires the introduction of some extra "check" rounds. Compared to other self-tests using the magic square game, ours requires a simpler experimental setup (one-side-local) and certifies a greater number of Bell states in parallel.

(iii) We also consider the set of $3\times n$ magic rectangle games, obtaining one-side-local quantum strategies for these (again winning with certainty) involving n Bell states.

(iv) From these strategies, we construct a parallel self-test of n Bell pairs that is one-side-local. This is our main result, as it offers an experimentally simpler parallel self-test that (i) has good input size scaling in the number of Bell states (constant for Alice and logarithmic for Bob), (ii) uses only perfect correlations, and (iii) is robust with robustness $O(n^{\frac{5}{2}}\sqrt{\varepsilon})$, where ε is the closeness of the ideal (perfect) correlations to those observed. Importantly, these properties are achieved simultaneously.

B. Overview of techniques

Our two main results are self-testing protocols for three and n Bell states, respectively. Informally, to self-test a quantum state one needs to provide a local isometry that maps an untrusted state (and operators) to a reference state (and operators), which are close to the desired ones. Our proofs proceed in five steps. In the first step, we define a nonlocal game (along with an optimal quantum winning strategy for that game) that will form the basis of the self-test. Importantly, the particular strategy given should involve the states that we are testing. In the second step, we give the honest behavior for the self-test. This fixes the experimental requirements for each side. The honest behavior includes (i) the optimal quantum strategy for the nonlocal game given earlier; and (ii) additional "check" rounds, where some further correlations (that do not need to exhibit nonlocality on their own) are requested [12]. In the third step, we define the (untrusted) observables and specify all the correlations that are to be tested. This is the information we have from experiment; it quantifies the proximity of the real experiment to the ideal maximum winning probabilities, and it forms the basis for obtaining the desired isometry. In the fourth step, the above correlations are used to prove that the untrusted single-qubit Pauli operators have commutation and anticommutation relations exactly as the corresponding (trusted) Pauli operators have. This is the hardest step, as it demonstrates that the correlations obtained from the experiment suffice to construct some untrusted operators that behave as the desired trusted operators. The fifth and final step is simply the application of a theorem of Coladangelo [13], wherein the existence of the desired local isometry was reduced to the satisfaction of the commutation and anticommutation relations obtained in the fourth step.

1. Self-test of three Bell states

a. Base nonlocal game. We introduce a strategy for winning the magic square game with certainty (Sec. III). This strategy has two interesting features. First, unlike the "standard" strategy that involves two Bell states [14], this strategy involves three Bell states. This means that any self-test based on this would result in self-testing more Bell states in parallel than using the magic square game in the standard way [15]. To succeed in the parallel self-testing of more Bell states requires some extra correlations (obtained from some "check" rounds) to prevent dishonest players from simply following the standard magic square strategy using only two Bell states. The second feature is that this strategy can be realized with Pauli measurements (as in the standard magic square strategy) but with one of the players (say Alice) needing only to perform local (single-qubit) measurements. In the usual magic square strategy, both parties must measure in entangled bases (see Sec. II C). This implies that a self-test based on this strategy would be simpler to execute experimentally and, importantly, impose fewer quantum-technological requirements on Alice's side—something of immediate interest for major applications of self-testing.

b. Honest run. Alice plays the one-side-local magic square strategy (see Sec. III), with the difference being that she measures locally each of her three qubits and returns these as her answer, allowing the product of pairs to be checked by a referee. Bob has two types of rounds: game rounds, where he plays the modified magic square game by measuring pairs of qubits in the $\hat{X}\otimes\hat{X}$, $\hat{Y}\otimes\hat{Y}$, and $\hat{Z}\otimes\hat{Z}$ bases simultaneously, and "check" rounds, where he measures his three qubits locally.

c. Untrusted observables and correlations. Alice has only untrusted local Pauli observables, while Bob has different untrusted observables in game and check rounds. Interestingly, Bob's observables in the check rounds are the ones used for the isometry, while the observables of game rounds are used to enforce the suitable commutation and anticommutation relations on Alice's side. The correlations observed are

those required for the magic square game along with the (perfect) Einstein–Podolsky–Rosen (EPR) correlations in check rounds.

d. Commutation and anticommutation. The main theorem for this case (Theorem 9 of Sec. IV C) is stated informally here.

Theorem 1 (Informal Theorem 9). The game-round observables of Alice and the check-round observables of Bob obey standard commutation and anticommutation relations up to $O(\sqrt{\varepsilon})$, where ε is the distance of the observed correlations from the ideal ones. The observables commute when acting on different qubits; commute when they are of the same type and act on the same qubit; and anticommute when they act on the same qubit and are conjugate (e.g., X and Z).

e. Isometry. Using the relations provided by the aforementioned theorem, and following [13], we obtain a suitable local isometry and complete the self-test.

2. Self-test of many Bell states

a. Base nonlocal game. We introduce a strategy that wins the $3\times n$ magic rectangle game with certainty using n Bell states (Sec. V A). Note that the $3\times n$ magic rectangle game can also be won with only two Bell states, but our strategy enables the parallel self-test of n Bell states, having the same one-side-locality as our previous result.

b. Honest run. Alice plays the magic rectangle strategy (see Sec. V A) described by measuring all of her qubits in one of the three Pauli bases (all in the same basis). Suitable products of her outcomes can be checked for consistency in the magic rectangle game by a referee. Bob now has three round types: game rounds, *local* check rounds (in which single-qubit correlations are checked), and *pair* check rounds (in which correlations of pairs of qubits are checked).

c. Untrusted observables and correlations. Alice has only untrusted local Pauli observables, while Bob has untrusted observables for all three round types. The local-check-round observables are used to construct the subsequent local isometry, while the other observables are used to obtain suitable commutation and anticommutation relations.

d. Commutation and anticommutation. The main theorem (Theorem 16 of Sec. V D) contains the same type of relations as in the case with three Bell states, where obtaining the anticommutation relations is considerably more complicated (and requires the extra set of rounds). This is stated informally as follows:

Theorem 2 (Informal Theorem 16). The game-round observables of Alice and the local-check-round observables of Bob obey standard commutation relations up to $O(\sqrt{\varepsilon})$ and anticommutation relations up to $O(n\sqrt{\varepsilon})$, where ε is the distance of the observed correlations from the ideal ones. The observables commute when acting on different qubits; commute when they are of the same type and act on the same qubit; and anticommute when they act on the same qubit and are conjugate (e.g., X and Z).

e. Isometry. Again following [13] and using the relations provided by Theorem 16, we recover the desired local isometry that results in a self-test of n Bell states.

C. Related works

The magic square game was first introduced by Mermin [16], Peres [17]. Aravind [14] gives a nontechnical demonstration of the Mermin-Peres magic square game. In a previous work, we examined an extension of the magic square game to arbitrary rectangular dimensions [10]. A family of these games is used as the basis for the self-test presented here.

The concept of self-testing was first introduced by Mayers and Yao [18] in a cryptographic context, with the first mention of the term "self-testing" appearing in [19]. Wu *et al.* [15] gave the first self-test of two maximally entangled pairs of qubits based on the magic square game, making use of the work of McKague [20] on self-testing in parallel. Coladangelo [13], Coudron and Natarajan [21] independently gave robust parallel self-tests of arbitrarily many Bell states based on the magic square game. A result of Coladangelo [13], which is in turn based on results of Chao *et al.* [22], is used in the present work (see Theorem 6). Natarajan and Vidick [23] gave the first example of a self-test for n Bell states with constant robustness. Subsequent work by the same authors achieved such a test where the number of bits of communication required is logarithmic in n [24]. A variant of this by Natarajan and Wright [25], called the "Pauli basis test," is presented as part of the work of Ji *et al.* [26]. Work in another direction is offered by Šupić *et al.* [27], who exhibit (without consideration of robustness) a constant-input-size parallel self-test for many copies of an arbitrary state given a self-test for a single copy. On self-testing maximally entangled states of arbitrary local dimension d, the results of Fu [28] and Mančinska *et al.* [29] provide robust self-tests using constant-sized questions and answers. However, the robustness of the former is exponential in d and in the latter is not constructed. Sarkar *et al.* [30] also provide such a self-test, however its robustness is not studied. More details on self-testing can be found in the recent and excellent review by Šupić and Bowles [31].

D. Organization of the paper

In Sec. II some background on the properties of quantum states, self-testing, and the magic square and rectangles nonlocal games is given. In Sec. III a one-side-local optimal quantum winning strategy for the magic square game is given, and in Sec. IV this strategy is used as the basis of a parallel, one-side-local self-test of three Bell states. In Sec. V a generalization of this one-side-local quantum strategy for $3\times n$ magic rectangle games is given, and the corresponding self-test for n Bell states is proven. We conclude in Sec. VI.

II. PRELIMINARIES

A. States and measurements

We let registers of observers Alice and Bob be labeled by the letters A and B, respectively. A local Hilbert space of Alice will be denoted $\mathcal{H}_A$, and similarly a local Hilbert space of Bob will be denoted $\mathcal{H}_B$. Sometimes we will need to talk about different Hilbert spaces local to an observer's subsystem. For this, we will use notation such as $\mathcal{H}'_A$ or $\tilde{\mathcal{H}}_A$ to mean different Hilbert spaces on Alice's side. The set of linear operators on $\mathcal{H}$ will be denoted $\mathcal{L}(\mathcal{H})$. The action of an operator $Q_A \in \mathcal{L}(\mathcal{H}_A)$

on a multipartite state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ will often be shortened as $Q_A|\Psi\rangle = Q_A \otimes I_B|\Psi\rangle$.

For the purposes of self-testing, all quantum measurements will be defined to have two possible outcomes labeled by ± 1. We will not make any other assumptions about the physical state spaces of Alice and Bob. In particular, we will not assume their dimensions. We take all unknown measurements to be projective on some unknown state, with observables of the form $M = M_+ - M_-$ for some orthogonal projections M_+ and M_- satisfying $M_+ + M_- = I$ and $M_+M_- = M_-M_+ = 0$. With our definitions, all unknown observables are also unitary operators and satisfy the involutory property $M^2 = I$. Such operators that are both Hermitian and unitary are also known as *reflection* operators. An operator that is not unknown (but is instead a *reference* operator) will be denoted by a hat symbol, for example the Pauli $\hat{X}$ observable.

The following lemma will be useful to estimate the action of unknown observables on an unknown state. The norm $\|\cdot\|$ associated with a Hilbert space will refer to that induced by its inner product throughout:

Lemma 3. Let $|\varphi\rangle$ and $|\chi\rangle$ be normalized states belonging to the same Hilbert space and let $\varepsilon \geqslant 0$. If the real part $\mathrm{Re}\langle\varphi|\chi\rangle \geqslant 1 - \varepsilon$, then $\||\varphi\rangle - |\chi\rangle\| \leqslant \sqrt{2\varepsilon}$.

Proof. Immediate from the definition of the induced norm $\||v\rangle\| = \sqrt{\langle v|v\rangle}$. ■

Remark. In the ideal case of $\varepsilon = 0$, we get $|\varphi\rangle = |\chi\rangle$.

We will denote by $|\Phi^+\rangle$ the maximally entangled Bell state shared between Alice and Bob,

$$|\Phi^+\rangle_{AB} = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}. \tag{1}$$

In cases in which Alice and Bob share multiple such states, we may label each by an additional index so that each qubit of an observer's register can be uniquely identified. That is, we may write

$$|\Phi^+\rangle_{AB}^{(i)} = \frac{|0\rangle_A^i \otimes |0\rangle_B^i + |1\rangle_A^i \otimes |1\rangle_B^i}{\sqrt{2}}. \tag{2}$$

To denote the case of n copies of such states, with one-half of each being held by Alice and the other by Bob, we will adopt the notation

$$|\Phi^+\rangle_{AB}^{\otimes n} = \bigotimes_{i=1}^{n} |\Phi^+\rangle_{AB}^{(i)}. \tag{3}$$

B. Self-testing

Consider local measurements made on a system shared by two observers, Alice and Bob, who are unable to communicate with one another. Self-testing is a procedure that allows the observers to deduce the quantum state they share from purely classical (and device-independent) observations. Specifically, given a probability distribution defining the behavior of untrusted measurement devices held by Alice and Bob, it is often possible to deduce (up to some local isometry) the quantum state they share. Moreover, one can also often deduce the local quantum measurements corresponding to different inputs and outputs for each device.

Instead of the physical unknown state being specified by a density operator ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$, we will work throughout with purifications $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P$ for some purifying space $\mathcal{H}_P$ separate from both observers. This is for the sake of mathematical convenience and, since all operations accessible to the observers will act trivially on this purifying space, we will often suppress it in our notation.

Let us denote a possible output of Alice upon an input x by a. Similarly, upon an input y, let b represent an output of Bob. A fixed configuration of probabilities $p(a, b|x, y)$ defines a behavior for the observers. Self-testing relies on the Born rule to express such probabilities in terms of quantum correlations $p(a, b|x, y) = \langle\Psi|M_{a|x} \otimes N_{b|y}|\Psi\rangle$ for some measurements $\{M_{a|x}\}_a \subset \mathcal{L}(\mathcal{H}_A)$ for Alice and $\{N_{b|y}\}_b \subset \mathcal{L}(\mathcal{H}_B)$ for Bob. An isometry $\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}'_A \otimes \mathcal{H}'_B$ is called *local* if it can be written as $\Phi = \Phi_A \otimes \Phi_B$ for some isometries $\Phi_D : \mathcal{H}_D \to \mathcal{H}'_D$, where D stands for either A or B. We are now ready to state what it means to self-test quantum states.

Definition 4 (Self-testing of states). A behavior defined by correlations $p(a, b|x, y)$ is said to δ-approximately *self-test* the state $|\Psi'\rangle \in \mathcal{H}'_A \otimes \mathcal{H}'_B$ if, for any state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P$ from which these correlations may arise, there exists a junk state $|\xi\rangle \in \tilde{\mathcal{H}}_A \otimes \tilde{\mathcal{H}}_B \otimes \mathcal{H}_P$ and isometries $\Phi_D : \mathcal{H}_D \to \mathcal{H}'_D \otimes \tilde{\mathcal{H}}_D$ defining the local isometry $\Phi = \Phi_A \otimes \Phi_B \otimes I_P$ such that

$$\|\Phi|\Psi\rangle - |\Psi'\rangle \otimes |\xi\rangle\| \leqslant \delta. \tag{4}$$

The definition of self-testing given here can be extended to the case in which we wish to self-test some quantum measurements in addition to a state.

Definition 5 (Self-testing of measurements). A behavior $p(a, b|x, y)$ is said to δ-approximately *self-test* the state $|\Psi'\rangle \in \mathcal{H}'_A \otimes \mathcal{H}'_B$ and measurements $\{\hat{M}_{a|x}\}_a \subset \mathcal{L}(\mathcal{H}'_A)$ and $\{\hat{N}_{b|y}\}_b \subset \mathcal{L}(\mathcal{H}'_B)$ if, for any state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P$ and measurements $\{M_{a|x}\}_a \subset \mathcal{L}(\mathcal{H}_A)$ and $\{N_{b|y}\}_b \subset \mathcal{L}(\mathcal{H}_B)$ from which these correlations may arise, there exists a junk state $|\xi\rangle \in \tilde{\mathcal{H}}_A \otimes \tilde{\mathcal{H}}_B \otimes \mathcal{H}_P$ and isometries $\Phi_D : \mathcal{H}_D \to \mathcal{H}'_D \otimes \tilde{\mathcal{H}}_D$ defining the local isometry $\Phi = \Phi_A \otimes \Phi_B \otimes I_P$ such that

$$\left\|\Phi M_{a|x}N_{b|y}|\Psi\rangle - \hat{M}_{a|x}\hat{N}_{b|y}|\Psi'\rangle \otimes |\xi\rangle\right\| \leqslant \delta \tag{5}$$

for all a, b, x, and y.

Since all unknown observables we will be dealing with take the form $M = M_+ - M_-$ satisfying $M_+ + M_- = I$, we can always write each measurement operator as $M_\pm = (I \pm M)/2$. To self-test a state $|\Psi'\rangle$ and a measurement $\{\hat{M}_+, \hat{M}_-\}$ (having observable $\hat{M} = \hat{M}_+ - \hat{M}_-$ and acting nontrivially only on one side of the reference space) according to Definition 5, it is sufficient by the linearity of isometries to instead show both

$$\|\Phi|\Psi\rangle - |\Psi'\rangle \otimes |\xi\rangle\| \leqslant \delta, \tag{6}$$

$$\|\Phi M|\Psi\rangle - \hat{M}|\Psi'\rangle \otimes |\xi\rangle\| \leqslant \delta. \tag{7}$$

The following theorem of Coladangelo [13] (based closely on the work of Chao *et al.* [22]) allows us to deduce the existence of a local isometry required for the parallel self-testing of n Bell states and single-qubit Pauli observables. Rather than using a behavior of the observers directly, the theorem states sufficient conditions in terms of appropriate correlation, anticommutation, and commutation relations of unknown observables available to Alice and Bob. Much of the current work will be dedicated to proving such relations from certain given correlations.

Theorem 6 (Ref. [13], Theorem 3.5). Let $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ have even dimension. Suppose there exist balanced reflections $X_A^i, Z_A^i \in \mathcal{L}(\mathcal{H}_A)$ and $X_B^i, Z_B^i \in \mathcal{L}(\mathcal{H}_B)$ for $i \in \{1, \ldots, n\}$ such that, for D either A or B and for all distinct i and j, they satisfy

$$\left\|\left(M_A^i - M_B^i\right)|\Psi\rangle\right\| \leqslant \delta, \tag{8a}$$

$$\left\|\left\{X_D^i, Z_D^i\right\}|\Psi\rangle\right\| \leqslant \delta, \tag{8b}$$

$$\left\|\left[M_D^i, N_D^j\right]|\Psi\rangle\right\| \leqslant \delta, \tag{8c}$$

where M and N can be either of X and Z. Then, there exists a state $|\xi\rangle \in \tilde{\mathcal{H}}_A \otimes \tilde{\mathcal{H}}_B$ and a local isometry $\Phi = \Phi_A \otimes \Phi_B$, where $\Phi_D : \mathcal{H}_D \to (\mathbb{C}^2)^{\otimes n} \otimes \tilde{\mathcal{H}}_D$, such that for all i,

$$\left\|\Phi|\Psi\rangle - |\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{3}{2}}\delta\right), \tag{9a}$$

$$\left\|\Phi M_D^i|\Psi\rangle - \hat{M}_D^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{3}{2}}\delta\right), \tag{9b}$$

where $\hat{X}_D^i$ and $\hat{Z}_D^i$ are Pauli observables acting on the ith qubit subsystem of register D.

The assumptions of Theorem 6 that the unknown state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ have even dimension and that the unknown reflection operators acting on these spaces are balanced (that is, their $+1$ and -1 eigenspaces have equal dimension) are not an issue for self-testing. In the construction of the isometry, one can always extend the $\mathcal{H}_D$ by direct sum with Hilbert spaces of appropriate dimensions on which the extension of $|\Psi\rangle$ is defined to have no mass, and correspondingly extend each reflection to have eigenspaces of equal dimensions. Thus we may freely assume these are automatically satisfied by any unknown reflections defined later as part of our self-testing proofs.

C. The magic square game

The Mermin-Peres magic square game [14] consists of two players, Alice and Bob, who are not allowed to communicate during each round of the game. This could be achieved, for example, by ensuring a spacelike separation between the two players. Each round consists of Alice and Bob, respectively, being assigned a row and column of an empty 3×3 table uniformly at random, which they must fill according to the following rules:

S1. Each filled cell must belong to the set $\{+1, -1\}$.

S2. Rows must contain an even number of negative entries (i.e., the product of Alice's entries to any assigned row must be $+1$).

S3. Columns must contain an odd number of negative entries (i.e., the product of Bob's entries to any assigned column must be -1).

Neither player has knowledge of which row or column the other has been assigned, nor does either player know what values the other has entered. The game is won if both players enter the same value into the cell shared by their row and column. It is clear that the optimal classical strategy succeeds with probability 8/9 only [32], and may be achieved by both players agreeing to each follow a particular configuration for their entire table before the game begins. Strikingly, if the players are allowed to share an entangled quantum state, it has been shown to be possible for them to win the magic square game with certainty [16,17].

$\hat{X} \otimes I$	$\hat{X} \otimes \hat{X}$	$I \otimes \hat{X}$
$-\hat{X} \otimes \hat{Z}$	$\hat{Y} \otimes \hat{Y}$	$-\hat{Z} \otimes \hat{X}$
$I \otimes \hat{Z}$	$\hat{Z} \otimes \hat{Z}$	$\hat{Z} \otimes I$

FIG. 1. A quantum strategy for the magic square game, in which the players share the entangled state given in Eq. (10). Observables $\hat{X}$, $\hat{Y}$, and $\hat{Z}$ are the Pauli spin operators, and I is the identity operator. Measurements of Alice correspond to a row, and those of Bob to a column. This strategy cannot be realized with either player performing only measurements localized to single-qubit registers.

A possible quantum winning strategy for the magic square allows the players to share the entangled state

$$|\Phi^+\rangle_{AB}^{(1)} \otimes |\Phi^+\rangle_{AB}^{(2)}. \tag{10}$$

Depending on which row and column are assigned, the players make measurements on their respective quantum systems according to the observables given in the corresponding cells of Fig. 1. The outcomes of these determine the values which Alice and Bob should enter into their respective row and column to win with certainty. Moreover, Fig. 1 shows that (unlike, say, the CHSH game) optimal strategies can be implemented by performing measurements of the two-qubit Pauli group only.

In the context of practical quantum strategies, we refer to measurements as *local* in the sense that they are performed on only a single-qubit register. It will be important for our purposes to understand that the strategy depicted here *cannot* be implemented, for either player, entirely with local measurements. To see this for Bob, consider the measurements contained in the second column of Fig. 1. Upon this column being selected, Bob is required to answer with three bits, produced by a measurement performed on his subsystem. The measurement, as given, is implemented as the simultaneous measurement of three observables (one for each bit of the answer). While the three corresponding observables $\hat{X} \otimes \hat{X}$, $\hat{Y} \otimes \hat{Y}$, and $\hat{Z} \otimes \hat{Z}$ are compatible when considered over Bob's entire subsystem, he cannot generally perform the six component measurements on his two registers independently and then combine the outcomes to obtain the required three-bit answer; the six local measurements $\hat{X} \otimes I$, $I \otimes \hat{X}$, $\hat{Y} \otimes I$, $I \otimes \hat{Y}$, $\hat{Z} \otimes I$, and $I \otimes \hat{Z}$ do not all commute in pairs, and thus the measurement cannot be realized as the simultaneous measurement of these six local observables. Similarly, consideration of the second row of Fig. 1 shows that the strategy for Alice also cannot be implemented by performing only local measurements. We present in Sec. III a strategy for the magic square

game that can be realized using only local measurements for one of the players, at the cost of requiring three shared Bell states.

D. Magic rectangle games

The magic square game can be generalized to be played on an $m\times n$ table [10]. Such a *magic rectangle* game corresponds to m possible questions for Alice and n for Bob. To avoid trivially winning strategies, the game rules are generalized accordingly.

Definition 7 (Magic rectangle games). An $m\times n$ game is specified by fixing some $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ each belonging to $\{+1, -1\}$, such that their product satisfies

$$\alpha_1, \ldots, \alpha_m \cdot \beta_1, \ldots, \beta_n = -1. \tag{11}$$

The rules of the given game are then as follows:

R1. Each filled cell must belong to the set $\{+1, -1\}$.

R2. Upon being assigned the ith row, the product of Alice's entries must be α_i.

R3. Upon being assigned the jth column, the product of Bob's entries must be β_j.

As before, the game is won if both players enter the same value into their shared cell.

The 3×3 magic square game described in Sec. II C is simply the special case in which $\alpha_1 = \alpha_2 = \alpha_3 = 1$ and $\beta_1 = \beta_2 = \beta_3 = -1$. In fact, there are 2^{m+n-1} different specifications of $m\times n$ games allowed by Eq. (11).

We will later be concerned specifically with $3\times n$ games in which entries to rows must all have positive products and entries to columns must all have negative products. Such games are defined by $\alpha_i = 1$ and $\beta_j = -1$ for all i and j and must have odd n due to Eq. (11). A particular class of winning strategies for these games will be used to build part of our self-test of n Bell states. In the case of these particular games, and as opposed to [10], we can rephrase the definition of magic rectangles in a way that will prove more useful for our self-testing purposes. If $(p_1, \ldots, p_n) \in \{+1, -1\}^n$ is any possible output row of Alice (whose product is required to be $+1$), then there exists an assignment of $a_1, \ldots, a_n \in \{+1, -1\}$ such that $p_j = \prod_{k\neq j} a_k$ for all j. To see this, simply take $a_k = p_k$ for all k. Conversely then, we may ask that Alice outputs some $a_1, \ldots, a_n \in \{+1, -1\}$ and leave it to the game referees to check whether the appropriate products $p_j = \prod_{k\neq j} a_k$ form a winning row. Notice in our special case of n odd, such p_j automatically satisfy the rule for Alice's rows $\prod_{j=1}^{n} p_j = +1$ for any assignment of the a_k. We now rephrase the definition of $3\times n$ magic rectangle games in this special case.

Definition 8 ($3\times n$ magic games). Given n odd, Alice and Bob receive inputs $x \in \{1, 2, 3\}$ and $y \in \{1, \ldots, n\}$, respectively. Alice outputs n bits $a_1, \ldots, a_n \in \{+1, -1\}$. Bob outputs $(b_1, b_2, b_3) \in \{+1, -1\}^3$ are required to satisfy $b_1 b_2 b_3 = -1$. The game is won if $\prod_{k\neq y} a_k = b_x$.

Remark. While Bob's output here is column y of a magic rectangle, Alice's output corresponds to filling row x as $(p_1, \ldots, p_n)$, where $p_j = \prod_{k\neq j} a_k$. The win condition is then equivalent to the familiar case when both players enter the same value into the shared cell $p_y = b_x$.

$I\otimes\hat{X}\otimes\hat{X}$	$\hat{X}\otimes I\otimes\hat{X}$	$\hat{X}\otimes\hat{X}\otimes I$
$I\otimes\hat{Y}\otimes\hat{Y}$	$\hat{Y}\otimes I\otimes\hat{Y}$	$\hat{Y}\otimes\hat{Y}\otimes I$
$I\otimes\hat{Z}\otimes\hat{Z}$	$\hat{Z}\otimes I\otimes\hat{Z}$	$\hat{Z}\otimes\hat{Z}\otimes I$

FIG. 2. The proposed magic square strategy. To realize any particular row, Alice is only required to measure each of her qubits locally, as the observables to be measured for any individual one of her three qubits commute within each row.

III. ONE-SIDE-LOCAL MAGIC SQUARE STRATEGY

Recall that the usual quantum winning strategy for the magic square game requires some measurements of both Alice and Bob to be performed in entangled bases (see the discussion of Sec. II C). We now propose a quantum strategy for the magic square game, also winning with certainty, which can be realized under the additional constraint that Alice may only make measurements localized to single qubits of her quantum system. Each round begins by allowing Alice and Bob to share three Bell states,

$$|\Psi\rangle = |\Phi^+\rangle_{AB}^{(1)} \otimes |\Phi^+\rangle_{AB}^{(2)} \otimes |\Phi^+\rangle_{AB}^{(3)}. \tag{12}$$

Half of each Bell state is given to Alice, and the other half to Bob. The proposed measurement strategy is depicted in Fig. 2.

Notice in Fig. 2 that each row is formed out of commuting observables whose product is equal to the identity operator. Similarly, the observables in each column commute and have a product equal to minus the identity operator. Moreover, the eigenvalues of each observable are $+1$ and -1. These facts combined show that Rules S1–S3 in Sec. II C are automatically satisfied by the outcomes of measuring a full row or column. If $\hat{M}_A$ is any observable for Alice's system contained in Fig. 2, and if $\hat{M}_B$ is the observable of the same cell for Bob's system, then it is easy to show the correlation

$$\langle\Psi|\hat{M}_A\hat{M}_B|\Psi\rangle = 1. \tag{13}$$

This can be seen, for example, by writing the Bell states comprising the shared state of Eq. (12) in terms of eigenstates of the $\hat{X}$, $\hat{Y}$, and $\hat{Z}$ operators, respectively,

$$\begin{aligned} |\Phi^+\rangle &= \frac{|+\rangle\otimes|+\rangle + |-\rangle\otimes|-\rangle}{\sqrt{2}} \\ &= \frac{|+i\rangle\otimes|-i\rangle + |-i\rangle\otimes|+i\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle}{\sqrt{2}}. \end{aligned} \tag{14}$$

Alice, therefore, always measures the same outcome as Bob for the shared cell (either both $+1$ or both -1), and so they win the game with certainty.

For any particular row assigned to Alice, it is clear from inspection of Fig. 2 that she need only make single-qubit measurements; for any given qubit of her system, the single-qubit observables she is required to measure with respect to that qubit of her register mutually commute within the row. That is, it is always possible for Alice to realize the required observables by recording the measurement outcomes of a particular Pauli operator ($\hat{X}$, $\hat{Y}$, or $\hat{Z}$ depending on the row) on each one of her three qubits. This strategy can thus be phrased naturally for the magic square game in the sense of Definition 8 with $n = 3$. Bob generates his outputs according to the columns of Fig. 2 as usual. The jth output bit a_j of Alice, however, results from the outcome of the single-qubit Pauli measurement $\hat{X}_A^j$, $\hat{Y}_A^j$, or $\hat{Z}_A^j$ on Alice's jth qubit depending on whether the first, second, or third row was assigned, respectively.

IV. SELF-TEST OF THREE BELL STATES

By augmenting the correlations arising from a winning magic square strategy by certain additional correlations that ensure Alice implements her side of the strategy locally, it is possible to self-test three copies of the Bell state $|\Phi^+\rangle$. These additional correlations are obtained from Bob making single-qubit Pauli measurements of his qubits in some rounds of the test, which we will call "check" rounds. Rounds that are not check rounds will be called "game" rounds. We now describe the structure of the self-test and specify its honest behavior. Afterward, we exhibit explicitly the correlations of unknown observables used in the test. Finally, we show how these correlations can be used to prove the relevant commutation and anticommutation relations required for a self-testing proof.

A. Structure and honest behavior

Alice receives an input $x \in \{1, 2, 3\}$ and Bob an input $y \in \{1, 2, 3\}$. Additionally, Bob receives an input $c \in \{0, 1\}$ controlling whether the round is a game or check round. If the round is a game round ($c = 0$), then it is the goal of the players to win at the magic square game (in the sense of Definition 8) with the row and column assigned to Alice and Bob given by x and y, respectively. Otherwise, if the round is a check round ($c = 1$), then the players are required to perfectly correlate certain combinations of their output bits (which will be convenient to state after our description of the honest behavior). Notice, however, that Alice is not directly provided with the information of whether the round is to be considered a game or check round. The protocol is summarized in Protocol 1.

Protocol 1. A protocol for certifying three Bell states. Strategies in which Alice uses entangled measurements are ruled out by *local check* rounds. The protocol is phrased in terms of the parameter n, as it will be extended in Sec. V B in order to self-test n Bell states.

Let $n = 3$ be the number of Bell states to be certified. In each round, a verifier chooses $c \in \{0, 1\}$ and $y \in \{1, \ldots, n\}$. The verifier sends Bob (c, y) and, depending on c, runs one of the following subprotocols:

0. *Magic game*: Send Alice $x \in \{1, 2, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and b_1, b_2, b_3 in $\{+1, -1\}$ satisfying $b_1 b_2 b_3 = -1$. Accept if and only if $\prod_{k \neq y} a_k = b_x$.
1. *Local check*: Send Alice $x \in \{1, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ in $\{+1, -1\}$.
   (a) If $x = 1$, accept if and only if $a_y = b_y$.
   (b) If $x = 3$, accept if and only if $a_j = b_j$ for all $j \neq y$.

In an honest round of the experiment, the players share three Bell states, so that $|\Psi\rangle = |\Phi^+\rangle_{AB}^{\otimes 3}$ as in the magic square strategy of Sec. III. Alice always performs her side of this magic square strategy, providing each of her output bits a_j to the referees (as in Definition 8) by measuring

$$\hat{X}_A^j \quad \text{if } x = 1, \tag{15a}$$

$$\hat{Y}_A^j \quad \text{if } x = 2, \tag{15b}$$

$$\hat{Z}_A^j \quad \text{if } x = 3. \tag{15c}$$

The honest behavior of Bob depends on the type of round c. If $c = 0$, then Bob also performs his side of our one-side-local magic square strategy, returning outputs according to measuring the observables in column y of Fig. 2 so that the magic square game is won with certainty. Otherwise, if $c = 1$, then the input y determines which one of three sets of single-qubit Pauli measurements he performs. Specifically, Bob's output bits are generated as the measurement outcomes of the set of Pauli observables,

$$\{\hat{X}_B^1, \hat{Z}_B^2, \hat{Z}_B^3\} \quad \text{if } y = 1, \tag{16a}$$

$$\{\hat{Z}_B^1, \hat{X}_B^2, \hat{Z}_B^3\} \quad \text{if } y = 2, \tag{16b}$$

$$\{\hat{Z}_B^1, \hat{Z}_B^2, \hat{X}_B^3\} \quad \text{if } y = 3. \tag{16c}$$

It is convenient at this point to call attention to the perfect correlations of output bits expected in honest check rounds. These are all the single-qubit quantum correlations $\langle\Psi|\hat{X}_A^j \hat{X}_B^j|\Psi\rangle = 1$ and $\langle\Psi|\hat{Z}_A^j \hat{Z}_B^j|\Psi\rangle = 1$. Observation of a version of these correlations using *untrusted* observables (which will not be assumed to be identical for Bob upon his different inputs) will become a requirement for our protocol to certify the desired reference state.

B. Unknown observables and correlations

We will denote the unknown state shared by the players by $|\Psi\rangle$, and the expectation value of an unknown

observable M with respect to this state by $\langle M\rangle = \langle\Psi|M|\Psi\rangle$. We now describe the unknown observables which will be used by Alice and Bob in our self-testing proof. Recall that, in contrast to the honest Pauli observables used in the previous Sec. IV A, such unknown observables are denoted without a hat symbol (using X for the corresponding unknown version of the Pauli $\hat{X}$ observable). We may not assume *a priori*, in the potentially dishonest case of the self-testing protocol, that the players measure any of the same observables upon being given different inputs. For this reason, we introduce notation in such a way that the observer and their input can always be deduced from the label of an unknown observable. This choice of notation will be seen in Eqs. (17), (18), and (20).

It is important to note that all unknown observables that are to be measured as part of the same local input commute by definition. For example, from the observables defined immediately below, it can always be assumed that $[X_A^1, X_A^2] = 0$, since both observables correspond to the input $x = 1$ for Alice. Furthermore, it can always be assumed that any two observables defined for different players commute. These two properties will be exploited frequently in proofs throughout the rest of the work.

1. Alice's observables

We define sets of mutually commuting unknown observables on Alice's side to be measured depending on her input x as

$$\left\{X_A^1, X_A^2, X_A^3\right\} \quad \text{if } x = 1, \tag{17a}$$

$$\left\{Y_A^1, Y_A^2, Y_A^3\right\} \quad \text{if } x = 2, \tag{17b}$$

$$\left\{Z_A^1, Z_A^2, Z_A^3\right\} \quad \text{if } x = 3. \tag{17c}$$

Each of these unknown observables corresponds to a single-qubit Pauli observable, which acts on the qubit of Alice indicated by its superscript.

2. Bob's observables (game rounds)

For game rounds ($c = 0$), we will denote the sets of unknown observables to be measured by Bob, depending on his input y, by

$$\left\{X_B^{\bar{1}}, Y_B^{\bar{1}}, Z_B^{\bar{1}}\right\} \quad \text{if } y = 1, \tag{18a}$$

$$\left\{X_B^{\bar{2}}, Y_B^{\bar{2}}, Z_B^{\bar{2}}\right\} \quad \text{if } y = 2, \tag{18b}$$

$$\left\{X_B^{\bar{3}}, Y_B^{\bar{3}}, Z_B^{\bar{3}}\right\} \quad \text{if } y = 3. \tag{18c}$$

The overline notation used in each superscript reflects that these observables correspond to the product of single-qubit Pauli observables acting on all qubits of Bob other than that indicated. For example, here the unknown observable $X_B^{\bar{1}}$ corresponds to $\hat{X}_B^2\hat{X}_B^3$ in the honest case. Note also that Rule S3 of the magic square game requires columns to have negative products. In terms of unknown observables, that is $\langle X_B^{\bar{y}} Y_B^{\bar{y}} Z_B^{\bar{y}}\rangle = -1$ for all y. Thus we need not have defined one observable in each set, say $Y_B^{\bar{y}}$, since this implies

$$Y_B^{\bar{y}}|\Psi\rangle = -X_B^{\bar{y}} Z_B^{\bar{y}}|\Psi\rangle. \tag{19}$$

We will, however, choose to keep all of these observables for notational convenience, referring to Eq. (19) when necessary.

3. Bob's observables (check rounds)

For check rounds ($c = 1$), Bob's unknown observables correspond to single-qubit Pauli X and Z observables acting on his system. These will be denoted as follows, with an additional subscript to distinguish unknown observables of different inputs:

$$\left\{X_{B,1}^1, Z_{B,1}^2, Z_{B,1}^3\right\} \quad \text{if } y = 1, \tag{20a}$$

$$\left\{Z_{B,2}^1, X_{B,2}^2, Z_{B,2}^3\right\} \quad \text{if } y = 2, \tag{20b}$$

$$\left\{Z_{B,3}^1, Z_{B,3}^2, X_{B,3}^3\right\} \quad \text{if } y = 3. \tag{20c}$$

4. Correlations

The correlations of unknown observables amounting to a uniformly ε_0-close to perfect strategy for the magic square game (i.e., correlations obtained in game rounds) are, for all distinct $i, j, k \in \{1, 2, 3\}$,

$$\left\langle X_A^i X_A^j X_B^{\bar{k}}\right\rangle \geqslant 1 - \varepsilon_0, \tag{21a}$$

$$-\left\langle Y_A^i Y_A^j X_B^{\bar{k}} Z_B^{\bar{k}}\right\rangle \geqslant 1 - \varepsilon_0, \tag{21b}$$

$$\left\langle Z_A^i Z_A^j Z_B^{\bar{k}}\right\rangle \geqslant 1 - \varepsilon_0. \tag{21c}$$

The correlations constituting uniformly ε_1-close to perfect check rounds are, again for all distinct $i, j \in \{1, 2, 3\}$,

$$\left\langle X_A^i X_{B,i}^i\right\rangle \geqslant 1 - \varepsilon_1, \tag{22a}$$

$$\left\langle Z_A^i Z_{B,j}^i\right\rangle \geqslant 1 - \varepsilon_1. \tag{22b}$$

Figure 3 clarifies the meaning of our unknown observables for game rounds.

C. Commutation and anticommutation relations

In this section, we prove commutation and anticommutation relations (acting on our unknown state) for those unknown observables of Alice and Bob corresponding to single-qubit Pauli measurements. To do this, we use the correlations of Sec. IV B. The results of this section are summarized in the following theorem:

Theorem 9. Let $i, j, k, l \in \{1, 2, 3\}$ be such that $i \neq k$ and $j \neq l$. We have correlations between each unknown observable of Alice with each of the corresponding observables on Bob's side,

$$\left\|\left(X_A^i - X_{B,i}^i\right)|\Psi\rangle\right\| \leqslant \sqrt{2\varepsilon_1}, \tag{23}$$

$$\left\|\left(Z_A^i - Z_{B,k}^i\right)|\Psi\rangle\right\| \leqslant \sqrt{2\varepsilon_1}. \tag{24}$$

We have the state-dependent anticommutativity of all unknown X observables with all unknown Z observables corresponding to the same qubit,

$$\left\|\left\{X_A^i, Z_A^i\right\}|\Psi\rangle\right\| \leqslant 9\sqrt{2\varepsilon_0} + 16\sqrt{2\varepsilon_1}, \tag{25}$$

$$\left\|\left\{X_{B,i}^i, Z_{B,k}^i\right\}|\Psi\rangle\right\| \leqslant 9\sqrt{2\varepsilon_0} + 20\sqrt{2\varepsilon_1}. \tag{26}$$

Finally, we have the state-dependent commutativity of unknown X and Z observables. On Bob's side, we have

$$\left\|\left[X_{B,i}^i, X_{B,j}^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{27}$$

$$\left\|\left[Z_{B,k}^i, Z_{B,l}^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}; \tag{28}$$

$X_A^2 X_A^3$	$X_A^1 X_A^3$	$X_A^1 X_A^2$
$Y_A^2 Y_A^3$	$Y_A^1 Y_A^3$	$Y_A^1 Y_A^2$
$Z_A^2 Z_A^3$	$Z_A^1 Z_A^3$	$Z_A^1 Z_A^2$

(a)

$X_B^{\bar{1}}$	$X_B^{\bar{2}}$	$X_B^{\bar{3}}$
$-X_B^{\bar{1}} Z_B^{\bar{1}}$	$-X_B^{\bar{2}} Z_B^{\bar{2}}$	$-X_B^{\bar{3}} Z_B^{\bar{3}}$
$Z_B^{\bar{1}}$	$Z_B^{\bar{2}}$	$Z_B^{\bar{3}}$

(b)

FIG. 3. The layout of unknown observables in a magic square strategy for (a) Alice and (b) Bob.

and moreover, restricting to observables corresponding to different qubits $i \neq j$,

$$\left\| \left[X_{B,i}^i, Z_{B,l}^j \right] |\Psi\rangle \right\| \leqslant 8\sqrt{2\varepsilon_1}. \tag{29}$$

On Alice's side, for different qubits $i \neq j$, we have

$$\left\| \left[M_A^i, N_A^j \right] |\Psi\rangle \right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{30}$$

where M and N can be either of X and Z.

Proof. Combine Propositions 10, 11, and 13. ■

Proposition 10 (Correlation). For all distinct $i, j \in \{1, 2, 3\}$,
we have the correlation estimates

$$\left\| \left(X_A^i - X_{B,i}^i \right) |\Psi\rangle \right\| \leqslant \sqrt{2\varepsilon_1}, \tag{31a}$$

$$\left\| \left(Z_A^i - Z_{B,j}^i \right) |\Psi\rangle \right\| \leqslant \sqrt{2\varepsilon_1}. \tag{31b}$$

Proof. Apply Lemma 3 to the correlations given in Eq. (22). ■

The following proposition shows the commutation of unknown observables which we expect to correspond to local measurements on different qubits. Since observables defined for different players are assumed to commute, we show commutation for the observables of each player separately.

Proposition 11 (Commutation). For all $i, j, k, l \in \{1, 2, 3\}$ such that $i \neq k$ and $j \neq l$, we have

$$\left\| \left[X_{B,i}^i, X_{B,j}^j \right] |\Psi\rangle \right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{32a}$$

$$\left\| \left[Z_{B,k}^i, Z_{B,l}^j \right] |\Psi\rangle \right\| \leqslant 4\sqrt{2\varepsilon_1}. \tag{32b}$$

Moreover, if $i \neq j$ we have commutation relations for Bob,

$$\left\| \left[X_{B,i}^i, Z_{B,l}^j \right] |\Psi\rangle \right\| \leqslant 8\sqrt{2\varepsilon_1}, \tag{33}$$

and for Alice,

$$\left\| \left[M_A^i, N_A^j \right] |\Psi\rangle \right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{34}$$

where M and N can be either of X and Z.

Proof. Using the triangle inequality with the estimates of Proposition 10, and the commutation of Alice's observables corresponding to the same input, we can write

$$\begin{aligned} \left\| \left[X_{B,i}^i, X_{B,j}^j \right] |\Psi\rangle \right\| &\leqslant 4\sqrt{2\varepsilon_1} + \left\| \left[X_A^j, X_A^i \right] |\Psi\rangle \right\| \\ &= 4\sqrt{2\varepsilon_1}, \end{aligned} \tag{35}$$

showing Eq. (32a). Similarly, to obtain Eq. (32b),

$$\begin{aligned} \left\| \left[Z_{B,k}^i, Z_{B,l}^j \right] |\Psi\rangle \right\| &\leqslant 4\sqrt{2\varepsilon_1} + \left\| \left[Z_A^j, Z_A^i \right] |\Psi\rangle \right\| \\ &= 4\sqrt{2\varepsilon_1}. \end{aligned} \tag{36}$$

We now assume $i \neq j$. From the definition of Bob's check-round observables [Eq. (20)] we have $[X_{B,i}^i, Z_{B,i}^j] = 0$. We use this and Proposition 10 to get

$$\begin{aligned} \left\| \left[X_A^i, Z_A^j \right] |\Psi\rangle \right\| &= \left\| X_A^i Z_A^j |\Psi\rangle - Z_A^j X_A^i |\Psi\rangle \right\| \\ &\leqslant 2\sqrt{2\varepsilon_1} + \left\| X_A^i Z_A^j |\Psi\rangle - X_{B,i}^i Z_{B,i}^j |\Psi\rangle \right\| \\ &= 2\sqrt{2\varepsilon_1} + \left\| X_A^i Z_A^j |\Psi\rangle - Z_{B,i}^j X_{B,i}^i |\Psi\rangle \right\| \\ &\leqslant 4\sqrt{2\varepsilon_1} + \left\| X_A^i Z_A^j |\Psi\rangle - X_A^i Z_A^j |\Psi\rangle \right\| \\ &= 4\sqrt{2\varepsilon_1}. \end{aligned} \tag{37}$$

Combining this with the definition of Alice's observables [Eq. (17)], from which we have $[X_A^i, X_A^j] = 0$ and $[Z_A^i, Z_A^j] = 0$, yields Eq. (34). To obtain Eq. (33), we again use Proposition 10 to write

$$\left\| \left[X_{B,i}^i, Z_{B,l}^j \right] |\Psi\rangle \right\| \leqslant 4\sqrt{2\varepsilon_1} + \left\| \left[Z_A^j, X_A^i \right] |\Psi\rangle \right\| \leqslant 8\sqrt{2\varepsilon_1}, \tag{38}$$

where the final inequality uses Eq. (34) just proved. ■

We now show an intermediate result that will allow us to prove the anticommutativity of unknown local X and Z observables. The lemma shows that Alice's unknown observables for pairs of X and Z operators not acting on the same qubits anticommute (cf. the observables used in the magic square strategy of Sec. III). The proof follows a similar line to [15].

Lemma 12. For all distinct $i, j, k \in \{1, 2, 3\}$ we have anticommutation relations for Bob's game round observables,

$$\left\| \left\{ X_A^i X_A^j, Z_A^i Z_A^k \right\} |\Psi\rangle \right\| \leqslant 9\sqrt{2\varepsilon_0}. \tag{39}$$

Proof. By estimating the game-round correlations of Eq. (21) using Lemma 3, and repeatedly applying the triangle

inequality,

$$\begin{aligned}
&\left\|\left\{X_A^i X_A^j, Z_A^i Z_A^k\right\}|\Psi\rangle\right\| \\
&\leqslant 4\sqrt{2\varepsilon_0} + \left\|Z_B^{\bar{j}} X_B^{\bar{k}}|\Psi\rangle + X_B^{\bar{j}} X_B^{\bar{i}} Z_A^i Z_A^k|\Psi\rangle\right\| \\
&= 4\sqrt{2\varepsilon_0} + \left\|X_B^{\bar{j}} Z_B^{\bar{j}} X_B^{\bar{k}} Z_A^i Z_A^j|\Psi\rangle + X_B^{\bar{i}} Z_A^j Z_A^k|\Psi\rangle\right\| \\
&\leqslant 6\sqrt{2\varepsilon_0} + \left\|\left(X_B^{\bar{j}} Z_B^{\bar{j}}\right)\left(X_B^{\bar{k}} Z_B^{\bar{k}}\right)|\Psi\rangle + X_B^{\bar{i}} Z_B^{\bar{i}}|\Psi\rangle\right\| \\
&\leqslant 8\sqrt{2\varepsilon_0} + \left\|\left(Y_A^i Y_A^j\right)\left(Y_A^i Y_A^k\right)|\Psi\rangle + X_B^{\bar{i}} Z_B^{\bar{i}}|\Psi\rangle\right\| \\
&= 8\sqrt{2\varepsilon_0} + \left\|Y_A^j Y_A^k|\Psi\rangle + X_B^{\bar{i}} Z_B^{\bar{i}}|\Psi\rangle\right\| \\
&\leqslant 9\sqrt{2\varepsilon_0}, \qquad (40)
\end{aligned}$$

where the first equality results from applying unitary operators $Z_A^i Z_A^j$ and $X_B^{\bar{j}}$ inside the norm. ■

We are now in a position to prove the required anticommutativity of unknown X observables with Z observables which act on the same qubits of the unknown state.

Proposition 13 (Anticommutation). For all $i \in \{1, 2, 3\}$ we have anticommutation relations for Alice's unknown observables,

$$\left\|\left\{X_A^i, Z_A^i\right\}|\Psi\rangle\right\| \leqslant 9\sqrt{2\varepsilon_0} + 16\sqrt{2\varepsilon_1}. \qquad (41)$$

Furthermore, for all $j \in \{1, 2, 3\}$ distinct from i we have anticommutation relations for Bob's check-round observables,

$$\left\|\left\{X_{B,i}^i, Z_{B,j}^i\right\}|\Psi\rangle\right\| \leqslant 9\sqrt{2\varepsilon_0} + 20\sqrt{2\varepsilon_1}. \qquad (42)$$

Proof. Let $k \in \{1, 2, 3\}$ be distinct from i and j. Then

$$\begin{aligned}
&\left\|\left\{X_A^i, Z_A^i\right\}|\Psi\rangle\right\| \\
&= \left\|X_{B,j}^j Z_{B,i}^k \left\{X_A^i, Z_A^i\right\}|\Psi\rangle\right\| \\
&= \left\|X_A^i Z_A^i X_{B,j}^j Z_{B,i}^k|\Psi\rangle + Z_A^i X_A^i X_{B,j}^j Z_{B,i}^k|\Psi\rangle\right\| \\
&\leqslant \left\|X_A^i Z_A^i Z_{B,i}^k X_{B,j}^j|\Psi\rangle + Z_A^i X_A^i X_{B,j}^j Z_{B,i}^k|\Psi\rangle\right\| \\
&\quad + 8\sqrt{2\varepsilon_1} \\
&\leqslant \left\|X_A^i Z_{B,i}^k X_{B,j}^j Z_{B,j}^i|\Psi\rangle + Z_A^i X_{B,j}^j Z_{B,i}^k X_{B,i}^i|\Psi\rangle\right\| \\
&\quad + 10\sqrt{2\varepsilon_1} \\
&= \left\|X_A^i Z_{B,i}^k Z_{B,j}^i X_{B,j}^j|\Psi\rangle + Z_A^i X_{B,j}^j X_{B,i}^i Z_{B,i}^k|\Psi\rangle\right\| \\
&\quad + 10\sqrt{2\varepsilon_1} \\
&\leqslant \left\|\left\{X_A^i X_A^j, Z_A^i Z_A^k\right\}|\Psi\rangle\right\| + 16\sqrt{2\varepsilon_1} \\
&\leqslant 9\sqrt{2\varepsilon_0} + 16\sqrt{2\varepsilon_1}. \qquad (43)
\end{aligned}$$

For the first inequality, we commuted Bob's check-round observables using Eq. (33) of Proposition 11. For the final inequality, we applied Lemma 12 to bound the anticommutator norm. All other inequalities were found from the correlation estimates of Proposition 10.

To obtain Eq. (42), we use Proposition 10 to write

$$\begin{aligned}
\left\|\left\{X_{B,i}^i, Z_{B,j}^i\right\}|\Psi\rangle\right\| &\leqslant 4\sqrt{2\varepsilon_1} + \left\|\left\{X_A^i, Z_A^i\right\}|\Psi\rangle\right\| \\
&\leqslant 9\sqrt{2\varepsilon_0} + 20\sqrt{2\varepsilon_1}, \qquad (44)
\end{aligned}$$

where the final inequality follows from Eq. (41) just proved. ■

V. SELF-TEST OF MANY BELL STATES

We can use similar techniques to Sec. IV to self-test $n > 3$ Bell states, provided $n \equiv 3 \pmod 4$ (which we will assume throughout this section). In this case, the honest strategy is played using a $3\times n$ magic game, as described by Definition 8. The strategy for this game upon which we base our self-test will be explained in Sec. V A. The structure and honest behavior of the self-test will simultaneously be described in Sec. V B, with all general unknown observables for Alice and Bob and their required correlations then defined in Sec. V C. All commutation and anticommutation relations required to construct a local self-testing isometry will finally be shown in Sec. V D. From this, we have the final self-testing statement for many Bell states.

Theorem 14. Let $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be an unknown state shared by Alice and Bob and let $n \equiv 3 \pmod 4$ with $n > 3$ be the number of Bell states to be self-tested. Let sets of pairwise commutative, ± 1-valued, unknown observables in $\mathcal{L}(\mathcal{H}_A)$ for Alice be given as in Eq. (54), and in $\mathcal{L}(\mathcal{H}_B)$ for Bob as in Eqs. (55), (57), and (58). Suppose that these observables satisfy all correlations given in Eqs. (59)–(61) and let $\varepsilon = \max\{\varepsilon_0, \varepsilon_1, \varepsilon_2\}$. Then, for any choice $(k_i)_{i=1}^n$ of elements in $\{1, \ldots, n\}$ where each $k_i \neq i$, there exists a junk state $|\xi\rangle$ and a local isometry Φ such that, for all $i \in \{1, \ldots, n\}$,

$$\left\|\Phi|\Psi\rangle - |\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \qquad (45a)$$

$$\left\|\Phi X_A^i|\Psi\rangle - \hat{X}_A^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \qquad (45b)$$

$$\left\|\Phi Z_A^i|\Psi\rangle - \hat{Z}_A^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \qquad (45c)$$

$$\left\|\Phi X_{B,i}^i|\Psi\rangle - \hat{X}_B^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right), \qquad (45d)$$

$$\left\|\Phi Z_{B,k_i}^i|\Psi\rangle - \hat{Z}_B^i|\Phi^+\rangle_{AB}^{\otimes n} \otimes |\xi\rangle\right\| \in O\left(n^{\frac{5}{2}}\sqrt{\varepsilon}\right). \qquad (45e)$$

Proof. Take the observables $\{X_A^i, Z_A^i\}_{i=1}^n$ of Eq. (54) and $\{X_{B,i}^i, Z_{B,k_i}^i\}_{i=1}^n$ of Eq. (57) to be the (extended if necessary) reflections assumed by Theorem 6, with δ given by the largest upper bound appearing in Theorem 16. ■

Relatively few of the unknown observables defined as part of the self-test are actually used to construct the isometry, with most only serving in the proofs of necessary commutation and anticommutation relations. The total number of observables defined in Eqs. (54), (55), (57), and (58) is $2n^2 + 4n$, while only $4n$ of these are required for the isometry of Theorem 6. In particular, we are free to use any n of the $Z_{B,y}^i$ of Eq. (57) provided that we cover all qubits (denoted by the superscript index). This freedom is expressed in Theorem 14 above by choice of the k_i. In the honest case, many of the unknown observables are in fact identical to one another.

For this self-test, Bob must make Pauli measurements on pairs of qubits to ensure their commutation. This was not explicitly required in the self-test of three Bell states, since

Bob's game-round observables (corresponding to products of Pauli observables on all but one of his qubits) automatically served this purpose. We would thus like a way to subdivide all possible pairs of (an odd number of) qubits into as few disjoint sets of disjoint pairs as possible. This is equivalent to finding an optimal edge coloring for the complete graph K_n where n is odd. The following lemma constructs such a coloring.

Lemma 15. Consider the complete graph K_n for n odd, whose vertices are labeled by $V = \{1, \ldots, n\}$. For each $v \in V$, color the edges $\{v - i, v + i\}$ by color v for all $i \in \{1, \ldots, \frac{n-1}{2}\}$, where addition is performed modulo n. This is a proper n-edge-coloring for K_n and is optimal in the sense that it uses as few colors as possible.

Proof. Define the color of each edge $\{a, b\}$ to be $\frac{a+b}{2}$ (mod n), where the multiplicative inverse of 2 modulo n always exists since 2 is coprime to any odd n. Suppose that two edges $\{x, i\}$ and $\{x, j\}$ have the same color under this definition. Then $\frac{x+i}{2} \equiv \frac{x+j}{2}$ (mod n), and thus $i = j$. Therefore, no two distinct adjacent edges can have the same color. That is, we defined a proper edge coloring. Notice that all edges of the same color v here take the form $\{v - i, v + i\}$ for $i \in \{1, \ldots, \frac{n-1}{2}\}$. Hence our coloring is identical to that given in the statement. Optimality results from the fact that the chromatic index of K_n is n when n is odd. ■

Remark. If the graph is depicted by straight lines drawn between the vertices of a regular n-gon, the given construction assigns a different color to each of n sets of parallel edges.

Since we will be dealing with many noncommutative objects, we unambiguously define the finite product notation to be formed with indices in ascending order as

$$\prod_{i=1}^{n} M_i \equiv M_1 M_2, \ldots, M_n. \tag{46}$$

We will use this notation to denote the composition of (not necessarily commutative) operators.

A. Magic game strategy

A simple winning strategy for $3\times n$ magic games, in which players share three Bell states and Alice need only make single-qubit measurements, can be constructed by appending deterministic columns to the 3×3 strategy of Sec. III. However, we will base our self-test on an alternative strategy, which will be described here.

Let Alice and Bob share the n Bell states,

$$|\Psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{AB}^{(j)}. \tag{47}$$

Figure 4 depicts the $3\times n$ measurement strategy on which our self-test will be based.

Since $n \equiv 3 \pmod 4$, the observable for each square of the strategy is composed of $2 \pmod 4$ single-qubit Pauli observables. Hence the three observables in each column mutually commute and satisfy Bob's negative product rule,

$$\left(\prod_{j\neq y} \hat{X}^j\right)\left(\prod_{j\neq y} \hat{Y}^j\right)\left(\prod_{j\neq y} \hat{Z}^j\right) = \prod_{j\neq y} \hat{X}^j \hat{Y}^j \hat{Z}^j = i^{n-1} I = i^2 I = -I. \tag{48}$$

$\prod_{j\neq 1} \hat{X}^j$	$\prod_{j\neq 2} \hat{X}^j$	…	$\prod_{j\neq n} \hat{X}^j$
$\prod_{j\neq 1} \hat{Y}^j$	$\prod_{j\neq 2} \hat{Y}^j$	…	$\prod_{j\neq n} \hat{Y}^j$
$\prod_{j\neq 1} \hat{Z}^j$	$\prod_{j\neq 2} \hat{Z}^j$	…	$\prod_{j\neq n} \hat{Z}^j$

FIG. 4. The $3\times n$ magic game strategy upon which our self-test is based. Pauli observables that act on qubit j of a player's register are denoted by $\hat{X}^j$, $\hat{Y}^j$, and $\hat{Z}^j$.

Since the Pauli observables appearing in each row are all of the same type, the squares in each row mutually commute. Moreover, since Pauli observables are involutory and there are an even number of such observables corresponding to each qubit in each row, every row has product $+I$. There is also perfect correlation between Alice's and Bob's observables for each square of the strategy. That is, letting $\hat{S}$ stand for $\hat{X}$, $\hat{Y}$, or $\hat{Z}$, and for all y,

$$\langle\Psi| \prod_{j\neq y} \hat{S}_A^j \prod_{j\neq y} \hat{S}_B^j |\Psi\rangle = \prod_{j\neq y} \langle\Phi^+| \hat{S}_A^j \hat{S}_B^j |\Phi^+\rangle_{AB}^{(j)} = (\pm 1)^{n-1} = 1. \tag{49}$$

This strategy can again be naturally phrased as a winning strategy for magic games in the sense of Definition 8. Alice generates her outputs a_j as the outcomes of measurements of $\hat{X}_A^j$, $\hat{Y}_A^j$, or $\hat{Z}_A^j$ depending on whether the first, second, or third row was assigned, respectively. Bob generates his outputs (b_1, b_2, b_3) according to the outcomes of observables in Fig. 4 for the column he was assigned. By Eq. (48), Bob's outputs always satisfy the rule $b_1 b_2 b_3 = -1$. By Eq. (49), for input row and columns x and y, respectively, the outputs always satisfy $\prod_{j\neq y} a_j = b_x$. Therefore, in the strategy described, the players win with certainty.

In terms of experimental implementation, note that Alice need only make single-qubit Pauli measurements for her side of the strategy. On Bob's side, making the required compatible measurements of $\prod_{j\neq y} \hat{X}_B^j$, $\prod_{j\neq y} \hat{Y}_B^j$, and $\prod_{j\neq y} \hat{Z}_B^j$ may seem impractical for systems with large n. Note, however, that since the pairs of Pauli observables $\hat{X} \otimes \hat{X}$, $\hat{Y} \otimes \hat{Y}$, and $\hat{Z} \otimes \hat{Z}$ mutually commute, Bob need only measure $\frac{3}{2}(n-1)$ such pairs to construct measurements of all three required observables.

B. Structure and honest behavior

As in our self-test for three Bell states, Alice receives an input $x \in \{1, 2, 3\}$. However, Bob now receives an input $y \in \{1, \ldots, n\}$. Furthermore, Bob's input controlling the type of round is now a trit $c \in \{0, 1, 2\}$. The additional value $c = 2$ determines that the players are requested to check correlations between certain pairs of Pauli observables. As such, we will

call such rounds where $c = 2$ *pair check* rounds, and rename those rounds where $c = 1$ to *local check* rounds to avoid ambiguity. Alice must always output n bits, whereas the number of output bits of Bob depends on the type of round c. The protocol is summarized in Protocol 2.

Protocol 2. Protocol for certifying n Bell states. Intuitively, *pair check* rounds rule out those single-qubit $3\times n$ magic rectangle game strategies found by extending strategies for smaller $3\times n'$ games using deterministic entries. Otherwise, the required correlations could be satisfied by provers sharing fewer Bell states.

Let $n = 3 \pmod 4$ be the number of Bell states to be certified. The verifier chooses $c \in \{0, 1, 2\}$ and performs Protocol 1 with an additional subprotocol if $c = 2$ is chosen:

2. *Pair check*: Send Alice $x \in \{1, 3\}$. Alice answers with $a_1, \ldots, a_n$. Bob answers with $n-1$ bits $b_{y-k,y+k}$ and $b'_{y-k,y+k}$ in $\{+1, -1\}$ (with addition taken modulo n) for all $k \in \{1, \ldots, \frac{n-1}{2}\}$.
   (a) If $x = 1$, accept if and only if $a_i a_j = b_{i,j}$ for all i, j.
   (b) If $x = 3$, accept if and only if $a_i a_j = b'_{i,j}$ for all i, j.

Honest rounds consist of the players sharing n Bell states,

$$|\Psi\rangle = \bigotimes_{j=1}^{n} |\Phi^+\rangle_{AB}^{(j)}. \tag{50}$$

Alice always provides each of her output bits a_j by measuring the n observables of our $3\times n$ magic game strategy (Sec. V A),

$$\hat{X}_A^j \quad \text{if } x = 1, \tag{51a}$$

$$\hat{Y}_A^j \quad \text{if } x = 2, \tag{51b}$$

$$\hat{Z}_A^j \quad \text{if } x = 3. \tag{51c}$$

This is structurally identical to Eq. (15) in the previous self-test of three Bell states, with the exception that n measurements are now made upon each input.

Once again the honest behavior of Bob depends on c. If it is a game round ($c = 0$), then Bob must output three bits, as usual with the goal of winning the $3\times n$ magic game. In the case of a local check round ($c = 1$), Bob proceeds similarly to Eq. (16) of the previous self-test, but now generates his jth of n output bits depending on the input y as the measurement outcomes of Pauli observables $\hat{S}_B^j$, where

$$\hat{S}_B^j = \begin{cases} \hat{X}_B^j & \text{if } y = j, \\ \hat{Z}_B^j & \text{otherwise.} \end{cases} \tag{52}$$

Finally, if it is a pair check round ($c = 2$), Bob measures $n-1$ Pauli observables of the form $\hat{X}\otimes\hat{X}$ and $\hat{Z}\otimes\hat{Z}$ on disjoint pairs of qubits. Depending on the input y, the observables he measures are

$$\left\{\hat{X}_B^{y-j}\hat{X}_B^{y+j}\right\}_{j=1}^{(n-1)/2} \cup \left\{\hat{Z}_B^{y-j}\hat{Z}_B^{y+j}\right\}_{j=1}^{(n-1)/2}, \tag{53}$$

where addition is taken modulo n. Notice that all observables in the set of Eq. (53) mutually commute, and by the construction given in Lemma 15 the combination of all n such sets covers every possible pair of n qubits.

The correlations that we expect to be satisfied from honest check rounds are the appropriate perfect correlations between Alice and Bob. For local check rounds, these are (as before) all the single-qubit correlations $\langle\Psi|\hat{X}_A^j\hat{X}_B^j|\Psi\rangle = 1$ and $\langle\Psi|\hat{Z}_A^j\hat{Z}_B^j|\Psi\rangle = 1$. For pair check rounds, these are the correlations between all pairs of observables $\langle\Psi|\hat{X}_A^j\hat{X}_A^k\hat{X}_B^j\hat{X}_B^k|\Psi\rangle = 1$ and $\langle\Psi|\hat{Z}_A^j\hat{Z}_A^k\hat{Z}_B^j\hat{Z}_B^k|\Psi\rangle = 1$.

C. Unknown observables and correlations

Recall that, as in Sec. IV B for the previous self-test of three Bell states, all unknown observables must be labeled uniquely with respect to each observer's possible input questions in order to avoid assumptions about their measurements in this potentially dishonest case.

1. Alice's observables

We define sets of mutually commuting unknown observables on Alice's side to be measured depending on her input x as

$$\left\{X_A^j\right\}_{j=1}^n \quad \text{if } x = 1, \tag{54a}$$

$$\left\{Y_A^j\right\}_{j=1}^n \quad \text{if } x = 2, \tag{54b}$$

$$\left\{Z_A^j\right\}_{j=1}^n \quad \text{if } x = 3. \tag{54c}$$

Each of these unknown observables corresponds to a single-qubit Pauli observable which acts on the qubit of Alice indicated by its superscript.

2. Bob's observables (game rounds)

For game rounds ($c = 0$), we will denote the sets of unknown observables to be measured by Bob, depending on his input y, by

$$\left\{X_B^{\bar{y}}, Y_B^{\bar{y}}, Z_B^{\bar{y}}\right\}. \tag{55}$$

It should once again be noted that one of the observables for each input is redundant, as

$$Y_B^{\bar{y}}|\Psi\rangle = -X_B^{\bar{y}}Z_B^{\bar{y}}|\Psi\rangle \tag{56}$$

by the rule for the product of Bob's outputs (see Definition 8). We will, however, keep all for notational convenience.

3. Bob's observables (local check rounds)

For local check rounds ($c = 1$), Bob's unknown observables correspond to single-qubit Pauli $\hat{X}$ and $\hat{Z}$ observables acting on his system. The set of observables for input y is defined by

$$\left\{X_{B,y}^y\right\} \cup \left\{Z_{B,y}^j : 1 \leqslant j \leqslant n, j \neq y\right\}. \tag{57}$$

4. Bob's observables (pair check rounds)

For pair check rounds ($c = 2$), we define sets of $n-1$ observables for each input y as

$$\left\{X_B^{y-j,y+j}\right\}_{j=1}^{(n-1)/2} \cup \left\{Z_B^{y-j,y+j}\right\}_{j=1}^{(n-1)/2}, \tag{58}$$

where addition is taken modulo n. In contrast to the honest case of Eq. (53), we have not assumed that Bob's outputs

arise as the product of multiple other observables. The two superscript indices denote that these observables correspond to the product of Pauli observables on pairs of qubits. For example, the unknown observable $X_B^{1,2}$ corresponds to $\hat{X}_B^1\hat{X}_B^2$ in the honest case. In the notation we have introduced, the order of superscript indices for an unknown observable is unimportant. Thus, for convenience, we also introduce labels with reversed ordering of superscripts and identify these with observables appearing in Eq. (58). Specifically, let the labels $X_B^{i,j} \equiv X_B^{j,i}$ and $Z_B^{i,j} \equiv Z_B^{j,i}$. This is consistent with the honest case, in which the corresponding pairs of observables commute. By Lemma 15, the pairs of indices $(y-j, y+j)$ appearing in Eq. (58) for a given input y are pairwise disjoint and the combination of these pairs over every input gives every possible index pair (up to ordering of the indices). Thus the n sets of $n-1$ pair check observables defined account for measurements of $\hat{X}\otimes\hat{X}$ and $\hat{Z}\otimes\hat{Z}$ on every possible pair of n qubits and, moreover, the observables for a given input mutually commute in the honest case as expected.

5. Correlations

The correlations of unknown observables amounting to a uniformly ε_0-close to perfect strategy for the $3\times n$ magic game (i.e., correlations obtained in game rounds) are, with reference to the winning strategy described in Sec. V A,

$$\left\langle \left(\prod_{j\neq k} X_A^j\right) X_B^{\bar{k}} \right\rangle \geqslant 1-\varepsilon_0, \tag{59a}$$

$$-\left\langle \left(\prod_{j\neq k} Y_A^j\right) X_B^{\bar{k}} Z_B^{\bar{k}} \right\rangle \geqslant 1-\varepsilon_0, \tag{59b}$$

$$\left\langle \left(\prod_{j\neq k} Z_A^j\right) Z_B^{\bar{k}} \right\rangle \geqslant 1-\varepsilon_0. \tag{59c}$$

The correlations constituting uniformly ε_1-close to perfect local check rounds are, for all distinct $i, j \in \{1,\ldots,n\}$,

$$\langle X_A^i X_{B,i}^i \rangle \geqslant 1-\varepsilon_1, \tag{60a}$$

$$\langle Z_A^i Z_{B,j}^i \rangle \geqslant 1-\varepsilon_1. \tag{60b}$$

The correlations describing uniformly ε_2-close to perfect pair check rounds are, for all distinct $i, j \in \{1,\ldots,n\}$,

$$\langle X_A^i X_A^j X_B^{i,j} \rangle \geqslant 1-\varepsilon_2, \tag{61a}$$

$$\langle Z_A^i Z_A^j Z_B^{i,j} \rangle \geqslant 1-\varepsilon_2. \tag{61b}$$

From the assumption that all of these correlations are satisfied for our unknown observables, we will deduce appropriate commutation and anticommutation relations which imply the existence of a local self-testing isometry by Theorem 6.

D. Commutation and anticommutation relations

Here we will deduce the appropriate state-dependent commutation and anticommutation relations of our unknown reflections from which a local self-testing isometry can be constructed. The results of this section are summarized in the following theorem.

Theorem 16. Let $i, j, k, l \in \{1,\ldots,n\}$ be such that $i \neq k$ and $j \neq l$. We have correlations between each unknown observable of Alice with each of the corresponding observables on Bob's side,

$$\left\|\left(X_A^i - X_{B,i}^i\right)|\Psi\rangle\right\| \leqslant \sqrt{2\varepsilon_1}, \tag{62}$$

$$\left\|\left(Z_A^i - Z_{B,k}^i\right)|\Psi\rangle\right\| \leqslant \sqrt{2\varepsilon_1}. \tag{63}$$

We have the state-dependent anticommutativity of all unknown X observables with all unknown Z observables corresponding to the same qubit,

$$\left\|\left\{X_A^i, Z_A^i\right\}|\Psi\rangle\right\| \leqslant 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 17\right)\sqrt{2\varepsilon_1}, \tag{64}$$

$$\left\|\left\{X_{B,i}^i, Z_{B,k}^i\right\}|\Psi\rangle\right\| \leqslant 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 21\right)\sqrt{2\varepsilon_1}. \tag{65}$$

Finally, we have the state-dependent commutativity of unknown X and Z observables. On Bob's side, we have

$$\left\|\left[X_{B,i}^i, X_{B,j}^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{66}$$

$$\left\|\left[Z_{B,k}^i, Z_{B,l}^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}; \tag{67}$$

and moreover restricting to observables corresponding to different qubits $i \neq j$,

$$\left\|\left[X_{B,i}^i, Z_{B,l}^j\right]|\Psi\rangle\right\| \leqslant 8\sqrt{2\varepsilon_1}. \tag{68}$$

On Alice's side, for different qubits $i \neq j$, we have

$$\left\|\left[M_A^i, N_A^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{69}$$

where M and N can be either of X and Z.

Proof. Combine Propositions 17–19. ∎

We begin by expressing the correlations of Eq. (60), between those observables of the players corresponding to local Pauli observables acting on the same qubit, in terms of norms.

Proposition 17 (Correlation). For all distinct $i, j \in \{1,\ldots,n\}$ we have the correlation estimates

$$\left\|\left(X_A^i - X_{B,i}^i\right)|\Psi\rangle\right\| \leqslant \sqrt{2\varepsilon_1}, \tag{70a}$$

$$\left\|\left(Z_A^i - Z_{B,j}^i\right)|\Psi\rangle\right\| \leqslant \sqrt{2\varepsilon_1}. \tag{70b}$$

Proof. Apply Lemma 3 to the correlations given in Eq. (60). ∎

We now show the required state-dependent commutation relations for observables that correspond to local Pauli observables acting on different qubits. Since observables of Alice are defined to commute exactly with those of Bob, it is only necessary to consider state-dependent commutation relations on each side separately.

Proposition 18 (Commutation). For all $i, j, k, l \in \{1,\ldots,n\}$ such that $i \neq k$ and $j \neq l$, we have

$$\left\|\left[X_{B,i}^i, X_{B,j}^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{71a}$$

$$\left\|\left[Z_{B,k}^i, Z_{B,l}^j\right]|\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}. \tag{71b}$$

Moreover, if $i \neq j$ we have commutation relations for Bob,

$$\left\| \left[X^i_{B,i}, Z^j_{B,l} \right] |\Psi\rangle \right\| \leqslant 8\sqrt{2\varepsilon_1} \tag{72}$$

and for Alice,

$$\left\| \left[M^i_A, N^j_A \right] |\Psi\rangle \right\| \leqslant 4\sqrt{2\varepsilon_1}, \tag{73}$$

where M and N can be either of X and Z.

Proof. As the proof of Proposition 11, but using the correlations of Eq. (60) instead of Eq. (22). ■

The following proposition states the robust state-dependent anticommutation relations between each pair of unknown X and Z observables corresponding to the same qubit, depending on the correlation errors ε_0, ε_1, and ε_2. A sketch proof is given below for the ideal case with vanishing errors, with the more lengthy, full proof being the contents of the Appendix.

Proposition 19 (Anticommutation). For all $i \in \{1, \ldots, n\}$ we have state-dependent anticommutation relations for unknown observables of Alice,

$$\left\| \left\{ X^i_A, Z^i_A \right\} |\Psi\rangle \right\| \leqslant 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 17 \right) \sqrt{2\varepsilon_1}. \tag{74}$$

Furthermore, for all $j \in \{1, \ldots, n\}$ distinct from i we have state-dependent anticommutation relations for Bob's check-round observables

$$\left\| \left\{ X^i_{B,i}, Z^i_{B,j} \right\} |\Psi\rangle \right\| \leqslant 3n\sqrt{2\varepsilon_0} + 2(n-1)\sqrt{2\varepsilon_2} + \left(\frac{13(n-1)}{2} + 21 \right) \sqrt{2\varepsilon_1}. \tag{75}$$

Sketch proof. For the sake of sketching the proof, take correlation errors to vanish $\varepsilon_0 = \varepsilon_1 = \varepsilon_2 = 0$. We will show the state-dependent anticommutation relation $\{X^1_A, Z^1_A\}|\Psi\rangle = 0$. The relations for observables corresponding to the other qubits follow similarly.

From the game correlations Eq. (59b), we have

$$\left(\prod_{k=2}^{n} Z^{\bar{k}}_B X^{\bar{k}}_B \right) |\Psi\rangle + Z^{\bar{1}}_B X^{\bar{1}}_B |\Psi\rangle = 0, \tag{76}$$

where the sign of the first term uses that n is odd. Swapping to Alice's side those observables acting immediately on the state and multiplying on the left by appropriate unitary operators gives

$$X^{\bar{2}}_B \left(\prod_{k=3}^{n-1} Z^{\bar{k}}_B X^{\bar{k}}_B \right) Z^{\bar{n}}_B |\Psi\rangle + Z^{\bar{2}}_B Z^{\bar{1}}_B X^n_A X^1_A |\Psi\rangle = 0. \tag{77}$$

Rewriting this by commuting those X and Z observables within each term of the product with k odd results in

$$\left(\prod_{k=1}^{(n-3)/2} X^{\overline{2k}}_B X^{\overline{2k+1}}_B Z^{\overline{2k+1}}_B Z^{\overline{2k+2}}_B \right) X^{\overline{n-1}}_B Z^{\bar{n}}_B |\Psi\rangle + Z^{\bar{2}}_B Z^{\bar{1}}_B X^n_A X^1_A |\Psi\rangle = 0. \tag{78}$$

Using the correlations of Eqs. (59a) and (59c) to swap Bob's observables to Alice's side (and freely inserting the identity operator as $X^{n-1}_A X^{n-1}_A$ into the resulting first term) yields

$$\left(\prod_{k \neq n} Z^k_A \right) \left(\prod_{k} X^k_A \right) \left(\prod_{k=1}^{(n-3)/2} X^{n-2k+1}_A Z^{n-2k+1}_A Z^{n-2k}_A X^{n-2k}_A \right) X^2_A |\Psi\rangle + X^n_A X^1_A Z^1_A Z^2_A |\Psi\rangle = 0. \tag{79}$$

From the correlations of Eq. (60) we have

$$X^2_A Z^1_{B,n} Z^2_{B,n} X^n_{B,n} X^1_{B,1} |\Psi\rangle = X^n_{B,n} Z^{1,2}_B X^{1,2}_B |\Psi\rangle. \tag{80}$$

Hence multiplying Eq. (79) on the left by $Z^1_{B,n} Z^2_{B,n} X^n_{B,n} X^1_{B,1}$, applying Eq. (80) via the triangle inequality in its first term (commuting the resulting observables for Bob with the existing observables of Alice), and in its second term using the correlations of Eq. (60),

$$X^n_{B,n} Z^{1,2}_B X^{1,2}_B \left(\prod_{k \neq n} Z^k_A \right) \left(\prod_{k} X^k_A \right) \left(\prod_{k=1}^{(n-3)/2} X^{n-2k+1}_A Z^{n-2k+1}_A Z^{n-2k}_A X^{n-2k}_A \right) |\Psi\rangle + \left(X^n_A X^1_A Z^1_A Z^2_A \right)^2 |\Psi\rangle = 0. \tag{81}$$

Lemma 20 shows for all $k \in \{1, \ldots, \frac{n-3}{4}\}$ that in particular

$$\left(X^{4k+2}_A Z^{4k+2}_A Z^{4k+1}_A X^{4k+1}_A \right) \left(X^{4k}_A Z^{4k}_A Z^{4k-1}_A X^{4k-1}_A \right) |\Psi\rangle = X^{4k-1,4k+1}_B Z^{4k-1,4k+1}_B Z^{4k,4k+2}_B X^{4k,4k+2}_B |\Psi\rangle. \tag{82}$$

Since $n \equiv 3 \pmod 4$, we can consider successive pairs of terms in the final product of Eq. (81). We can replace each pair of these terms using pair check observables by repeatedly applying Eq. (82) and commuting the resulting observables of Bob with

those of Alice. This gives

$$X_{B,n}^{n} Z_B^{1,2} X_B^{1,2} \left(\prod_{k=1}^{(n-3)/4} X_B^{4k-1,4k+1} Z_B^{4k-1,4k+1} Z_B^{4k,4k+2} X_B^{4k,4k+2} \right) \left(\prod_{k \neq n} Z_A^k \right) \left(\prod_k X_A^k \right) |\Psi\rangle + \left(X_A^n X_A^1 Z_A^1 Z_A^2 \right)^2 |\Psi\rangle = 0. \tag{83}$$

Lemma 21 with $\sigma = \mathrm{id}$ chosen to be the identity permutation shows

$$\left(\prod_{k \neq n} Z_A^k \right) \left(\prod_k X_A^k \right) |\Psi\rangle = X_A^n X_B^{1,2} \left(\prod_{k=1}^{(n-3)/4} X_B^{4k-1,4k+1} X_B^{4k,4k+2} \right) Z_B^{1,2} \left(\prod_{k=1}^{(n-3)/4} Z_B^{4k-1,4k+1} Z_B^{4k,4k+2} \right) |\Psi\rangle. \tag{84}$$

If we assume that all pair check observables appearing in Eq. (83) are measured as part of the same (pair check round) input for Bob (which is compatible with an honest strategy since all of these observables have either disjoint or identical superscript index pairs to all others), then all such observables mutually commute. Thus applying Eq. (84) to Eq. (83) and using the involutory property of all pair check observables to achieve many cancellations, we get

$$X_A^n X_{B,n}^n |\Psi\rangle + \left(X_A^n X_A^1 Z_A^1 Z_A^2 \right)^2 |\Psi\rangle = 0. \tag{85}$$

It should be noted that, for the simplicity of this sketch, the set of mutually commuting pair check observables used as an input here does not necessarily match one of the inputs defined in Eq. (58). Nonetheless, it is still the case that only n such sets must be used to complete the proof for all anticommutation relations of Alice's observables, and (with the proof essentially unchanged) the set used here matches one of those in Eq. (58) under a suitable permutation of the qubit labels.

Applying the correlations of Eq. (60a) once in the first term of Eq. (85) and then multiplying on the left by $Z_A^2 Z_A^1 X_A^1 X_A^n$ gives

$$\left\{ X_A^1 X_A^n, Z_A^1 Z_A^2 \right\} |\Psi\rangle = 0. \tag{86}$$

By identical argument to the proof of Proposition 13, but using Propositions 17 and 18 instead of Propositions 10 and 11 and using Eq. (86) in place of Lemma 12, this implies the desired state-dependent anticommutation relation $\{X_A^1, Z_A^1\}|\Psi\rangle = 0$ for Alice's observables.

The state-dependent anticommutation relations for Bob can all be obtained by simple application of Proposition 17, given those just proved for Alice's observables. ■

VI. DISCUSSION

In this work, we introduced one-side-local quantum strategies for the magic square and $3 \times n$ magic rectangle games that win with certainty. We then supplemented these strategies with some extra correlations obtained via "check" rounds to obtain the desired self-tests. Our final result is a parallel self-test for n maximally entangled Bell states, which has several practical advantages over other protocols. Being a parallel self-test of n Bell states, our protocol makes no assumptions within the n single-qubit systems of each side.

We examine first the experimental requirements of realizing our self-test—something that is determined by the honest runs. All observables used in the honest strategy for our self-test can be implemented as the tensor product of at most two Pauli operators (of the same type) acting on different pairs of qubits. A unique advantage of our work is that, moreover, Alice need only ever make local measurements of single-qubit Pauli observables in the honest case. This is especially important for major uses of self-testing. For example, in the context of delegated quantum computation, the "client" could have very limited quantum capabilities. It suffices that they are able to measure single qubits in Pauli bases.

Another interesting property of our self-test concerns its communication complexity. Of particular importance is the size of input questions, which quantify how much randomness must be consumed by the protocol in each round of interaction. Our test requires constant size (1 trit) input questions for Alice, and for Bob it requires $O(\log_2 n)$ bit inputs. With a few exceptions [27–30] (in each of which robustness is either not explicitly constructed or doubly exponential in n), other works have achieved at best logarithmic input complexities (see, for example, Refs. [22,24]). In our protocol, one of the players need only receive questions of a constant size. Players must each output $O(n)$ bit answers, except for in game rounds, in which Bob need only return 2 bit outputs.

Our protocol also has the practical advantage that it makes use of solely perfect correlations; any optimal strategy succeeds with certainty, thus requiring fewer rounds of experiment to achieve a desired statistical confidence.

The final figure of merit that we consider is robustness to noise. Given correlations that are at worst ε-close to perfect, using a self-testing theorem that can be found in [13], our results achieve a robustness that is $O(n^{\frac{5}{2}}\sqrt{\varepsilon})$ for the collection of Bell states and all single-qubit Pauli observables. That is, to achieve a robustness δ it is sufficient that $\varepsilon(n, \delta) \in O(n^{-5}\delta^2)$. The self-testing works of Coladangelo [13] and Coudron and Natarajan [21] using instead the parallel repetition of the magic square game as a basis perform slightly better in this regard, with $\varepsilon(n, \delta) \in O(n^{-3}\delta^2)$ and $\varepsilon(n, \delta) \in O(n^{-4}\delta^4)$ being sufficient for robustness δ, respectively. The work of Coudron and Natarajan [21] achieves robustness for observables acting on all qubits simultaneously, however both works are examples of strictly parallel self-tests and thus necessarily require $O(n)$ bit inputs. A protocol of Natarajan and Vidick [23] exhibits the interesting property that its robustness does not depend on n. The same authors later extended this work to have communication complexity only logarithmic in the number of entangled states to be certified. The protocol, however, instead self-tests N maximally entangled *qudit* states and corresponding single-*qudit* Pauli observables defined over a finite field $\mathbb{F}_q$, where q increases with N [24]. It is unclear whether the honest strategy provided can be realized with local measurements with respect to Bell states [33].

TABLE I. Comparison between certain protocols capable of self-testing n EPR pairs in parallel. Cells highlighted in green depict favorable comparisons within the property being considered. Those in red compare unfavorably and those in yellow neutrally. We consider whether the honest strategy of each protocol uses only local (single-qubit) measurements, is constructed entirely from measurements of the Pauli group (on standard Bell states), and makes use of only perfect correlations (so that the strategy wins with certainty). The error tolerance $\varepsilon(n,\delta)$ is a sufficient maximum error in the observed correlations so that the states and measurements tested (up to local isometry) are a distance at most δ from ideal. Input question sizes (the amounts of randomness consumed) are given in units of information.

Protocol	Local	Pauli	Perfect corr.	Error tol. $\varepsilon(n,\delta)$	Input size	
					Alice	Bob
$3\times n$ protocol (**this work**)	Alice	Yes	Yes	$O(n^{-5}\delta^2)$	$O(1)$	$O(\log n)$
Šupić *et al.* [27]	Depends on base self-tests			N/A	$O(1)$	
Chao *et al.* [22]	Yes	No	No	$O(n^{-5}\delta^2)$	$O(\log n)$	
Natarajan and Vidick [24]	No	No	Yes	$O(\text{poly}(\delta))$	$O(\text{poly}(\log n))$	
Natarajan and Vidick [23]	As CHSH or magic square			$O(\delta^{16})$	$O(n)$	
Coladangelo [13] (magic square)	No	Yes	Yes	$O(n^{-3}\delta^2)$	$O(n)$	
Coladangelo [13] (CHSH)	Yes	No	No	$O(n^{-3}\delta^2)$	$O(n)$	
Coudron and Natarajan [21]	No	Yes	Yes	$O(n^{-4}\delta^4)$	$O(n)$	
McKague [20] (Mayers–Yao)	Yes	No	No	$O(n^{-8}\delta^8)$	$O(\log\log n)$	

Our protocol is unique in that it achieves several desirable properties simultaneously. The prover with minimal quantum-technological capabilities (the client) need only make local single-qubit measurements in Pauli bases upon accepting questions all of constant size. Despite this, our protocol relies entirely on perfect correlations, maintains a noise tolerance comparable with that of most others, and requires questions provided to the server to be of size at most logarithmic in the number of Bell states tested. Sample comparisons with some other protocols can be found in Table I. The list of works included is not exhaustive, and other figures of merit could also be considered depending on intended applications.

Future works

Aside from our self-testing result, all self-tests whose honest strategies rely solely on the magic square game (such as those of [13,21]) can of course be implemented using our one-side-local strategy if desired. It may also be possible to use our one-side-local strategy as a direct replacement for honest subroutines in other protocols (such as the CHSH game in the protocol of Chao *et al.* [22] or for the anticommutation test of Natarajan and Vidick [23]), allowing them to function with the additional benefits of local Pauli measurements and perfect correlations at the same time.

In this work, we made use of a theorem of Coladangelo [13] to translate our main state-dependent commutation/anticommutation results into a proper self-testing statement on the existence of a desired local isometry. Other choices of isometry could equally well have been made. On the one hand, other results based on the relevant commutativity and anticommutativity of untrusted observables exist. For example, a result of Ref. [20] (Lemma 6) could be directly substituted for that used here, offering the additional property of simultaneously testing multiple Pauli measurements at the cost of poorer robustness scaling $\varepsilon(n,\delta)\in O(n^{-8}\delta^4)$. On the other hand, it would be interesting to examine the plausibility of more robust isometries for our self-test. Such isometries could arise either as improved general techniques for the construction of self-testing isometries given certain relations between the untrusted observables (similar to [13,20]), or alternatively in the form of specially constructed isometries making use of features unique to the testing scenario. Another possible future direction is to study the robustness of our protocol experimentally (or numerically under the semidefinite-programming characterization of quantum correlations [34–37]).

Adaptation of our results for device-independent versions of delegated verifiable blind quantum computation protocols, or other secure quantum computation protocols [38,39], could be explored. The utility of our protocol for device-independent quantum key distribution could also be examined.

ACKNOWLEDGMENTS

S.A.A. gratefully acknowledges EPSRC studentship funding under Grant No. EP/R513209/1. P.W. acknowledges support by the UK Hub in Quantum Computing and Simulation, part of the UK National Quantum Technologies Programme with funding from EPSRC Grant No. EP/T001062/1.

APPENDIX: ROBUST ANTICOMMUTATION RELATIONS

Lemma 20. For all distinct $i,j,k,l\in\{1,\ldots,n\}$ we have the estimate between Alice's observables and Bob's pair check observables,

$$\left\|\left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\Psi\rangle - X_B^{i,k} Z_B^{i,k} Z_B^{j,l} X_B^{j,l}|\Psi\rangle\right\| \leqslant 18\sqrt{2\varepsilon_1} + 4\sqrt{2\varepsilon_2}. \tag{A1}$$

Proof. First, commuting X_A^j with X_A^k (as they correspond to the same input) and then using Proposition 17 and the triangle inequality to swap four of Alice's observables to Bob's side, we have

$$\left\|\left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\Psi\rangle - X_A^l Z_A^l Z_A^k X_A^j X_A^i X_{B,i}^i Z_{B,k}^i Z_{B,k}^j X_{B,k}^k |\Psi\rangle\right\| \leqslant 4\sqrt{2\varepsilon_1}. \tag{A2}$$

Commuting $X_{B,k}^k$ with observables of the same input ($Z_{B,k}^i$ and $Z_{B,k}^j$) and then again using the correlations to swap observables back to Alice's side gives

$$\left\|\left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\Psi\rangle - X_A^l Z_A^l Z_A^k X_A^j Z_A^j Z_A^i X_A^k X_A^i |\Psi\rangle\right\| \leqslant 8\sqrt{2\varepsilon_1}. \tag{A3}$$

Applying Eq. (61a) correlations between Alice's observables and Bob's pair check observables once followed by swapping five of Alice's observables to Bob's side gives

$$\left\|\left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\Psi\rangle - X_B^{i,k} X_A^l Z_{B,l}^i Z_{B,l}^j X_{B,j}^j Z_{B,j}^k Z_{B,j}^l |\Psi\rangle\right\| \leqslant 13\sqrt{2\varepsilon_1} + \sqrt{2\varepsilon_2}. \tag{A4}$$

Commuting $X_{B,j}^j$ with observables of the same input ($Z_{B,j}^k$ and $Z_{B,j}^l$) and again swapping local check observables back to Alice's side yields

$$\left\|\left(X_A^l Z_A^l Z_A^k X_A^k\right)\left(X_A^j Z_A^j Z_A^i X_A^i\right)|\Psi\rangle - X_B^{i,k} X_A^l X_A^j Z_A^l Z_A^k Z_A^j Z_A^i |\Psi\rangle\right\| \leqslant 18\sqrt{2\varepsilon_1} + \sqrt{2\varepsilon_2}. \tag{A5}$$

Finally, commuting Z_A^j with Z_A^k and applying three correlations of Eq. (61) to switch all observables of Alice with pair check observables of Bob gives the result.

Lemma 21. For any permutation σ of $\{1, \ldots, n\}$, letting $\sigma_k = \sigma(k)$ for each k, we have the estimate

$$\left\|\left(\prod_{k\neq n} Z_A^{\sigma_k}\right)\left(\prod_k X_A^{\sigma_k}\right)|\Psi\rangle - X_A^{\sigma_n} X_B^{\sigma_1,\sigma_2}\left(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} X_B^{\sigma_{4k},\sigma_{4k+2}}\right)\right.$$
$$\left. Z_B^{\sigma_1,\sigma_2}\left(\prod_{k=1}^{(n-3)/4} Z_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k},\sigma_{4k+2}}\right)|\Psi\rangle\right\| \leqslant 2n\sqrt{2\varepsilon_1} + (n-1)\sqrt{2\varepsilon_2}. \tag{A6}$$

Proof. Noting that all the X_A^k pairwise commute and using the correlations of Eq. (61a) to swap Alice's observables with Bob's pair check observables,

$$\left\|\left(\prod_{k\neq n} Z_A^{\sigma_k}\right)\left(\prod_k X_A^{\sigma_k}\right)|\Psi\rangle - X_B^{\sigma_1,\sigma_2}\left(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} X_B^{\sigma_{4k},\sigma_{4k+2}}\right)\left(\prod_{k\neq n} Z_A^{\sigma_k}\right) X_A^{\sigma_n}|\Psi\rangle\right\| \leqslant \frac{n-1}{2}\sqrt{2\varepsilon_2}. \tag{A7}$$

Consider only the final part of the second term in Eq. (A7). We can repeatedly apply the triangle inequality with Proposition 17 to write

$$\left\|\left(\prod_{k\neq n} Z_A^{\sigma_k}\right) X_A^{\sigma_n}|\Psi\rangle - X_{B,\sigma_n}^{\sigma_n}\left(\prod_{k\neq n} Z_{B,\sigma_n}^{\sigma_k}\right)|\Psi\rangle\right\| \leqslant n\sqrt{2\varepsilon_1}. \tag{A8}$$

Since all of Bob's observables in this equation correspond to the same input, we can commute $X_{B,\sigma_n}^{\sigma_n}$ with the product to its right and then use Proposition 17 again to give

$$\left\|\left(\prod_{k\neq n} Z_A^{\sigma_k}\right) X_A^{\sigma_n}|\Psi\rangle - X_A^{\sigma_n}\left(\prod_{k\neq n} Z_A^{\sigma_k}\right)|\Psi\rangle\right\| \leqslant 2n\sqrt{2\varepsilon_1}. \tag{A9}$$

Combining this with Eq. (A7) via the triangle inequality yields

$$\left\|\left(\prod_{k\neq n} Z_A^{\sigma_k}\right)\left(\prod_k X_A^{\sigma_k}\right)|\Psi\rangle - X_A^{\sigma_n} X_B^{\sigma_1,\sigma_2}\left(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} X_B^{\sigma_{4k},\sigma_{4k+2}}\right)\left(\prod_{k\neq n} Z_A^{\sigma_k}\right)|\Psi\rangle\right\| \leqslant 2n\sqrt{2\varepsilon_1} + \frac{n-1}{2}\sqrt{2\varepsilon_2}. \tag{A10}$$

Finally, since all the Z_A^k pairwise commute, the correlations of Eq. (61b) imply

$$\left\|\left(\prod_{k\neq n} Z_A^{\sigma_k}\right)|\Psi\rangle - Z_B^{\sigma_1,\sigma_2}\left(\prod_{k=1}^{(n-3)/4} Z_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k},\sigma_{4k+2}}\right)|\Psi\rangle\right\| \leqslant \frac{n-1}{2}\sqrt{2\varepsilon_2}. \tag{A11}$$

Combining this with the previous Eq. (A10) using the triangle inequality yields the result. ■

We now exhibit the full proof of Proposition 19 with nonzero correlation errors.

Proof of Proposition 19. Let $i \in \{1, \ldots, n\}$ and let $\sigma_k = \sigma(k)$ for each $k \in \{1, \ldots, n\}$, where σ is some permutation of $\{1, \ldots, n\}$. Assume that σ is such that $\sigma_1 = i$. From the game correlations Eq. (59b) we have

$$\left\| \left(\prod_{k=2}^{n} Y_A^{\sigma_k} \right) |\Psi\rangle + Z_B^{\overline{\sigma_1}} X_B^{\overline{\sigma_1}} |\Psi\rangle \right\| \leqslant \sqrt{2\varepsilon_0}. \tag{A12}$$

Again, from the same correlations,

$$\left\| \left(\prod_{k=2}^{n} Z_B^{\overline{\sigma_k}} X_B^{\overline{\sigma_k}} \right) |\Psi\rangle + Z_B^{\overline{\sigma_1}} X_B^{\overline{\sigma_1}} |\Psi\rangle \right\| \leqslant n\sqrt{2\varepsilon_0}, \tag{A13}$$

where the sign of the first term uses that n is odd. Now using the game correlations Eq. (59a),

$$\left\| \left(\prod_{k=2}^{n-1} Z_B^{\overline{\sigma_k}} X_B^{\overline{\sigma_k}} \right) Z_B^{\overline{\sigma_n}} \left(\prod_{k\neq n} X_A^{\sigma_k} \right) |\Psi\rangle + Z_B^{\overline{\sigma_1}} \left(\prod_{k\neq 1} X_A^{\sigma_k} \right) |\Psi\rangle \right\| \leqslant (n+2)\sqrt{2\varepsilon_0}. \tag{A14}$$

Multiplying on the left by the unitary operators $\prod_{k\neq n} X_A^{\sigma_k}$ and $Z_B^{\overline{\sigma_2}}$ leaves the norm unchanged and gives

$$\left\| X_B^{\overline{\sigma_2}} \left(\prod_{k=3}^{n-1} Z_B^{\overline{\sigma_k}} X_B^{\overline{\sigma_k}} \right) Z_B^{\overline{\sigma_n}} |\Psi\rangle + Z_B^{\overline{\sigma_2}} Z_B^{\overline{\sigma_1}} X_A^{\sigma_n} X_A^{\sigma_1} |\Psi\rangle \right\| \leqslant (n+2)\sqrt{2\varepsilon_0}. \tag{A15}$$

Rewriting this by commuting those X and Z observables within each term of the product with k odd results in

$$\left\| \left(\prod_{k=1}^{(n-3)/2} X_B^{\overline{\sigma_{2k}}} X_B^{\overline{\sigma_{2k+1}}} Z_B^{\overline{\sigma_{2k+1}}} Z_B^{\overline{\sigma_{2k+2}}} \right) X_B^{\overline{\sigma_{n-1}}} Z_B^{\overline{\sigma_n}} |\Psi\rangle + Z_B^{\overline{\sigma_2}} Z_B^{\overline{\sigma_1}} X_A^{\sigma_n} X_A^{\sigma_1} |\Psi\rangle \right\| \leqslant (n+2)\sqrt{2\varepsilon_0}. \tag{A16}$$

Using the correlations of Eq. (59a) and (59c) to swap Bob's observables to Alice's side (and freely inserting the identity operator as $X_A^{\sigma_{n-1}} X_A^{\sigma_{n-1}}$ into the resulting first term) yields

$$\left\| \left(\prod_{k\neq n} Z_A^{\sigma_k} \right) \left(\prod_{k} X_A^{\sigma_k} \right) \left(\prod_{k=1}^{(n-3)/2} X_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k}} X_A^{\sigma_{n-2k}} \right) X_A^{\sigma_2} |\Psi\rangle + X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2} |\Psi\rangle \right\| \leqslant 3n\sqrt{2\varepsilon_0}. \tag{A17}$$

Now notice from the correlations of Eq. (60) we have the estimate

$$\left\| X_A^{\sigma_2} Z_{B,\sigma_n}^{\sigma_1} Z_{B,\sigma_n}^{\sigma_2} X_{B,\sigma_n}^{\sigma_n} X_{B,\sigma_1}^{\sigma_1} |\Psi\rangle - X_{B,\sigma_n}^{\sigma_n} Z_B^{\sigma_1,\sigma_2} X_B^{\sigma_1,\sigma_2} |\Psi\rangle \right\| \leqslant 3\sqrt{2\varepsilon_1} + 2\sqrt{2\varepsilon_2}, \tag{A18}$$

where we achieved this by commuting $X_{B,\sigma_n}^{\sigma_n}$ with other observables of the same input and converting local check observables to observables of Alice and then to pair check observables. Hence multiplying Eq. (A17) on the left by $Z_{B,\sigma_n}^{\sigma_1} Z_{B,\sigma_n}^{\sigma_2} X_{B,\sigma_n}^{\sigma_n} X_{B,\sigma_1}^{\sigma_1}$, applying Eq. (A18) via the triangle inequality in its first term (commuting the resulting observables for Bob with the existing observables of Alice), and in its second term using the correlations of Eq. (60),

$$\begin{aligned} &\left\| X_{B,\sigma_n}^{\sigma_n} Z_B^{\sigma_1,\sigma_2} X_B^{\sigma_1,\sigma_2} \left(\prod_{k\neq n} Z_A^{\sigma_k} \right) \left(\prod_{k} X_A^{\sigma_k} \right) \left(\prod_{k=1}^{(n-3)/2} X_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k+1}} Z_A^{\sigma_{n-2k}} X_A^{\sigma_{n-2k}} \right) |\Psi\rangle + \left(X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2} \right)^2 |\Psi\rangle \right\| \\ &\quad \leqslant 3n\sqrt{2\varepsilon_0} + 7\sqrt{2\varepsilon_1} + 2\sqrt{2\varepsilon_2}. \end{aligned} \tag{A19}$$

Since $n \equiv 3 \pmod 4$, we can consider successive pairs of terms in the final product of Eq. (A19). We can estimate each pair of terms using pair check observables by repeatedly applying the estimate of Lemma 20 in the first term and commuting the resulting observables of Bob with those of Alice. This gives

$$\begin{aligned} &\left\| X_{B,\sigma_n}^{\sigma_n} Z_B^{\sigma_1,\sigma_2} X_B^{\sigma_1,\sigma_2} \left(\prod_{k=1}^{(n-3)/4} X_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k-1},\sigma_{4k+1}} Z_B^{\sigma_{4k},\sigma_{4k+2}} X_B^{\sigma_{4k},\sigma_{4k+2}} \right) \left(\prod_{k\neq n} Z_A^{\sigma_k} \right) \left(\prod_{k} X_A^{\sigma_k} \right) |\Psi\rangle + \left(X_A^{\sigma_n} X_A^{\sigma_1} Z_A^{\sigma_1} Z_A^{\sigma_2} \right)^2 |\Psi\rangle \right\| \\ &\quad \leqslant 3n\sqrt{2\varepsilon_0} + \left(\frac{9(n-3)}{2} + 7 \right) \sqrt{2\varepsilon_1} + (n-1)\sqrt{2\varepsilon_2}. \end{aligned} \tag{A20}$$

We may assume the permutation σ to in fact be such that all pair check observables appearing in Eq. (A6) of Lemma 21 and Eq. (A20) correspond to the same (pair check round) input for Bob. This is compatible with an honest behavior (in which pair check observables correspond to pairs of Pauli observables) since all of these observables $M_B^{l,m}$ (where M represents either X or Z) have either disjoint or identical indices to all others. Specifically, referring to the definition [see Eq. (53)] of Bob's observables to be measured upon an input y when $c = 2$, we may assume they all correspond to the input $y = \sigma_n$, in which qubit σ_n is not

to be tested. Therefore, after applying the estimate of Lemma 21 to the first term in Eq. (A20), we may freely commute all pair check observables and use their involutory property to achieve many cancellations. This yields

$$\left\|X_A^{\sigma_n}X_{B,\sigma_n}^{\sigma_n}|\Psi\rangle+\left(X_A^{\sigma_n}X_A^{\sigma_1}Z_A^{\sigma_1}Z_A^{\sigma_2}\right)^2|\Psi\rangle\right\|\leqslant 3n\sqrt{2\varepsilon_0}+\frac{13(n-1)}{2}\sqrt{2\varepsilon_1}+2(n-1)\sqrt{2\varepsilon_2}. \tag{A21}$$

Applying the correlations of Eq. (60a) once in the first term and then multiplying on the left by $Z_A^{\sigma_2}Z_A^{\sigma_1}X_A^{\sigma_1}X_A^{\sigma_n}$ gives

$$\left\|\left\{X_A^{\sigma_1}X_A^{\sigma_n},Z_A^{\sigma_1}Z_A^{\sigma_2}\right\}|\Psi\rangle\right\|\leqslant 3n\sqrt{2\varepsilon_0}+\left(\frac{13(n-1)}{2}+1\right)\sqrt{2\varepsilon_1}+2(n-1)\sqrt{2\varepsilon_2}. \tag{A22}$$

By identical argument to the proof of Proposition 13, but using Propositions 17 and 18 instead of Propositions 10 and 11 and using the bound of Eq. (A22) in place of Lemma 12, this implies

$$\left\|\left\{X_A^{\sigma_1},Z_A^{\sigma_1}\right\}|\Psi\rangle\right\|\leqslant 3n\sqrt{2\varepsilon_0}+\left(\frac{13(n-1)}{2}+17\right)\sqrt{2\varepsilon_1}+2(n-1)\sqrt{2\varepsilon_2}. \tag{A23}$$

That $\sigma_1=i$ yields the result of Eq. (74).

To obtain Eq. (75) we use Proposition 17 to write

$$\begin{aligned}\left\|\left\{X_{B,i}^{i},Z_{B,j}^{i}\right\}|\Psi\rangle\right\|&\leqslant 4\sqrt{2\varepsilon_1}+\left\|\left\{X_A^{i},Z_A^{i}\right\}|\Psi\rangle\right\|\\&\leqslant 3n\sqrt{2\varepsilon_0}+\left(\frac{13(n-1)}{2}+21\right)\sqrt{2\varepsilon_1}+2(n-1)\sqrt{2\varepsilon_2},\end{aligned} \tag{A24}$$

where the final equality follows from Eq. (74) just proved. ■

[1] J. S. Bell, On the Einstein Podolsky Rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).

[2] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, J. Phys. A **44**, 095305 (2011).

[3] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[4] M. McKague, Interactive proofs for BQP via self-tested graph states, Theor. Comput. **12**, 1 (2016).

[5] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, Device-independent verifiable blind quantum computation, arXiv:1502.02563.

[6] A. Gheorghiu, E. Kashefi, and P. Wallden, Robustness and device independence of verifiable blind quantum computing, New J. Phys. **17**, 083040 (2015).

[7] A. Gheorghiu, P. Wallden, and E. Kashefi, Rigidity of quantum steering and one-sided device-independent verifiable quantum computation, New J. Phys. **19**, 023043 (2017).

[8] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, Phys. Rev. A **96**, 012303 (2017).

[9] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches, Theor. Comput. Syst. **63**, 715 (2019).

[10] S. A. Adamson and P. Wallden, Quantum magic rectangles: Characterization and application to certified randomness expansion, Phys. Rev. Res. **2**, 043317 (2020).

[11] We refer to a measurement performed on an observer's system of qubits as *local* (as opposed to *entangled*) or *single-qubit* if it can be realized from measurements made on individual qubits independently.

[12] It is precisely these extra checks that allow us to self-test three Bell states using a nonlocal game that is normally used to self-test two Bell states (the magic square game). This is extended later for the n Bell state case with a game whose optimal winning probability could be saturated with a quantum strategy involving just a pair of Bell states.

[13] A. Coladangelo, Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game, Quantum Inf. Comput. **17**, 831 (2017).

[14] P. K. Aravind, Quantum mysteries revisited again, Am. J. Phys. **72**, 1303 (2004).

[15] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Device-independent parallel self-testing of two singlets, Phys. Rev. A **93**, 062121 (2016).

[16] N. D. Mermin, Simple Unified form for the Major No-Hidden-Variables Theorems, Phys. Rev. Lett. **65**, 3373 (1990).

[17] A. Peres, Incompatible results of quantum measurements, Phys. Lett. A **151**, 107 (1990).

[18] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (IEEE, Piscataway, NJ, 1998), pp. 503–509.

[19] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[20] M. McKague, Self-testing in parallel, New J. Phys. **18**, 045013 (2016).

[21] M. Coudron and A. Natarajan, The parallel-repeated magic square game is rigid, arXiv:1609.06306.

[22] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick, Test for a large amount of entanglement, using few measurements, Quantum **2**, 92 (2018).

[23] A. Natarajan and T. Vidick, A quantum linearity test for robustly verifying entanglement, in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017 (ACM Press, New York, 2017), pp. 1003–1015.

[24] A. Natarajan and T. Vidick, Low-degree testing for quantum states, and a quantum entangled games PCP for QMA, in *Proceedings of the 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, NJ, 2018), pp. 731–742.

[25] A. Natarajan and J. Wright, NEEXP is contained in MIP*, in *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, NJ, 2019), pp. 510–518.

[26] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, MIP* = RE, Commun. ACM **64**, 131 (2021).

[27] I. Šupić, D. Cavalcanti, and J. Bowles, Device-independent certification of tensor products of quantum states using single-copy self-testing protocols, Quantum **5**, 418 (2021).

[28] H. Fu, Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension, Quantum **6**, 614 (2022).

[29] L. Mančinska, J. Prakash, and C. Schafhauser, Constant-sized robust self-tests for states and measurements of unbounded dimension, arXiv:2103.01729.

[30] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, Self-testing quantum systems of arbitrary local dimension with minimal number of measurements, npj Quantum Inf. **7**, 151 (2021).

[31] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, Quantum **4**, 337 (2020).

[32] G. Brassard, A. Broadbent, and A. Tapp, Quantum pseudo-telepathy, Found. Phys. **35**, 1877 (2005).

[33] While maximally entangled qudit states and generalized qudit Pauli measurement projectors are isomorphic to tensor products of $|\Phi^+\rangle$ and *qubit* Pauli measurement projectors, respectively (as shown in a lemma of [26]), it is not clear that all of the measurements used in the qudit honest strategy of [24] can be mapped under such an isomorphism to local measurements with respect to each two-dimensional register (in general they may become entangled measurements).

[34] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[35] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[36] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Robust and Versatile Black-Box Certification of Quantum Devices, Phys. Rev. Lett. **113**, 040401 (2014).

[37] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from non-local correlations, Phys. Rev. A **91**, 022115 (2015).

[38] E. Kashefi and P. Wallden, Garbled quantum computation, Cryptography **1**, 6 (2017).

[39] E. Kashefi and A. Pappa, Multiparty delegated quantum computing, Cryptography **1**, 12 (2017).