Parallel Self-Testing of EPR Pairs Under Computational Assumptions

Honghao Fu
CSAIL, Massachusetts Institute of Technology, Cambridge, MA, USA

Daochen Wang
QuICS, University of Maryland, College Park, MD, USA

Qi Zhao
QuICS, University of Maryland, College Park, MD, USA
QICI, The University of Hong Kong, China

Abstract

Self-testing is a fundamental feature of quantum mechanics that allows a classical verifier to force untrusted quantum devices to prepare certain states and perform certain measurements on them. The standard approach assumes at least two spatially separated devices. Recently, Metger and Vidick [39] showed that a single EPR pair of a single quantum device can be self-tested under *computational assumptions*. In this work, we generalize their results to give the first parallel self-test of N EPR pairs and measurements on them in the single-device setting under the same computational assumptions. We show that our protocol can be passed with probability negligibly close to 1 by an honest quantum device using poly(N) resources. Moreover, we show that any quantum device that fails our protocol with probability at most ϵ must be poly(N, ϵ)-close to being honest in the appropriate sense. In particular, our protocol can test any distribution over tensor products of computational or Hadamard basis measurements, making it suitable for applications such as device-independent quantum key distribution [38] under computational assumptions. Moreover, a simplified version of our protocol is the first that can efficiently certify an arbitrary number of qubits of a single cloud quantum computer using only classical communication.

2012 ACM Subject Classification Theory of computation → Interactive proof systems

Keywords and phrases Quantum complexity theory, self-testing, LWE

Digital Object Identifier 10.4230/LIPIcs.ICALP.2023.64

Category Track A: Algorithms, Complexity and Games

Related Version *Full Version*: https://arxiv.org/abs/2201.13430 [21]

Funding *Honghao Fu*: NSF QLCI program (grant OMA-2016245).
Daochen Wang: Army Research Office (grant W911NF-20-1-0015); the Department of Energy, Office of Science, Office of Advanced Scientific Computing Research, Accelerated Research in Quantum Computing program; and the National Science Foundation (grant DMR-1747426).
Qi Zhao: Department of Defense through the QuICS Hartree Postdoctoral Fellowship.

Acknowledgements We especially thank Carl Miller, Tony Metger, and Thomas Vidick for many helpful discussions and correspondence. We also thank Nai-Hui Chia, Shih-Han Hung, Yi Lee, Atul Mantri, and Jiayu Zhang for helpful discussions.

1 Introduction

Self-testing is a fundamental feature of quantum mechanics that allows a classical verifier to force a quantum device (sometimes called prover) to prepare certain states and measure them in certain bases up to local isometries [4, 47, 50, 43, 7, 35, 48, 18, 25, 8, 36, 37, 41, 42, 13, 20, 46, 45, 19, 28]. In the standard *nonlocal setting*, the key assumption is that there are two

50th International Colloquium on Automata, Languages, and Programming (ICALP 2023).
Editors: Kousha Etessami, Uriel Feige, and Gabriele Puppis; Article No. 64; pp. 64:1–64:19
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

or more spatially separated devices. However, it is difficult to certify spatial separation in practice, especially if the devices fall outside our physical control. Therefore, it is interesting to ask whether we can replace this assumption by another one so that we can self-test a *single* quantum device. We illustrate the nonlocal and single-device settings in Fig. 1.

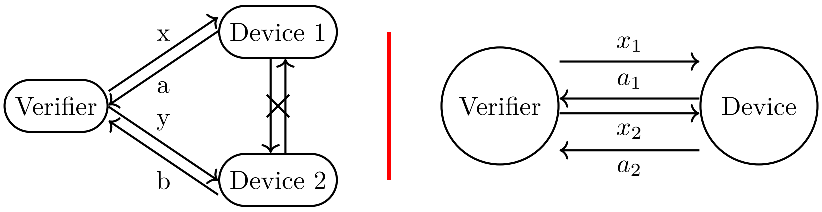


Figure 1 Self-testing in the nonlocal setting (left) involves (at least) two spatially separated devices that cannot communicate. In the single-device setting (right), there is only one device.

Computational self-testing. Recently, beginning with seminal work by Mahadev [33] on the classical verification of quantum computations, a series of works, e.g., [24, 6, 14, 1, 52, 53, 29, 5, 27, 32, 55, 39, 38, 40], have explored how computational assumptions can be leveraged by a classical verifier to control a single quantum device in certain ways. Typically, the assumption used is that the Learning-With-Errors (LWE) [44] problem is hard to solve efficiently, even for quantum computers, which is a standard assumption. However, except for [24, 53, 39, 38, 40], the level of control established in these works is much weaker than in nonlocal self-testing. For example, if a device passes Mahadev's verification protocol [33], it only means that, to quote [39], "*there exists* a quantum state such that the distribution over the prover's answers *could have been* produced by performing the requested measurements on this state". We do not know whether the prover *actually* prepared that state and performed the requested measurements on it.

Metger and Vidick [39] are the first to explicitly propose the self-testing of a single device under computational assumptions. The main limitation of [39] and follow-up work [40] is that they only self-test two and three qubits, respectively. In this work, we introduce a self-test that certifies the preparation and measurement of N EPR pairs in the computational (or single-device) setting. Our work differs from the concurrent work [23] in that [23] certifies the preparation (but not measurement) of BB84 states.

Main results. We give a self-test that certifies the EPR pairs:

$$\left\{ |\tau^{\diamond,v}\rangle := \frac{1}{\sqrt{2^N}} \bigotimes_{i=1}^{N} (\sigma^X)^{v_i} \otimes (\sigma^X)^{v_{N+i}} (|0\rangle_i |+\rangle_{N+i} + |1\rangle_i |-\rangle_{N+i}) \;\middle|\; v \in \{0,1\}^{2N} \right\},$$

and states $\{|\tau^{\theta,v}\rangle \mid \theta \in \{0, 1 \ldots, 2N\}, v \in \{0,1\}^{2N}\}$, which is a subset of BB84 states specified in Section 3.

Moreover, our self-test certifies any distribution over tensor products of computational (Pauli-Z) or Hadamard (Pauli-X) basis measurements on $2N$ qubits:

$$\left\{ \{\Pi_q^u := |B_{q_1}^{u_1}\rangle\langle B_{q_1}^{u_1}| \otimes \ldots \otimes |B_{q_{2N}}^{u_{2N}}\rangle\langle B_{q_{2N}}^{u_{2N}}| \mid u \in \{0,1\}^{2N}\} \;\middle|\; q \in \{0,1\}^{2N} \right\}, \tag{1}$$

where $|B_0^0\rangle := |0\rangle, |B_0^1\rangle := |1\rangle, |B_1^0\rangle := |+\rangle$, and $|B_1^1\rangle := |-\rangle$.

Our self-test generalizes protocols in [24, 39] and uses the Extended Noisy Trapdoor Claw-Free function Families (ENTCFs) introduced by Mahadev in [33]. An ENTCF consists of two function-pair families, a claw-free family $\mathcal{F}$ and an injective family $\mathcal{G}$, that have certain cryptographic properties under the LWE hardness assumption.

In our self-test, the classical verifier first samples $\theta \in \{0,1,\dots,2N\} \cup \{\diamond\}$ uniformly at random. Then it generates the public keys and trapdoors of $2N$ function pairs from $\mathcal{F} \cup \mathcal{G}$ according to θ as follows.

1. $\theta = 0$: all pairs are from $\mathcal{G}$.
2. $\theta \in \{1,\dots,2N\}$: the θ^{th} pair is from $\mathcal{F}$ and the remaining $2N-1$ pairs are from $\mathcal{G}$.
3. $\theta = \diamond$: all pairs are from $\mathcal{F}$.

The verifier sends the public keys to the device. The device then sends back $2N$ images, $y_1,\dots,y_{2N}$, of these function pairs – these play the role of a commitment. In the second round, the verifier either (i) checks the commitment by asking for preimages of the y_is and accepts or rejects accordingly, or (ii) asks for an equation involving the preimages of the y_is. In case (ii), there is a final round where the verifier sends with probability $1/2$ a uniformly random $q \in \{0^{2N}, 1^{2N}, 0^N1^N, 1^N0^N\}$ and with probability $1/2$ a random $q \in \{0,1\}^{2N}$ according to some distribution μ of its choosing. The device sends back the result $u \in \{0,1\}^{2N}$ of performing some measurement $\{P_q^u\}_u$. The verifier lastly checks that u is consistent with measuring $|\tau^{\theta,v}\rangle$ using $\{\Pi_q^u\}_u$, where $v \in \{0,1\}^{2N}$ is some bitstring that the verifier can compute efficiently using the trapdoors, and accepts or rejects accordingly. We allow our verifier to pick any distribution μ on $q \in \{0,1\}^{2N}$ so that our protocol can be composed with other protocols. For example, in our applications, the distribution on $q \in \{0,1\}^{2N}$ is non-uniform.

▶ **Theorem 1** (Informal). *Let $\lambda \in \mathbb{N}$ be a security parameter and let $N = \mathrm{poly}(\lambda)$ be a fixed polynomially-bounded function of λ. Assuming the LWE problem of size λ cannot be solved in $\mathrm{poly}(\lambda)$ time, our self-test satisfies the following properties.*

Completeness. *Using $\mathrm{poly}(\lambda)$ qubits and quantum gates, a quantum device can prepare one of the $2N$-qubit states in $\{|\tau^{\theta,v}\rangle \mid \theta \in \{0,1,\dots,2N\} \cup \{\diamond\}, v \in \{0,1\}^{2N}\}$ and measure it using $\{\Pi_q^u \mid u \in \{0,1\}^{2N}\}$ upon question $q \in \{0,1\}^{2N}$ to pass our self-test with probability $\geq 1 - \mathrm{negl}(\lambda)$. Moreover, the verifier can be classical and run in $\mathrm{poly}(\lambda)$ time.*

Soundness. *If a quantum device passes our self-test in $\mathrm{poly}(\lambda)$ time with probability $\geq 1-\epsilon$, then the device must have prepared a (sub-normalized) state $\sigma^{\theta,v}$, measured it using $\{P_q^u\}_u$, and received outcome u, such that*

$$\sum_{v\in\{0,1\}^{2N}} \|V\sigma^{\theta,v}V^\dagger - |\tau^{\theta,v}\rangle\langle\tau^{\theta,v}| \otimes \alpha^{\theta,v}\|_1 \leq O(N^{7/4}\epsilon^{1/32}) \quad \textit{and} \tag{2}$$

$$\mathbb{E}_{q\leftarrow\mu}\Big[\sum_{u,v\in\{0,1\}^{2N}} \|VP_q^u\,\sigma^{\theta,v}\,P_q^uV^\dagger - \Pi_q^u\,|\tau^{\theta,v}\rangle\langle\tau^{\theta,v}|\,\Pi_q^u \otimes \alpha^{\theta,v}\|_1\Big] \leq O(N^2\epsilon^{1/32}), \tag{3}$$

where $\theta \in \{0,1,\dots,2N\} \cup \{\diamond\}$, μ is the distribution on $\{0,1\}^{2N}$ chosen by the verifier in our self-test, $u,v \in \{0,1\}^{2N}$ are known to the verifier, V is an efficient isometry independent of $\{\theta,\mu,u,v\}$, and the $\alpha^{\theta,v}$s are some auxiliary states that are computationally indistinguishable from some fixed state α.

Note that $\theta = \diamond$ corresponds to self-testing EPR pairs. We also highlight the $\mathrm{poly}(N,\epsilon)$ soundness error (or robustness) that we achieve. Good robustness is critical if we want to use our self-test in practice because real quantum devices are imperfect. The more imperfect a device is, the more robust a self-test needs to be to control it.

Techniques. The main challenge is to prove soundness. We give a high-level overview here and provide more details in Section 4. We start by defining $4N$ observables of the device $\{X_i, Z_i \mid i \in [2N]\}$ using its measurement operators. The strategy is to characterize these observables as the standard σ_i^X and σ_i^Z Pauli observables on $2N$ qubits where i indexes those qubits. Then, we characterize the device's states by their invariance under products of projectors corresponding to these observables and the device's measurements as products of these projectors. To characterize X_i and Z_j, we first generalize techniques in [39] to show that X_i and Z_j obey certain state-dependent commutation and anti-commutation relations (Proposition 10). To carry out the generalization, it is important for the verifier to select θ from the set $[2N] \cup \{0, \diamond\}$ for two reasons. The first is that they allow us to bound the failure probability associated with *each* σ^θ by $2N+2$ (the number of possible θs) times the *average* failure probability over all θs. The second is that this restricted set of θs suffices for us to characterize X_i and Z_i as σ_i^X and σ_i^Z. Intuitively, $\theta = 0$ is used to characterize $\{Z_1, \ldots, Z_{2N}\}$, $\theta \in [2N]$ is used to characterize X_θ, and $\theta = \diamond$ is used to characterize EPR pairs. We give a more precise correspondence in Table 1.

Then, we introduce new techniques to handle products of projectors corresponding to the X_i, Z_i observables. These techniques differ significantly from [39] because their techniques are not susceptible to generalization to arbitrary N (as we discuss after Proposition 15). These techniques also differ significantly from those used in nonlocal self-testing because we lack the perfect state-*independent* commutation relations between observables on two spatially-separated devices. More specifically, we introduce a "operator-state commutation" relation (Proposition 11) that, together with the computational indistinguishability of the σ^θs (which follows from the LWE hardness assumption), gives us the ability to "commute an observable past a state". We then use this ability to handle products of projectors. The usefulness of the ability to commute can be seen in the following simple example. Observe that $X_1 Z_2 X_3 \psi = Z_2 X_1 X_3 \psi$ (1) does not follow from the commutation relation $X_1 Z_2 \psi = Z_2 X_1 \psi$, where ψ is some density operator. However, (1) would follow if we could commute X_3 past ψ first because X_1 and Z_2 would then be directly next to ψ. Having all (1)-like relations involving products of up to N X_i and Z_i implies that these observables can be characterized as σ_i^X and σ_i^Z respectively, which follows from results in approximate representation theory [51, 26]. We remark that the preceding discussion is for intuition only: in fact, our proof directly shows that an explicit "swap" isometry (defined in Definition 12) approximately maps X_i and Z_i to σ_i^X and σ_i^Z respectively.

Applications. We present two applications of our result, the first is for device-independent (DI) quantum key distribution (QKD), and the second is for dimension testing. We stress that for both applications, we crucially rely on the characterization of *measurements* in Equation (3) of Theorem 1.

DIQKD. A DI protocol is one where the parties involved do not need to trust the inner working of the devices they use to be sure that the devices have successfully implemented the protocol. A QKD protocol is one for establishing information-theoretically secure keys between two parties. Previous DIQKD protocols rely on the nonlocal assumption. This assumption is usually justified experimentally by spatially separating two devices by a large distance, which is difficult to implement. Recently, Metger et. al. [38] proposed a different setting for DIQKD: they replace the nonlocal assumption with the assumption that the two devices are computationally bounded. However, since their protocol sequentially repeats the self-test in [39], their soundness proof relies on the IID assumption that the device behaves identically and independently at each repetition to argue that it has prepared and measured many EPR pairs.

Our DIQKD protocol consists of a random number of "test rounds" followed by a final "generation round", where both round types are based on our self-test. The N EPR pairs certified in the generation round are used to generate $\Omega(N)$ shared keys. Because of the parallel nature of our self-test, our DIQKD protocol does not require the IID assumption. We sketch a soundness proof that uses a "cut-and-choose" argument from [23, Theorem 4.33] to upper bound the failure probability of the device in the generation round, conditioned on the protocol not aborting in the test rounds. This argument does not require an IID assumption *between* rounds. Then, we use Equation (3) of Theorem 1 to lower bound the key rate, which does not require an IID assumption *within* any round. Hence we remove the IID assumption overall. The application of our self-test to remove the IID assumption from DIQKD in the computational setting can be viewed as analogous to the application of the nonlocal self-test to remove the IID assumption from DIQKD in the usual nonlocal setting [45].

Dimension testing. Our dimension-test is a simplified version of our self-test and is inspired by the non-local dimension test in [11] and its exposition in [51, Section 2.5.2]. The protocol in [11] works as follows. The verifier chooses a random bit $\theta \in \{0, 1\}$ and random bitstring $x \in \{0, 1\}^n$ and sends n qubits to the device such that the qubits encode x in the computational basis ($\theta = 0$) or in the Hadamard basis ($\theta = 1$). After the device has received all n qubits, the verifier sends θ to the device and asks it to return a bitstring $x' \in \{0, 1\}^n$. If $x' = x$, the verifier certifies that the device has a large quantum dimension. Our protocol can be viewed as a version of this protocol, where the verifier classically delegates the preparation of the appropriate n-qubit states to the prover in a secure manner. Although our protocol is inspired by [11], our security proof uses Theorem 1 and differs significantly from that in [11].

We prove that, under the same computational assumptions as in Theorem 1, if a quantum device runs in poly(λ) time and passes our dimension-test with probability $\geq 1 - \epsilon$, then its quantum dimension is at least $(1 - O(N^2\epsilon^{1/32}))2^N$ $(*)$. To obtain a non-trivial bound, it suffices to estimate ϵ to precision 1/poly(N), which can be done by repeating the dimension-test poly(N) times. Since a single run of the dimension test also only takes poly(N) time, the total time taken is poly(N). Intuitively, we prove $(*)$ by using Equation (3) of Theorem 1 to argue that the Hilbert space $\mathcal{H}$ of the device must be able to accommodate all possible post-measurement states that could result from performing a Hadamard basis measurement of N qubits in a computational basis state. Since there are 2^N such post-measurement states, and they are all orthogonal, we deduce a quantum dimension lower bound of 2^N. A formal proof is more challenging because Equation (3) of Theorem 1 gives an approximation and we need to prove that the rank of a quantum state is robust against the approximation error.

Compared to nonlocal dimension-tests [9, 10, 17], the advantage of ours is that we do not need to assume spatial separation between multiple devices. Compared to prepare-and-measure dimension-tests [22, 12, 13, 11], the advantage of ours is that the verifier does not need to be quantum – all computations and communications are classical. To the best of our knowledge, our dimension-test is the first[1] that can test for an arbitrary quantum dimension in the computational setting. In fact, whether this is possible was recently raised as an open question by Vidick in [51, pg. 84].

Discussion. One interesting direction is to further improve the efficiency and robustness of our protocol. When $N = \lambda$, one bottleneck in improving the efficiency is that sending (the public key of) one function pair already requires poly(λ) = poly(N) bits of communication. In recent work, it has been shown that, instead of sending the public keys, the verifier can apply a *succinct batch key generation algorithm* to reduce the cost of sending public keys [3]. We expect that techniques in [3] can be used to shorten other messages of our protocol as

[1] More recently, [34] also claims a dimension test using completely different methods.

well. Turning to robustness, we note that there exists a nonlocal self-test [41] which uses $\mathrm{poly}(N)$ bits of communication and achieves robustness $\mathrm{poly}(\epsilon)$. It might be possible to combine our techniques with those in [41] to achieve similar robustness in the computational setting. Another interesting question to ask is what MIP^* protocols can be compiled into computation delegation protocols under computational assumptions. For comparison, it has been shown that classical MIP protocols sound against non-signalling provers can be turned into computation delegation protocols [49, 31]. It would also be interesting to see if a systematic way exists to translate nonlocal self-tests into computational ones. We note that [29] suggests that the two settings might not be too different at a conceptual level by presenting a test of quantumness in the computational setting that closely resembles the nonlocal CHSH test [16]. Recently, Kalai et. al. proposed a way to construct a proof-of-quantumness protocol from any nonlocal game with a classical and quantum separation using quantum homomorphic encryption [30]. However, it is unknown if the aforementioned protocols are quantumly sound. Going beyond quantum dimension testing, it would be interesting to see if our protocol can be combined with those that test quantum circuit depth [15, 2] to give a protocol that tests the quantum volume of a quantum computer.

2 Preliminaries

Notation. $\mathbb{N}$ is the set of positive integers. For $k \in \mathbb{N}$, we write $[k] := \{1, 2, \ldots, k\}$. For a probability distribution μ on X, we use the notation $x \leftarrow_\mu X$ to mean that x is sampled from X according to μ. $\mathcal{H}$ denotes a finite-dimensional Hilbert space, $\mathcal{L}(\mathcal{H})$ denotes the set of linear operators on $\mathcal{H}$, and $\mathrm{Pos}(\mathcal{H})$ denotes the set of positive semi-definite operators on $\mathcal{H}$. We sometimes refer to operators in $\mathrm{Pos}(\mathcal{H})$ or vectors in $\mathcal{H}$, not necessarily normalized, as (quantum) states. For an operator $X \in \mathcal{L}(\mathcal{H})$, we write $\|X\|_p := \mathrm{Tr}[|X|^p]^{1/p}$, where $|X| := \sqrt{X^\dagger X}$, for the Schatten p-norm. For $\phi, \psi \in \mathcal{L}(\mathcal{H})$, we write $\phi \approx_\epsilon \psi$ to mean $\|\phi - \psi\|_1^2 \leq O(\epsilon)$. For $A, B \in \mathcal{L}(\mathcal{H})$ and $\psi \in \mathrm{Pos}(\mathcal{H})$, we write $\|A\|_\psi^2 := \mathrm{Tr}[A^\dagger A \psi] = \|A\sqrt{\psi}\|_2^2$ and $A \approx_{\epsilon,\psi} B \iff \|A - B\|_\psi^2 \leq O(\epsilon)$. The single-qubit Z and X Pauli operators are denoted $\sigma_Z := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\sigma_X := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ which have eigenstates $\{|0\rangle := \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), |1\rangle := \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)\}$ and $\{|(-)^0\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |(-)^1\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, respectively.

We write $\lambda \in \mathbb{N}$ for the security parameter. Most quantities in this work are dependent on λ. Therefore, for convenience, we often make the dependence implicit. A function $f : \mathbb{N} \to \mathbb{R}$ is said to be negligible if for any polynomial $p \in \mathbb{R}[x]$, $\lim_{\lambda \to \infty} f(\lambda)p(\lambda) = 0$. We denote such functions by $\mathrm{negl}(\lambda)$.

ENTCFs. We informally summarize the properties that we employ of Extended Noisy Trapdoor Claw-free function Families (ENTCFs). For full details about the properties of ENTCFs, see the arXiv version of [33].

Let $\lambda \in \mathbb{N}$ be a security parameter. Let $\mathcal{X} \subseteq \{0,1\}^w$ and $\mathcal{Y}$ be finite sets that depend on λ, where $w = w(\lambda)$ is some integer that is a polynomially-bounded function of λ. An ENTCF consists of two families of function pairs, $\mathcal{F}$ and $\mathcal{G}$. Function pairs from these two families are labeled by public keys. The set of public keys for $\mathcal{F}$ is denoted by $\mathcal{K}_\mathcal{F}$, and the set of public keys for $\mathcal{G}$ is denoted by $\mathcal{K}_\mathcal{G}$. For $k \in \mathcal{K}_\mathcal{F}$, a function pair $(f_{k,0}, f_{k,1})$ from $\mathcal{F}$ is called a *claw-free* pair. For $k \in \mathcal{K}_\mathcal{G}$, a function pair $(f_{k,0}, f_{k,1})$ from $\mathcal{G}$ is called an *injective* pair. For any $k \in \mathcal{K}_\mathcal{F} \cup \mathcal{K}_\mathcal{G}$, the functions[2] $f_{k,0}, f_{k,1} \colon \mathcal{X} \to \mathcal{Y}$. Note that the keys and function pairs of an ENTCF are functions of λ. We use the terms "efficient" and "negligible" to refer to $\mathrm{poly}(\lambda)$-time and $\mathrm{negl}(\lambda)$ respectively. We need the following properties of ENTCFs:

[2] This is a convenient simplification. These functions actually map to probability distributions on $\mathcal{Y}$. See Section 2.2 of the full version for details.

1. *Efficient function generation property* [33, Definitions 4.1 (1), 4.2 (1)]. There exist efficient classical probabilistic algorithms $\mathrm{Gen}_{\mathcal{F}}$ and $\mathrm{Gen}_{\mathcal{G}}$ for $\mathcal{F}$ and $\mathcal{G}$ respectively with $\mathrm{Gen}_{\mathcal{F}}(1^\lambda) \to (k \in \mathcal{K}_{\mathcal{F}}, t_k)$ and $\mathrm{Gen}_{\mathcal{G}}(1^\lambda) \to (k \in \mathcal{K}_{\mathcal{G}}, t_k)$, where t_k is known as a trapdoor.
2. *(Disjoint) injective pair property* [33, Definitions 4.1 (2), 4.2 (2)]. For all $k \in \mathcal{K}_{\mathcal{F}} \cup \mathcal{K}_{\mathcal{G}}$, $x, x' \in \mathcal{X}$ with $x \neq x'$, and $b \in \{0,1\}$, $f_{k,b}(x) \neq f_{k,b}(x')$. For all $k \in \mathcal{K}_{\mathcal{F}}$ and $x \in \mathcal{X}$, there exists an $x' \neq x$ such that $f_{k,0}(x) = f_{k,1}(x')$. We call any such pair of (x, x') a *claw.*
3. *Efficient range superposition property* [33, Definitions 4.1 (3.c), 4.2 (3.b), 4.3 (1)]. Given $k \in \mathcal{K}_{\mathcal{F}} \cup \mathcal{K}_{\mathcal{G}}$, there exists an efficient quantum algorithm that prepares a state that is negligibly close to $|\psi\rangle := \frac{1}{\sqrt{2\cdot|\mathcal{X}|}} \sum_{b\in\{0,1\}} \sum_{x\in\mathcal{X}} |b\rangle\,|x\rangle\,|f_{k,b}(x)\rangle$, in trace distance.
4. *Efficient decoding property* [33, Definitions 4.1 (2, 3.a, 3.b), 4.2 (2, 3.a), 4.3 (1)]. We define the following "decoding maps" that decode the output of functions from an ENTCF. For $k \in (\mathcal{K}_{\mathcal{F}} \cup \mathcal{K}_{\mathcal{G}})^m$ with $m = \mathrm{poly}(\lambda)$, $k_{\mathcal{G}} \in \mathcal{K}_{\mathcal{G}}$, $k_0 \in \mathcal{K}_{\mathcal{F}} \cup \mathcal{K}_{\mathcal{G}}$, and $k_{\mathcal{F}} \in \mathcal{K}_{\mathcal{F}}$

$$\mathrm{CHK}(k, y, b, x) = 0 \text{ if } y_i = f_{k_i,b_i}(x_i) \text{ for all } i \in [m],\ \text{else } = 1$$

$$\hat{b}(k_{\mathcal{G}}, y) = b \text{ if } y \in \mathrm{Im}(f_{k_{\mathcal{G}},b}),\ \text{else } =\perp$$

$$\hat{x}(b, k_0, y) := x \text{ if } f_{k_0,b}(x) = y,\ \text{else } =\perp$$

$$\hat{h}(k_{\mathcal{F}}, y, d) := d \cdot (\hat{x}(0, k_{\mathcal{F}}, y) \oplus \hat{x}(1, k_{\mathcal{F}}, y)) \text{ if } y \in \mathrm{Im}(f_{k_{\mathcal{F}},0}) \text{ and } d \neq 0^w, \text{else } =\perp .$$

   The efficient decoding property states that $\hat{b}$, $\hat{x}$, and $\hat{h}$ can be computed efficiently given a trapdoor t_k for k by a classical deterministic algorithm and that CHK can be computed efficiently even without a trapdoor by a classical deterministic algorithm.
5. *Adaptive hardcore bit property* [33, Definition 4.1 (4)]. There does not exist an efficient quantum algorithm that, given $k \leftarrow \mathrm{Gen}_{\mathcal{F}}(1^\lambda)_{\mathrm{key}}$, can compute $b \in \{0,1\}$ and $x_b \in \mathcal{X}$ for some $b \in \{0,1\}$, $d \in \{0,1\}^w \backslash \{0^w\}$, and, with non-negligible advantage, a bit $d \cdot (x_0 \oplus x_1) \in \{0,1\}$ such that (x_0, x_1) is a claw.
6. *Injective invariance property* [33, Definition 4.3 (2)]. There does not exist an efficient quantum algorithm that can distinguish between the marginal key distributions of $\mathrm{Gen}_{\mathcal{F}}(1^\lambda)$ and of $\mathrm{Gen}_{\mathcal{G}}(1^\lambda)$ with non-negligible advantage.

3 Completeness of self-testing protocol

In this section, we present our self-testing protocol in Fig. 2. We sketch a proof of its completeness (Theorem 2), partly to establish some notation. For details, see Section 3 of the full version.

▶ **Theorem 2.** *There exists an efficient quantum device that is accepted by our self-testing protocol with probability $\geq 1 - \mathrm{negl}(\lambda)$. Moreover, the classical verifier is efficient.*

Proof sketch. In the first round, for each $i \in [2N]$, by the efficient range superposition property of ENTCFs (Item 3), the device uses k_i to efficiently prepare a state that is negligibly close to

$$|\psi_i\rangle := \frac{1}{\sqrt{2\cdot|\mathcal{X}|}} \sum_{b\in\{0,1\}} \sum_{x\in\mathcal{X}} |b\rangle\,|x\rangle\,|f_{k_i,b}(x)\rangle .$$

Then, the device measures the (image) y register of $|\psi_i\rangle$ and sends the outcome to the verifier. By the (disjoint) injective pair property of ENTCFs (Item 2), after the y measurement, the state $|\psi_i\rangle$ collapses to $|\phi_i\rangle\,|y_i\rangle$, where

$$|\phi_i\rangle := \begin{cases} |\hat{b}(k_i, y_i)\rangle\,|\hat{x}(k_i, y_i)\rangle & \text{if } k_i \in \mathcal{K}_{\mathcal{G}}, \\ \frac{1}{\sqrt{2}}(|0\rangle\,|\hat{x}_0(k_i, y_i)\rangle + |1\rangle\,|\hat{x}_1(k_i, y_i)\rangle) & \text{if } k_i \in \mathcal{K}_{\mathcal{F}}. \end{cases}$$

1. Input: $\lambda \in \mathbb{N}$. Set $N = \text{poly}(\lambda)$. Given a distribution μ on $\{0,1\}^{2N}$. Sample $\theta \leftarrow_U [2N] \cup \{0, \diamond\}$ uniformly at random. Sample $2N$ key-trapdoor pairs $(k_1, t_{k_1}), \ldots, (k_{2N}, t_{k_{2N}})$ from an ENTCF according to θ as follows:

   $\theta \in [2N]$: the θ-th key-trapdoor pair is sampled from $\text{Gen}_{\mathcal{F}}(1^\lambda)$ and the remaining $2N-1$ pairs are all sampled from $\text{Gen}_{\mathcal{G}}(1^\lambda)$.

   $\theta = 0$: all the key-trapdoor pairs are sampled from $\text{Gen}_{\mathcal{G}}(1^\lambda)$.

   $\theta = \diamond$: all the key-trapdoor pairs are sampled from $\text{Gen}_{\mathcal{F}}(1^\lambda)$.

   Send the keys $k = (k_1, \ldots, k_{2N})$ to the device.

2. Receive $y = (y_1, \ldots, y_{2N}) \in \mathcal{Y}^{2N}$ from the device.

3. Sample round type “preimage” or “Hadamard” uniformly at random and send to the device.

Case “preimage”: receive

$$(b, x) = (b_1, \ldots, b_{2N}, x_1, \ldots, x_{2N})$$

from the device, where $b \in \{0,1\}^{2N}$ and $x \in \{0,1\}^{2Nw}$.
If $\text{CHK}(k_i, y_i, b_i, x_i) = 0$ for all $i \in [2N]$, **accept**, else **reject**.

Case “Hadamard”: receive

$$d = (d_1, \ldots, d_{2N}) \in \{0,1\}^{2Nw}$$

from the device.

4. With probability $1/2$, sample $q \leftarrow_U \{0^{2N}, 1^{2N}, 0^N 1^N, 1^N 0^N\}$ uniformly at random, and with probability $1/2$ sample $q \leftarrow_\mu \{0,1\}^{2N}$ according to the distribution μ. Send q to the device.

   Receive $u \in \{0,1\}^{2N}$ from the device.

case A $\theta = 0$ and
    if $q_i = 0$ and $\hat{b}(k_i, y_i) \neq u_i$ for some $i \in [2N]$, **reject**,
    else **accept**.

case B $\theta \in [2N]$ and
    if $q_i = 0$ and $\hat{b}(k_i, y_i) \neq u_i$ for some $i \neq \theta$, **reject**,
    if $q_\theta = 1$ and $\hat{h}(k_\theta, y_\theta, d_\theta) \oplus \hat{b}(k_{\theta+N}, y_{\theta+N}) \neq u_\theta$, **reject**,
    else **accept**.

case C $\theta = \diamond$ and
    if $q_i = 0$, $q_{N+i} = 1$ and $u_i \oplus u_{N+i} \neq \hat{h}(k_{N+i}, y_{N+i}, d_{N+i})$ for some $i \in [N]$, **reject**,
    if $q_i = 1$, $q_{N+i} = 0$ and $u_i \oplus u_{N+i} \neq \hat{h}(k_i, y_i, d_i)$ for some $i \in [N]$, **reject**,
    else **accept**.

Figure 2 A protocol that self-tests EPRs of a computationally efficient device.

In the following, we use the shorthand $\hat{b}_i := \hat{b}(k_i, y_i) \in \{0,1\}$ and, for $a \in \{0,1\}$, $\hat{x}_{a,i} := \hat{x}(a, k_i, y_i) \in \mathcal{X}$.

In the second round, there are two cases, “preimage” or “Hadamard”. In the “preimage” case, the device measures the b and x registers of each $|\phi_i\rangle$ in the computational basis and sends the outcome to the device. This will always be accepted by the device using the definition of CHK.

In the “Hadamard” case, the device measures the x register of each $|\phi_i\rangle$ in the Hadamard basis and sends the outcome $d = (d_1, d_2, \ldots, d_{2N})$ to the verifier. After this measurement, $|\phi_i\rangle$ collapses to $|\alpha_i\rangle |d_i\rangle$, where, if $\theta \in [2N]$, then

$$|\alpha_i\rangle = \begin{cases} |\hat{b}_i\rangle & \text{if } i \neq \theta, \\ (|0\rangle + (-1)^{d_\theta \cdot (\hat{x}_{0,\theta} \oplus \hat{x}_{1,\theta})} |1\rangle)/\sqrt{2} & \text{if } i = \theta; \end{cases}$$

if $\theta = 0$, then $|\alpha_i\rangle = |\hat{b}_i\rangle$; and if $\theta = \diamond$, then $|\alpha_i\rangle = (|0\rangle + (-1)^{d_i \cdot (\hat{x}_{0,i} \oplus \hat{x}_{1,i})} |1\rangle)/\sqrt{2}$.

In the following, we use the shorthand $\hat{h}_i := d_i \cdot (\hat{x}_{0,i} \oplus \hat{x}_{1,i}) \in \{0,1\}$ and $\hat{h}' := (\hat{h}_{N+1}, \ldots, \hat{h}_{2N}, \hat{h}_1, \hat{h}_2, \ldots, \hat{h}_N) \in \{0,1\}^{2N}$.

For $v \in \{0,1\}^{2N}$, we also define the state

$$|\psi^v\rangle := \frac{1}{\sqrt{2^N}} \bigotimes_{i=1}^{N} (\sigma^X)^{v_i} \otimes (\sigma^X)^{v_{N+i}} (|0\rangle_i |+\rangle_{N+i} + |1\rangle_i |-\rangle_{N+i}), \tag{4}$$

which consists of N (locally-rotated) EPR pairs.

Then, the device applies N controlled-σ^Z gates between the i-th and $(N+i)$-th qubits of $\bigotimes_{i=1}^{2N} |\alpha_i\rangle$ for all $i \in [N]$ (note that the controlled-σ^Z gate is independent of which qubit is the control and which qubit is the target). The device has now prepared the $2N$-qubit state

$$|\alpha\rangle := \begin{cases} |\hat{b}_1, \ldots, \hat{b}_{\theta-1}\rangle |(-)^{\hat{b}_{\theta+N} \oplus \hat{h}_\theta}\rangle |\hat{b}_{\theta+1}, \ldots, \hat{b}_{2N}\rangle & \text{if } \theta \in [2N],\ \theta \leq N, \\ |\hat{b}_1, \ldots, \hat{b}_{\theta-1}\rangle |(-)^{\hat{b}_{\theta-N} \oplus \hat{h}_\theta}\rangle |\hat{b}_{\theta+1}, \ldots, \hat{b}_{2N}\rangle & \text{if } \theta \in [2N],\ \theta > N, \\ |\hat{b}_1, \ldots, \hat{b}_{2N}\rangle & \text{if } \theta = 0, \\ |\psi^{\hat{h}'}\rangle & \text{if } \theta = \diamond. \end{cases} \tag{5}$$

In the "Hadamard" case, there is a third and final round where the verifier sends a bitstring $q \in \{0,1\}^{2N}$ to the device. The device performs the following q-dependent measurements. For $i \in [2N]$, if $q_i = 0$, measure the ith qubit of $|\alpha\rangle$ in the computational basis, otherwise, measure the ith qubit of $|\alpha\rangle$ in the Hadamard basis. The device finally sends the outcome $u \in \{0,1\}^{2N}$ of these measurements to the verifier. The right-hand side of Equation (5) implies that the device passes the last checks made by the verifier.

The "moreover" part of the theorem follows directly from the efficient function generation and the efficient decoding properties of ENTCFs (Items 1 and 4). ◀

4 Soundness of self-testing protocol

In this section, we show that our self-testing protocol achieves $\mathrm{poly}(N, \epsilon)$ soundness error. Unlike the proof of completeness in Section 3, we use the adaptive hardcore bit and injective invariance properties of ENTCFs to prove soundness in this section. Therefore, it is necessary for us to make the LWE hardness assumption throughout this section. All proofs can be found in Section 4 of the full version.

We start with a mathematical model of quantum devices.

▶ **Definition 3.** *A device $D = (S, M, \Pi, P)$ is specified by Hilbert spaces named $\mathcal{H}_D$, $\mathcal{H}_Y$, and $\mathcal{H}_R$, with $\dim(\mathcal{H}_Y) = |\mathcal{Y}|^{2N}$ and $\dim(\mathcal{H}_R) = 2^{2Nw}$, and the following.*

1. *A set $S := \{\psi^\theta \mid \theta \in [2N] \cup \{0, \diamond\}\} \subset \mathcal{D}(\mathcal{H}_D \otimes \mathcal{H}_Y)$ of states where each state ψ^θ is classical on $\mathcal{H}_Y$:*

$$\psi^\theta := \sum_{y \in \mathcal{Y}^{2N}} \psi^\theta_y \otimes |y\rangle\langle y|.$$

The state ψ^θ_y models the device's state immediately after returning $y \in \mathcal{Y}^{2N}$ to the verifier if the verifier initially sampled $\theta \in [2N] \cup \{0, \diamond\}$. More precisely, ψ^θ_y (and hence ψ^θ) is a function of the public keys $k \in (\mathcal{K}_\mathcal{F} \cup \mathcal{K}_\mathcal{G})^{2N}$ that the verifier sampled according to θ, as described in the protocol. We choose to make the k-dependence implicit for notational convenience.

2. *A projective measurement Π for the preimage test on $\mathcal{H}_D \otimes \mathcal{H}_Y$:*

$$\Pi := \left\{ \Pi^{b,x} := \sum_{y \in \mathcal{Y}^{2N}} \Pi^{b,x}_y \otimes |y\rangle\langle y| \;\middle|\; b \in \{0,1\}^{2N}, x \in \mathcal{X}^{2N} \right\}.$$

The measurement outcome b, x is the device's answer for the preimage test.

3. *A projective measurement M on $\mathcal{H}_D \otimes \mathcal{H}_Y$ for the device's first answer in the Hadamard test:*

$$M := \left\{ M^d := \sum_{y \in \mathcal{Y}^{2N}} M_y^d \otimes |y\rangle\langle y| \;\middle|\; d \in \{0,1\}^{2Nw} \right\}. \tag{6}$$

We write $\sigma^\theta(D)$ for the classical-quantum state that results from measuring M on ψ^θ followed by writing measurement outcome d into another classical register whose Hilbert space is denoted by $\mathcal{H}_R$. That is,

$$\sigma^\theta(D) := \sum_{y \in \mathcal{Y}^{2N},\, d \in \{0,1\}^{2Nw}} \sigma^\theta_{y,d}(D) \otimes |y,d\rangle\langle y,d| \in \mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R, \tag{7}$$

where $\sigma^\theta_{y,d}(D) := M_y^d \psi_y^\theta M_y^d$.

4. *Projective measurements P_q on $\mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R$ for the device's second answer in the Hadamard test when asked questions $q \in \{0,1\}^{2N}$:*

$$P_q := \left\{ P_q^u = \sum_{y \in \mathcal{Y}^{2N}, d \in \{0,1\}^{2Nw}} P^u_{q,y,d} \otimes |y,d\rangle\langle y,d| \;\middle|\; u \in \{0,1\}^{2N} \right\}. \tag{8}$$

The measurement outcome v is the device's answer for the question q.

▶ **Definition 4.** *A device $D = (S, \Pi, M, P)$ is efficient if all the states in S can be efficiently prepared and all the measurements $\Pi, M,$ and P are efficient.*

We use P to define observables of the quantum device that we call X_i and Z_i, which should act as Pauli X and Z operators on the ith qubit respectively.

▶ **Definition 5** (Marginal observables)**.** *Let $D = (S, \Pi, M, P)$ be a device. For $i \in [2N]$ and $q \in \{0,1\}^{2N}$, we define the binary observables*

$$Z_{q,i}(D) := \sum_{v \in \{0,1\}^{2N}} (-1)^{v_i} P_q^v \quad \text{if } q_i = 0 \quad \text{and} \quad X_{q,i}(D) := \sum_{v \in \{0,1\}^{2N}} (-1)^{v_i} P_q^v \quad \text{if } q_i = 1.$$

Note that $Z_{q,j}(D)$ commutes with $X_{q,k}(D)$ for $j \neq k$ according to these definitions.

In the rest of the paper, we use the abbreviations $Z_i(D) := Z_{0^{2N},i}(D)$ and $X_i(D) := X_{1^{2N},i}(D)$ for all $i \in [2N]$; $\widetilde{Z}_i(D) := Z_{0^N 1^N,i}(D)$ if $i \leq N$; $\widetilde{Z}_i(D) := Z_{0^N 1^N,i}(D)$ if $i > N$; $\widetilde{X}_i(D) := X_{1^N 0^N,i}(D)$ if $i \leq N$; and $\widetilde{X}_i(D) := X_{0^N 1^N,i}(D)$ if $i > N$.

For different choices of θ, our goal is to characterize the actions of the observables X_i and Z_i on the state σ^θ, which is the post-M-measurement state defined below.

▶ **Definition 6** ($\sigma^{\theta,v}$)**.** *Let D be a device. For $\theta \in [2N] \cup \{0, \diamond\}$ and $v \in \{0,1\}^{2N}$, we define the state*

$$\sigma^{\theta,v}(D) := \sum_{(y,d) \in \Sigma(\theta,v)} \sigma^\theta_{y,d}(D) \otimes |y,d\rangle \langle y,d| \in \mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R, \tag{9}$$

where, $\Sigma(\theta, v)$ is set to

$$\begin{cases} \left\{(y,d) \;\middle|\; \hat{b}(k_i, y_i) = v_i \text{ for all } i \neq \theta \text{ and } \hat{h}(k_\theta, y_\theta, d_\theta) = v_\theta \oplus v_{\mathrm{mod}(\theta+N,2N)}\right\} & \text{if } \theta \in [2N], \\ \left\{(y,d) \;\middle|\; \hat{b}(k_i, y_i) = v_i \text{ for all } i\right\} & \text{if } \theta = 0, \\ \left\{(y,d) \;\middle|\; \hat{h}(k_i, y_i, d_i) = v_{\mathrm{mod}(i+N,2N)} \text{ for all } i\right\} & \text{if } \theta = \diamond. \end{cases}$$

In all cases, (y,d) ranges over $\mathcal{Y}^{2N} \times \{0,1\}^{2Nw}$, i ranges over $[2N]$, and the state $\sigma^{\theta,v}(D)$ implicitly depends on keys $k \in (\mathcal{K}_\mathcal{F} \cup \mathcal{K}_\mathcal{G})^{2N}$ chosen according to θ as described in the protocol.

Unlike the nonlocal self-testing case, where there is only one state, e.g. EPR pairs, to characterize, we have multiple states and multiple observables to characterize. Hence, we first decompose $\sigma^\theta \approx \sum_{v\in\{0,1\}^{2N}} \sigma^{\theta,v}$, where $\sigma^{\theta,v}$ are defined above. We then characterize the behavior of different observables on different $\sigma^{\theta,v}$ using the failure probabilities of different test cases:

▶ **Definition 7** (Failure probabilities). *Let D be a device. For $q \in \{0,1\}^{2N}$, we define $\epsilon_P(D)$ to be the probability that D fails the preimage test, $\epsilon_{H,q}(D)$ to be the probability that D fails question q of the Hadamard test, and $\epsilon_H(D)$ to be the maximum of $\epsilon_{H,q}(D)$ over $q \in \{0^{2N}, 1^{2N}, 0^N1^N, 1^N0^N\}$. Then, the average failure probability is*

$$\epsilon(D) := \epsilon_P(D)/2 + \Big(\sum_{q\in\{0^{2N},1^{2N},0^N1^N,1^N0^N\}} \frac{1}{4}\epsilon_{H,q}(D) + \sum_{q\in\{0,1\}^{2N}} \mu(q)\epsilon_{H,q}(D)\Big)/4.$$

Henceforth, when D is clear from the context, we mostly omit the D dependence.

The probability that this device can pass the tests of our protocol allows us to say that the operator acts in the same way as the ideal operator acts on the ideal state. Therefore, we will use ϵ_P and $\epsilon_{H,q}$ to bound how far away the $Z_{q,i}, X_{q,i}$ observables and $\sigma^{\theta,v}$ states are from the ideal observables and states. How we characterize the states and observables using the passing probabilities of the four key questions: $q = 0^2N$, 1^{2N}, 0^N1^N and 1^N0^N is summarized in Table 1. Note that $q \in \{0^N1^N, 1^N0^N\}$ are for testing EPR pairs.

Table 1 Correspondence between the (θ, q) used in our protocol and the observables tested.

(q_i, q_{i+N}) with $i \le N$	$\theta = 0$	$\theta \in [2N]$	$\theta = \diamond$
$(0,0)$	$Z_{q,i}$ and $Z_{q,i+N}$	-	-
$(1,1)$	-	$X_{q,\theta}$ if $\theta \in \{i, i+N\}$	-
$(0,1)$	-	-	$Z_{q,i} \cdot X_{q,i+N}$
$(1,0)$	-	-	$X_{q,i} \cdot Z_{q,i+N}$

Our use of only $2N+2$ distinct θs allows us to bound the failure probability associated with each σ^θ by $O(N\epsilon)$. If we had naively used $\theta \in \{0,1\}^{2N}$, the robustness of our self-test would be $2^{\Omega(N)}\epsilon$. The fact that using only $2N+2$ distinct θs is *sufficient* for self-testing crucially relies on the following proposition, which can be proven using the injective invariance property of ENTCFs (Item 6).

▶ **Proposition 8.** *Any pair of states in $\{\sigma^\theta \mid \theta \in [2N] \cup \{0, \diamond\}\}$ of an efficient device D are computationally indistinguishable.*

In the next step, we use the computational indistinguishability of the σ^θs to argue that for all (q,i), the observables $Z_{q,i}$ and $X_{q,i}$ act like Z_i and X_i on any σ^θ.

▶ **Proposition 9.** *For all $q \in \{0,1\}^{2N}$, $\theta \in [2N] \cup \{0, \diamond\}$, and $i \in [2N]$, we have*

$$Z_{q,i} \approx_{N(\epsilon_{H,q}+\epsilon_H+\epsilon_P),\sigma^\theta} Z_i \text{ if } q_i = 0, \quad \text{and} \quad X_{q,i} \approx_{N(\epsilon_{H,q}+\epsilon_H+\epsilon_P),\sigma^\theta} X_i \text{ if } q_i = 1.$$

For self-testing, we not only need to characterize the action of a single operator on σ^θ as sketched above, we also need to characterize the actions of products of the operators. Next, we establish the commutation and anti-commutation relations of the observables with respect to σ^θ. Proving commutation is straightforward, while proving anti-commutation relies on the adaptive hardcore bit property. Our proof generalizes and refines techniques in [39, 24]: one difference is that we associate error parameters to each $\sigma^{\theta,v}$, where $v \in \{0,1\}^{2N}$, and use them collectively to bound the overall approximation error associated with σ^θ.

▶ **Proposition 10.** *Let D be an efficient perfect device. For all $i, j, \theta \in [2N]$, we have*

Commutation. $[Z_i, Z_j] = 0,\ [X_i, X_j] = 0,$ *and* $[Z_i, X_j] \approx_{N\epsilon_H + \mathrm{negl}(\lambda), \sigma^\theta} 0$ *if* $i \neq j$.

Anti-commutation. $\{Z_i, X_i\} \approx_{\sqrt{N\epsilon_H} + \mathrm{negl}(\lambda), \sigma^\theta} 0.$

The above relations allow us to handle products of two operators from $\{Z_i, X_i\}_{i\in[2N]}$. However, as mentioned in Section 1, we also want to show relations such as $Z_1X_3Z_2\sigma^3 \approx X_3Z_1Z_2\sigma^3$ ($\star$), which does *not* directly follow because Z_1 and X_3 are not directly next to the state σ^3. We want to establish relations like ($\star$) involving products of multiple observables Z_i and X_i in order to characterize Z_i and X_i as Pauli operators σ_i^Z and σ_i^X under the swap isometry defined later.

Our solution to this problem is the next proposition which shows observable-state commutation relations for certain pairs of observables and states. For example, we can now easily prove ($\star$) by first using the proposition to commute Z_2 past σ^3. We view our use of observable-state commutation relations, which has no analog in prior work, as one of the main technical contributions of this work. These techniques should be useful in any future work that aims to efficiently self-test more than one qubit.

▶ **Proposition 11** (Operator-state commutation). *Let D be an efficient perfect device. For all $i, \theta \in [2N]$ with $i \neq \theta$ and $q \in \{0,1\}^{2N}$, we have*

$$Z_{q,i}\,\sigma^\theta \approx_{N(\epsilon_H+\epsilon_{H,q})+\mathrm{negl}(\lambda)} \sigma^\theta\, Z_{q,i} \text{ if } q_i = 0 \text{ and } X_{q,\theta}\,\sigma^\theta \approx_{N(\epsilon_H+\epsilon_{H,q})+\mathrm{negl}(\lambda)} \sigma^\theta\, X_{q,\theta} \text{ if } q_\theta = 1.$$

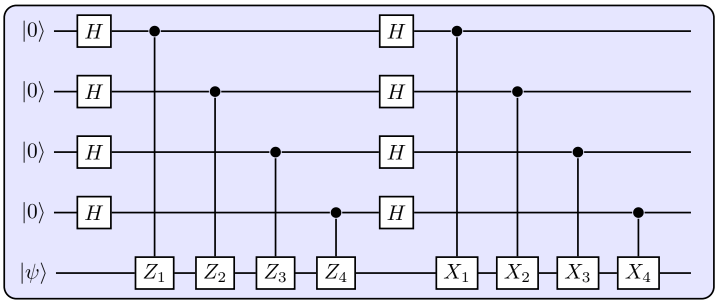
Observe that the proposition above does *not* say $Z_{q,i}$ and $X_{q,i}$ commute with σ^θ for all pairs (i, θ) as we would have desired to prove all ($\star$)-like relations. To get around this problem, we make use of the computational indistinguishability of the σ^θs to argue that efficient observables must act similarly on different σ^θs. For example, consider the following relation that looks similar to ($\star$): $Z_1X_3Z_2\sigma^2 \approx X_3Z_1Z_2\sigma^2$ ($\star'$). In this case, we cannot directly apply Proposition 11, since Z_2 does not commute with σ^2. Nevertheless, by using the computational indistinguishability of σ^2 and σ^3, we can derive an "operational version" of ($\star'$) from ($\star$). The operational version allows us to interchange the left-hand and right-hand sides of ($\star'$) when they appear inside traces (i.e., Tr). We can only derive such an operational version because the computational indistinguishability of σ^2 and σ^3 only allows us to interchange σ^2 and σ^3 inside traces; see the lifting lemmas in the full version. For an example of our using this technique, see the long aligned equation in the proof of Lemma 4.33 in the full version.

Next, we define our swap isometry $\mathcal{V}$. We will show that $\mathcal{V}$ maps the states, observables, and measurements of the device to their ideal counterparts. This swap isometry can be viewed as a special case of the swap isometry proposed in [54, Figure 2] in the nonlocal setting. It is not the obvious generalization of the swap isometry used in [39, Proof of Lemma 4.28] as that is more difficult to analyze.

▶ **Definition 12.** *Let D be a device and let $\mathcal{H} := \mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R$. The swap isometry is the map $\mathcal{V} : \mathcal{H} \to \mathbb{C}^{2^{2N}} \otimes \mathcal{H}$ defined by*

$$\mathcal{V} = \sum_{u\in\{0,1\}^{2N}} |u\rangle \otimes \prod_{i\in[2N]} X_i^{u_i} \prod_{j\in[2N]} Z_j^{(u_j)}.$$

We illustrate $\mathcal{V}$ when $2N = 4$ below.



We proceed to analyze the effect of the swap isometry on the observables and states of the device. More specifically, in Proposition 13, we show that $\mathcal{V}$ maps the X_i and Z_i observables approximately to σ^X and σ^Z operators acting on the ith qubit of an auxiliary system.

▶ **Proposition 13.** *Let D be an efficient perfect device. For all $k \in [2N]$, $\theta \in [2N] \cup \{0, \diamond\}$, and $q \in \{0,1\}^{2N}$, we have*

$$\mathcal{V}^\dagger(\sigma_k^Z \otimes \mathbb{1})\mathcal{V} \approx_{N(\epsilon_H+\epsilon_{H,q})+\mathrm{negl}(\lambda),\sigma^\theta} Z_{q,k} \text{ if } q_k = 0, \text{ and}$$
$$\mathcal{V}^\dagger(\sigma_k^X \otimes \mathbb{1})\mathcal{V} \approx_{N^{3/2}\sqrt{\epsilon_H}+N\epsilon_{H,q},\sigma^\theta} X_{q,k} \text{ if } q_k = 1.$$

Moreover, for $k \in [N]$ and $\theta \in [2N] \cup \{0, \diamond\}$,

$$\mathcal{V}^\dagger(\sigma_k^X \otimes \sigma_{N+k}^Z \otimes \mathbb{1})\mathcal{V} \approx_{N^{3/8}\epsilon_H^{1/8},\sigma^\theta} \widetilde{X}_k\widetilde{Z}_{N+k} \quad \text{and} \quad \mathcal{V}^\dagger(\sigma_k^Z \otimes \sigma_{N+k}^X \otimes \mathbb{1})\mathcal{V} \approx_{N^{3/8}\epsilon_H^{1/8},\sigma^\theta} \widetilde{Z}_k\widetilde{X}_{N+k}.$$

In Proposition 15, we show that $\mathcal{V}$ maps the states of the device to states of the form $\tau^{\theta,v} \otimes \alpha^{\theta,v}$, where $\tau^{\theta,v}$ is the ideal state defined below and $\alpha^{\theta,v}$ is some junk state that is computationally indistinguishable to a fixed state α for all θ and v.

▶ **Definition 14** (density operators $\tau^{\theta,v}$). *Let $v \in \{0,1\}^{2N}$. For $\theta \in [2N] \cup \{0, \diamond\}$, we define the $2N$-qubit density operator $\tau^{\theta,v} := |\tau^{\theta,v}\rangle\langle\tau^{\theta,v}|$, according to the following three cases.*

$$|\tau^{\theta,v}\rangle := \begin{cases} |v_1\rangle \otimes \cdots \otimes |v_{\theta-1}\rangle \otimes |(-)^{v_\theta}\rangle \otimes |v_{\theta+1}\rangle \otimes \cdots \otimes |v_{2N}\rangle & \text{if } \theta \in [2N], \\ |v\rangle := |v_1\rangle \otimes \cdots \otimes |v_{2N}\rangle & \text{if } \theta = 0, \\ |\psi^v\rangle & \text{if } \theta = \diamond, \end{cases} \tag{10}$$

where $|\psi^v\rangle$ is as defined in Equation (4).

▶ **Proposition 15.** *Let D be an efficient perfect device. For all $\theta \in [2N] \cup \{0, \diamond\}$ and $v \in \{0,1\}^{2N}$, there exists a state $\alpha^{\theta,v} \in \mathrm{Pos}(\mathcal{H})$ such that*

$$\sum_{v\in\{0,1\}^{2N}} \|\mathcal{V}\sigma^{\theta,v}\mathcal{V}^\dagger - \tau^{\theta,v} \otimes \alpha^{\theta,v}\|_1 \le O(N^{7/4}\epsilon_H^{1/4}), \text{ for } \theta \neq \diamond, \text{ and}$$
$$\sum_{v\in\{0,1\}^{2N}} \|\mathcal{V}\sigma^{\diamond,v}\mathcal{V}^\dagger - \tau^{\diamond,v} \otimes \alpha^{\diamond,v}\|_1 \le O(N^{35/32}\epsilon_H^{1/32}).$$

Moreover, there exists a state $\alpha \in \mathrm{Pos}(\mathcal{H})$ and numbers $\{\delta(v) \geq 0 \mid v \in \{0,1\}^{2N}\}$ such that any efficient device can distinguish between $\alpha^{\theta,v}$ and $\alpha/2^{2N}$ with advantage at most $O(\delta(v))$ for all $v \in \{0,1\}^{2N}$, with $\sum_{v\in\{0,1\}^{2N}} \delta(v) \le O(N^{49/32}\epsilon_H^{1/32})$.

The proofs of the two propositions above rely heavily on Propositions 10 and 11 which crucially allows us to bound the soundness error in Theorem 16 by $O(\mathrm{poly}(N,\epsilon))$. If we directly generalize the soundness analysis of [39], we would obtain an $O(2^N\epsilon^{1/2^N})$ bound on the soundness error which is extremely loose.[3]

[3] [23, End of Section 1.3] explains why the technique in [39] would lead to such a loose bound.

Lastly, we put everything together to give our main soundness result, Theorem 16. The main task is to characterize the measurement operator P_q^u, which is approximately a product of $2N$ binary projectors of the form $Z_{q,i}^{(u_i)}$ and $X_{q,i}^{(u_i)}$. We use the operator-state commutation relation to sequentially replace each projector in the product by its ideal counterpart.

▶ **Theorem 16.** *Let D be an efficient device. Let $\mathcal{H} := \mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R$ be the Hilbert space of D. Let $\mathcal{V} : \mathcal{H} \to \mathbb{C}^{2^{2N}} \otimes \mathcal{H}$ be the swap isometry defined in Definition 12. For $\theta \in [2N] \cup \{0, \diamond\}$ and $v \in \{0,1\}^{2N}$, let $\sigma^{\theta,v} \in \mathrm{Pos}(\mathcal{H})$ be the states that D prepares after returning the first answer in the Hadamard round, as defined in Definition 6. Let $\{\{P_q^u\}_{u\in\{0,1\}^{2N}} \mid q \in \{0,1\}^{2N}\}$ be the measurements defined in Equation (8) of Definition 3.*

Suppose that D fails the protocol in Fig. 2 (with an input distribution μ on $\{0,1\}^{2N}$ and $N = \mathrm{poly}(\lambda)$) with probability at most ϵ. Then, there exist states $\{\alpha^{\theta,v} \mid \theta \in [2N] \cup \{0, \diamond\}, v \in \{0,1\}^{2N}\}$, that are computationally indistinguishable from a single state $\alpha \in \mathrm{Pos}(\mathcal{H})$ in the way specified in Proposition 15, such that

$$\sum_{v\in\{0,1\}^{2N}} \|\mathcal{V}\sigma^{\theta,v}\mathcal{V}^\dagger - \tau^{\theta,v} \otimes \alpha^{\theta,v}\|_1 \le O(N^{7/4}\epsilon^{1/32}),$$

$$\mathop{\mathbb{E}}_{q\leftarrow\mu}\left[\sum_{u,v\in\{0,1\}^{2N}} \|\mathcal{V}P_q^u\sigma^{\theta,v}P_q^u\mathcal{V}^\dagger - \langle B_q^u| \tau^{\theta,v} |B_q^u\rangle \, |B_q^u\rangle\langle B_q^u| \otimes \alpha^{\theta,v}\|_1\right] \le O(N^2\epsilon^{1/32}),$$

and, for all $q \in \{0^{2N}, 1^{2N}, 0^N1^N, 1^N0^N\}$,

$$\sum_{u,v\in\{0,1\}^{2N}} \|\mathcal{V}P_q^u\sigma^{\theta,v}P_q^u\mathcal{V}^\dagger - \langle B_q^u| \tau^{\theta,v} |B_q^u\rangle \, |B_q^u\rangle\langle B_q^u| \otimes \alpha^{\theta,v}\|_1 \le O(N^2\epsilon^{1/32}).$$

5 Applications

In this section, we briefly describe two applications of our self-test: DIQKD and dimension-testing. For details, see Section 5 of the full version.

DIQKD. We describe how to adapt the protocol for DIQKD under computational assumptions in [38] to use our self-testing protocol as its main component. The resulting DIQKD protocol operates under the same setting and assumptions as in [38] except we remove the IID assumption. In particular, we highlight the fact that we retain the advantage of the generated key being information-theoretically secure.

Recall that in our self-testing protocol, there is a single verifier interacting with a single device. On the other hand, in DIQKD, there are two verifiers, Alice and Bob, that each interact with their own (untrusted) device. In DIQKD *under computational assumptions*, the two devices are not assumed to be non-communicating and are modeled as a single device with two *components*, one on Alice's side, and one on Bob's. At a high level, to resolve the difference in the number of verifiers, we will let Alice play the role of the single verifier in our self-testing protocol while Bob will play a relaying role.

In Fig. 3, we describe a single test round of our DIQKD protocol. In Fig. 4, we describe how to modify the test round to give a single generation round of our DIQKD protocol. We construct our overall DIQKD protocol by using multiple test rounds followed by a single generation round. After the generation round, Alice and Bob proceed to key extraction, which is essentially the same as that in [38, Protocol 3].

1. Alice samples $\theta \leftarrow_U [2N] \cup \{0, \diamond\}$ uniformly at randomly, generates $2N$ key-trapdoor pairs (k_1, t_1), …, (k_{2N}, t_{2N}) according to θ, and sends $k_{N+1}, \ldots, k_{2N}$ to Bob. Note that Alice has all the trapdoors $\{t_i\}_{i=1}^{2N}$. Then Alice sends $k_1, \ldots, k_N$ to her component. Bob sends $k_{N+1}, \ldots, k_{2N}$ to his component.
2. Alice receives back $(y_1, \ldots, y_N) \in \mathcal{Y}^N$ and Bob receives back images $(y_{N+1}, \ldots, y_{2N}) \in \mathcal{Y}^N$.
3. Alice samples $c \leftarrow_U \{\text{preimage}, \text{Hadamard}\}$ uniformly at random, sends it to Bob, and they both send c to their components.

   Case c = preimage. Alice receives $(b_1, \ldots b_N, x_1, \ldots, x_N) \in \{0,1\}^{N+Nw}$ from her component and Bob receives $(b_{N+1}, \ldots, b_{2N}, x_{N+1}, \ldots, x_{2N}) \in \{0,1\}^{N+Nw}$ from his component and sends it to Alice. Alice verifies $(b_1, \ldots, b_{2N}, x_1, \ldots, x_{2N})$ according to our self-testing protocol.

   Case c = Hadamard.

   a. Alice receives $(d_1, \ldots, d_N) \in \{0,1\}^{Nw}$ from her component and Bob receives $(d_{N+1}, \ldots, d_{2N}) \in \{0,1\}^{Nw}$ from his component.

   b. Alice samples $a \leftarrow_U \{0,1\}$ uniformly at random.
      - If $a = 0$, Alice samples $q \leftarrow_U \{0^{2N}, 1^{2N}, 0^N 1^N, 1^N 0^N\}$ uniformly at random.
      - If $a = 1$, Alice sets $q = 1^N 0^N$.

      Note that the resulting distribution on $(q_1, \ldots, q_{2N}) \in \{0,1\}^{2N}$ is the same as in Step 4 of our self-testing protocol (Fig. 2) with μ chosen as the distribution that always outputs $1^N 0^N$.

      Alice sends q_{N+1} to Bob. Alice sends $q_1, \ldots, q_N$ to her component. Bob sends $q_{N+1}, \ldots, q_{N+1}$ $(= q_{N+1}, \ldots, q_{2N})$ to his component.

   c. Alice receives $(u_1, \ldots, u_N) \in \{0,1\}^N$ from her component and Bob receives $(u_{N+1}, \ldots, u_{2N}) \in \{0,1\}^N$ from his component. Alice sends "Test" to Bob. Bob sends $\{(y_i, d_i, u_i)\}_{i=N+1}^{2N}$ to Alice. Alice verifies $\{(y_i, d_i, u_i)\}_{i=1}^{2N}$ according to our self-testing protocol using the trapdoors that she holds, $(t_1, \ldots, t_{2N})$.

Figure 3 Test round for device-independent quantum key distribution (DIQKD) protocol.

Same as the test round (see Fig. 3) except with the following modifications.

- At Step 1, Alice chooses $\theta = \diamond$.
- At the start of Step 3, Alice chooses c = Hadamard.
- At the start of Step 3(b), instead of sampling q, Alice sets $q = 1^N 0^N$.
- Replace Step 3 (c) by the following. Alice receives $(u_1, \ldots, u_N) \in \{0,1\}^N$ from her component and Bob receives $(u_{N+1}, \ldots, u_{2N}) \in \{0,1\}^N$ from his component. Alice sends "Generation" to Bob.

Figure 4 Generation round for device-independent quantum key distribution (DIQKD) protocol.

The completeness of this DIQKD protocol essentially follows from the completeness of our self-testing protocol. The soundness follows from the soundness of our self-testing protocol combined with the key rate analysis used to prove [38, Theorem 1] and the "cut-and-choose" argument used to prove [23, Theorem 4.33].

Dimension-testing. We simplify our self-testing protocol to give a protocol that tests if a quantum device can store N qubits. The simplifications are: 1. θ is sampled from $\{0, 1, \ldots, N\}$, 2. in the Hadamard case, there are only two questions $q = 0^N$ and $q = 1^N$. Details of this protocol can be found in Section 5.2 of the full version. The honest prover's behavior is similar to that of our self-test.

The intuition behind the soundness of this protocol is that, when it is passed with high probability, Theorem 16 guarantees the existence of a quantum state $\rho^\star$ on the quantum part of the device's memory that is close to the maximally mixed state up to some isometry. More specifically, $\rho^\star$ comes from using Theorem 16 to force the device to perform a Hadamard basis measurement on N qubits that are in the computational basis and discarding the measurement results. Then, the main proposition of this section, Proposition 17, shows that the guarantee on $\rho^\star$ is strong enough for us to lower bound the rank of $\rho^\star$, which is also a lower bound on the quantum dimension of the device's memory.

▶ **Proposition 17.** *Let $\rho, \alpha \in D(\mathcal{H})$ be density operators. If there exists a unitary $U \in \mathcal{L}(\mathbb{C}^{2^n} \otimes \mathcal{H})$ such that $\|U(|0\rangle\langle 0|^{\otimes n} \otimes \rho)U^\dagger - 2^{-n}\mathbb{1} \otimes \alpha\|_1 \le \epsilon$, then $\mathrm{Rank}(\rho) \ge (1-\epsilon)2^n$.*

We now use Proposition 17 to prove the main theorem of this section. Much of the proof is devoted to bookkeeping to ensure that the (normalized) density operator condition in Proposition 17 is satisfied and that we are bounding the *quantum* dimension.

▶ **Theorem 18.** *Let D be an efficient device with Hilbert space $\mathcal{H} = \mathcal{H}_D \otimes \mathcal{H}_Y \otimes \mathcal{H}_R$. Let the classical-quantum decomposition of $\mathcal{H}$ be $\mathcal{H}_C \otimes \mathcal{H}_Q$, so that all states and observables of D on $\mathcal{H}$ are classical on $\mathcal{H}_C$, i.e., block-diagonal in a fixed basis $\{|c\rangle \mid c \in [\dim(\mathcal{H}_C)]\}$ of $\mathcal{H}_C$. If D can pass the dimension test protocol with probability $\ge 1-\epsilon$, then the quantum dimension of D, $\dim(H_Q)$, is at least $(1 - O(N^2\epsilon^{1/32}))2^N$.*

References

1 Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung. Non-interactive Classical Verification of Quantum Computation. In *Theory of Cryptography*, pages 153–180. Springer International Publishing, 2020. doi:10.1007/978-3-030-64381-2_6.

2 Atul Singh Arora, Andrea Coladangelo, Matthew Coudron, Alexandru Gheorghiu, Uttam Singh, and Hendrik Waldner. Quantum depth in the Random Oracle Model, 2022. arXiv:2210.06454

3 James Bartusek, Yael Tauman Kalai, Alex Lombardi, Fermi Ma, Giulio Malavolta, Vinod Vaikuntanathan, Thomas Vidick, and Lisa Yang. Succinct Classical Verification of Quantum Computation, 2022. arXiv:2206.14929

4 J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

5 Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device. *Journal of the ACM*, 68(5), 2021. doi:10.1145/3441309.

6 Zvika Brakerski, Venkata Koppula, Umesh V. Vazirani, and Thomas Vidick. Simpler Proofs of Quantumness. In *Proceedings of the 15th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC)*, 2020. doi:10.4230/LIPIcs.TQC.2020.8.

7 Samuel L. Braunstein, A. Mann, and M. Revzen. Maximal violation of Bell inequalities for mixed states. *Physical Review Letters*, 68:3259–3261, 1992. doi:10.1103/PhysRevLett.68.3259.

8 Spencer Breiner, Amir Kalev, and Carl A. Miller. Parallel Self-Testing of the GHZ State with a Proof by Diagrams. *Electronic Proceedings in Theoretical Computer Science*, 287:43–66, 2019. doi:10.4204/eptcs.287.3.

9 Nicolas Brunner, Stefano Pironio, Antonio Acin, Nicolas Gisin, André Allan Méthot, and Valerio Scarani. Testing the Dimension of Hilbert spaces. *Physical Review Letters*, 100(21):210503, 2008. doi:10.1103/PhysRevLett.100.210503.

10 Yu Cai, Jean-Daniel Bancal, Jacquiline Romero, and Valerio Scarani. A new device-independent dimension witness and its experimental implementation. *Journal of Physics A: Mathematical and Theoretical*, 49(30):305301, 2016. doi:10.1088/1751-8113/49/30/305301.

11 Rui Chao and Ben W. Reichardt. Quantum dimension test using the uncertainty principle, 2020. arXiv:2002.12432

12 Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping Qubits. In *Proceedings of the 8th Innovations in Theoretical Computer Science Conference (ITCS)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 48:1–48:21, 2017. doi:10.4230/LIPIcs.ITCS.2017.48.

13 Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *Quantum*, 2:92, 2018. doi:10.22331/q-2018-09-03-92.

14 Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. Classical Verification of Quantum Computations with Efficient Verifier. In *Theory of Cryptography*, pages 181–206. Springer International Publishing, 2020. `doi:10.1007/978-3-030-64381-2_7`.

15 Nai-Hui Chia and Shih-Han Hung. Classical verification of quantum depth, 2022. `arXiv:2205.04656`

16 John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969. `doi:10.1103/PhysRevLett.23.880`.

17 Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. *Quantum*, 4:282, 2020. `doi:10.22331/q-2020-06-18-282`.

18 Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8(1):15485, 2017. `doi:10.1038/ncomms15485`.

19 Andrea Coladangelo, Alex B. Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-Leash: New Schemes for Verifiable Delegated Quantum Computation, with Quasilinear Resources. In *Advances in Cryptology – EUROCRYPT 2019*, pages 247–277, 2019. `doi:10.1007/978-3-030-17659-4_9`.

20 Honghao Fu. Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension. *Quantum*, 6:614, 2022. `doi:10.22331/q-2022-01-03-614`.

21 Honghao Fu, Daochen Wang, and Qi Zhao. Parallel self-testing of EPR pairs under computational assumptions. *arXiv preprint arXiv:2201.13430*, 2022.

22 Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. Device-independent tests of classical and quantum dimensions. *Physical Review Letters*, 105(23):230501, 2010. `doi:10.1103/PhysRevLett.105.230501`.

23 Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more, 2022. `arXiv:2201.13445`

24 Alexandru Gheorghiu and Thomas Vidick. Computationally-Secure and Composable Remote State Preparation. In *Proceedings of the 60th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 1024–1033, 2019. `doi:10.1109/FOCS.2019.00066`.

25 Koon Tong Goh, Jedrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Physical Review A*, 97:022104, 2018. `doi:10.1103/PhysRevA.97.022104`.

26 W T Gowers and O Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784–1817, 2017. `doi:10.1070/sm8872`.

27 Shuichi Hirahara and François Le Gall. Test of Quantumness with Small-Depth Quantum Circuits. In *Proceedings of the 46th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, pages 59:1–59:15, 2021. `doi:10.4230/LIPIcs.MFCS.2021.59`.

28 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE, 2020. `arXiv:2001.04383`.

29 Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. Classically verifiable quantum advantage from a computational Bell test. *Nature Physics*, 18(8):918–924, 2022. `doi:10.1038/s41567-022-01643-7`.

30 Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum Advantage from Any Non-Local Game, 2022. `arXiv:2203.15877`

31 Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. How to Delegate Computations: The Power of No-Signaling Proofs. In *Proceedings of the 46th ACM Symposium on the Theory of Computing (STOC)*, pages 485–494, 2014. `doi:10.1145/2591796.2591809`.

32 Zhenning Liu and Alexandru Gheorghiu. Depth-efficient proofs of quantumness. *Quantum*, 6:807, 2022. `doi:10.22331/q-2022-09-19-807`.

33 U. Mahadev. Classical Verification of Quantum Computations. In *Proceedings of the 59th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 259–267, 2018. doi:10.1109/FOCS.2018.00033.

34 Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. Efficient Certifiable Randomness from a Single Quantum Device, 2022. arXiv:2204.11353

35 Dominic Mayers and Andrew Yao. Self Testing Quantum Apparatus. *Quantum Info. Comput.*, 4(4):273–286, 2004. doi:10.26421/QIC4.4-3.

36 M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012. doi:10.1088/1751-8113/45/45/455304.

37 Matthew McKague. Self-testing in parallel with CHSH. *Quantum*, 1:1, 2017. doi:10.22331/q-2017-04-25-1.

38 Tony Metger, Yfke Dulek, Andrea Wei Coladangelo, and Rotem Arnon-Friedman. Device-independent quantum key distribution from computational assumptions. *New Journal of Physics*, 2021. doi:10.1088/1367-2630/ac304b.

39 Tony Metger and Thomas Vidick. Self-testing of a single quantum device under computational assumptions. *Quantum*, 5:544, 2021. doi:10.22331/q-2021-09-16-544.

40 Akihiro Mizutani, Yuki Takeuchi, Ryo Hiromasa, Yusuke Aikawa, and Seiichiro Tani. Computational self-testing for entangled magic states. *Physical Review A*, 106:L010601, 2022. doi:10.1103/PhysRevA.106.L010601.

41 Anand Natarajan and Thomas Vidick. A Quantum Linearity Test for Robustly Verifying Entanglement. In *Proceedings of the 49th ACM Symposium on the Theory of Computing (STOC)*, pages 1003–1015, 2017. doi:10.1145/3055399.3055468.

42 Anand Natarajan and Thomas Vidick. Low-Degree Testing for Quantum States, and a Quantum Entangled Games PCP for QMA. In *Proceedings of the 59th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 731–742, 2018. doi:10.1109/FOCS.2018.00075.

43 Sandu Popescu and Daniel Rohrlich. Which states violate Bell's inequality maximally? *Physics Letters A*, 169(6):411–414, 1992. doi:10.1016/0375-9601(92)90819-8.

44 Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, 56(6), 2009. doi:10.1145/1568318.1568324.

45 Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013. doi:10.1038/nature12035.

46 Pavel Sekatski, Jean-Daniel Bancal, Sebastian Wagner, and Nicolas Sangouard. Certifying the Building Blocks of Quantum Computers from Bell's Theorem. *Physical Review Letters*, 121:180505, 2018. doi:10.1103/PhysRevLett.121.180505.

47 Stephen J. Summers and Reinhard Werner. Maximal violation of Bell's inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, 110(2):247–259, 1987. doi:10.1007/BF01207366.

48 Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, 2020. doi:10.22331/q-2020-09-30-337.

49 Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. Delegation for bounded space. In *Proceedings of the 45th ACM Symposium on the Theory of Computing (STOC)*, pages 565–574, 2013. doi:10.1145/2488608.2488679.

50 B. S. Tsirel'son. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987. doi:10.1007/BF01663472.

51 Thomas Vidick. Course FSMP, Fall 2020: Interactions with Quantum Devices, 2020. Lecture notes available at: http://users.cms.caltech.edu/~vidick/teaching/fsmp/fsmp.pdf. Date accessed: 29th March 2023.

52 Thomas Vidick and Tina Zhang. Classical zero-knowledge arguments for quantum computations. *Quantum*, 4:266, 2020. doi:10.22331/q-2020-05-14-266.

53 Thomas Vidick and Tina Zhang. Classical Proofs of Quantum Knowledge. In *Advances in Cryptology – EUROCRYPT 2021*, pages 630–660, 2021. doi:10.1007/978-3-030-77886-6_22.

54 Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87:050102, 2013. doi:10.1103/PhysRevA.87.050102.

55 Daiwei Zhu, Gregory D. Kahanamoku-Meyer, Laura Lewis, Crystal Noel, Or Katz, Bahaa Harraz, Qingfeng Wang, Andrew Risinger, Lei Feng, Debopriyo Biswas, Laird Egan, Alexandru Gheorghiu, Yunseong Nam, Thomas Vidick, Umesh Vazirani, Norman Y. Yao, Marko Cetina, and Christopher Monroe. Interactive Protocols for Classically-Verifiable Quantum Advantage, 2021. arXiv:2112.05156