Letter

Impossibility of adversarial self-testing and secure sampling

Akshay Bansal,[1,*] Atul Singh Arora,[2,3,*] Thomas Van Himbeeck,[4] and Jamie Sikora[1]
[1]*Department of Computer Science, Virginia Tech, Blacksburg, Virginia 24061, USA*
[2]*Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, California 91125, USA*
[3]*Joint Center for Quantum Information and Computer Science (QuICS), University of Maryland & NIST, College Park, Maryland 20742, USA*
[4]*Télécom Paris—LTCI, Inria, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France*

(Received 29 October 2023; accepted 9 July 2024; published 21 August 2024)

Self-testing is the task where spatially separated Alice and Bob cooperate to deduce the inner workings of untrusted quantum devices by interacting with them in a classical manner. We examine the task above where Alice and Bob do not trust each other which we call adversarial self-testing. We show that adversarial self-testing implies secure sampling—a simpler task that we introduce where distrustful Alice and Bob wish to sample from a joint probability distribution with the guarantee that an honest party's marginal is not biased. By extending impossibility results in two-party quantum cryptography, we give a simple proof that both of these tasks are impossible in all but trivial settings.

DOI: 10.1103/PhysRevResearch.6.L032039

Introduction. The last few decades have witnessed massive leaps in the capabilities of quantum computers, in terms of both theory and implementation. With intensified efforts from government, industry, and academia, the future where useful quantum computers are widely accessible is becoming closer to a reality every day. The availability of such quantum devices begs the question of whether one can trust that they are performing as advertised. In other words, should we blindly trust the output of quantum mechanical devices? And if not, is there a way to test them?

Somewhat surprisingly, one can sometimes test spatially separated devices to see if they are doing what they are purported to be doing based solely on its (classical) input/output behavior and the assumption that quantum mechanics is a faithful description of Nature. This area is broadly referred to as self-testing. As an early example, Coladangelo, Goh, and Scarani showed that any pure bipartite state can be self-tested [1]. In addition, other strong results have been reported [2–9]. Many of these deal with two parties, call them Alice and Bob, who cooperate to ascertain the inner workings of the respective quantum devices.[1]

In this Letter, we prove that to self-test quantum devices, it is necessary that Alice and Bob cooperate. More precisely, we define adversarial self-testing as the self-testing task in the setting where Alice and Bob do not trust each other and give a surprisingly simple proof that this task cannot be realized. To this end, we use adversarial self-testing to perform a simpler task we call secure sampling, and then leveraging results from quantum cryptography, show that secure sampling is impossible. We now introduce these two tasks in detail.

Self-testing setting. Consider a quantum mechanical device shared by two mutually trusting parties, Alice and Bob, each having their own part of the device which we refer to as a box. Each box has several buttons (input choices) and, upon pressing a button, one of several lights turns on (indicating an output). Crucially, suppose that the two boxes are not allowed to communicate after they are distributed to the parties (e.g., by ensuring enough physical separation between them).

The most general physical description of such a device is given by a device specification

$$\mathsf{spec} := \left(|\psi\rangle_{AB}, \{M_a^x\}, \{M_b^y\} \right),$$

where $|\psi\rangle_{AB}$ is bipartite quantum state in an arbitrary Hilbert space, the projector M_a^x corresponds to Alice inputting x and obtaining outcome a, and similarly M_b^y corresponds to Bob inputting y and obtaining outcome b. We call the joint probability distribution of getting outcomes (a, b) from the boxes, given inputs (x, y), a quantum correlation, and denote it by

$$p(ab|xy) = \langle\psi| M_a^x \otimes M_b^y |\psi\rangle . \tag{1}$$

Note that the marginals satisfy $p(a|x) = p(a|xy)$ and $p(b|y) = p(b|xy)$.

In some cases, given that such a device produces a specific correlation $p(ab|xy)$, one can deduce the state $|\psi\rangle_{AB}$ and the measurements $\{M_a^x\}, \{M_b^y\}$ up to local isometries, i.e., one can self-test the device. In particular, one may be able to deduce that the state is entangled. In cryptographic contexts, self-testing allows one to model the quantum devices as black boxes and thereby establish device-independent security for tasks such as quantum key distribution. Treating quantum devices as black boxes already includes the possibility that the

[*]These authors contributed equally to this work.

[1]Recent works [10,11] give self-testing schemes of single devices using computational assumptions. We do not place any such limitations on Alice and Bob in this work.

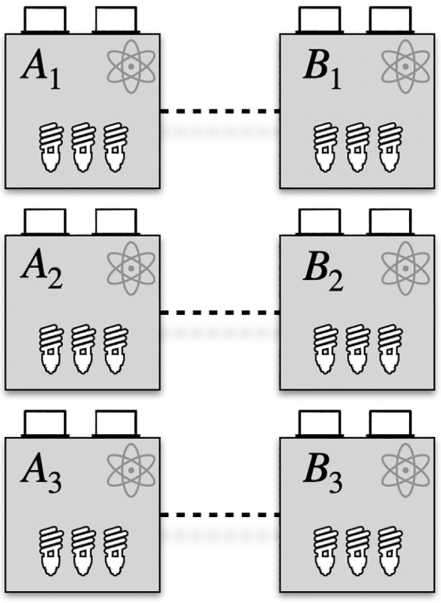

FIG. 1. Alice and Bob share several pairs of boxes but have no reason to trust them. They could test all but one and deduce (with hopefully high confidence) that either the boxes are faulty or the untested box will behave as expected.

quantum devices are prepared by the adversary and therefore yield secure constructions even against such powerful adversaries [12–15].

How does one test whether the device, in fact, produces the purported correlation $p(ab|xy)$? Assuming Alice and Bob can communicate classically, they can start with n devices and use $n-1$ randomly among them to test for the right correlation [16].[2] More concretely (see also Fig. 1), Alice could randomly select $n-1$ devices, measure them, and share this information with Bob who can then measure his part of the corresponding devices. He can then decide whether the purported correlation is consistent and share the result with Alice. If they are satisfied, they can use the remaining device, confident that it will work as claimed.

The literature on self-testing and its use in quantum cryptography, in summary, points to the following recurring theme.

Theme: The ability to self-test suggests security in quantum cryptography.

Note that in the discussion above, even though Alice and Bob did not trust their quantum devices, they did trust each other.

Adversarial self-testing. Consider the fully distrustful setting [17] where Alice trusts neither her devices nor Bob, and similarly Bob trusts neither his devices nor Alice. Conceptually, define adversarial self-testing to be the natural extension of self-testing to this fully distrustful setting.

[2]In the literature, the more common setting is where all n devices are measured right away. See, e.g., [15] that shows how self-testing is used for key distribution. Note that, in both cases, the devices are not assumed to be identical.

We first look at why the self-testing procedure involving n devices fails and then suggest a plausible alternative.

In (standard) self-testing as described above, suppose Bob is malicious and he created the devices for his own nefarious purposes. If Alice suspects this might be the case, then she has no reason to trust the tests (that only he performed) nor his final decision to use the remaining device.

To alleviate this issue, we allow the parties to exchange boxes—this can be achieved using quantum communication [17]. We also allow them to prevent communication across the boxes they possess (e.g., by shielding). The idea is to have both parties perform tests and, furthermore, if a party chooses to test device i, they ask for the corresponding box from the other party to run the test themselves using both boxes. A plausible protocol based on the cut-and-choose idea is for Bob to test roughly half the devices, selected uniformly at random, and then if he is satisfied, to allow Alice to perform her own tests. She can select all but one of the remaining devices and perform her own tests. If she is also satisfied, then they agree to use the remaining device.

Why might such a strategy work? Since Alice and Bob's test involve randomly select devices, then regardless of who might have tampered with the devices, neither of them has full control over which device is ultimately used and as such, each device is likely to be tested.

Before proceeding, we briefly remark on two important distinctions between the two settings. First, even though exchanging boxes is relevant for adversarial self-testing, as motivated above, it does not offer any advantage in the (standard) self-testing setting. This is because Alice and Bob can coordinate and broadcast their inputs and outputs and collectively process their statistics. Second, in (standard) self-testing, once the boxes are prepared and distributed, they can no longer be modified. However, for adversarial self-testing, a malicious party can tamper with the boxes at any point during the protocol as long as the box is in their possession. In fact, the only constraint is that the malicious party cannot tamper with the boxes currently held by the honest party. For example, suppose Alice and Bob share two pairs of boxes and Alice asks Bob to send her his box from the first pair. Then Bob can tamper with his box right before he sends it, such that it acts in a way favorable to him. See Fig. 2 for an illustration.

What is known about adversarial self-testing? Recently, notions closely related to it have implicitly appeared in certain device-independent cryptographic settings, such as weak coin flipping [16] and network entanglement certification [18]. In these works, only one-sided tests were used, i.e., where either Alice tests Bob or Bob tests Alice. Moreover, for coin flipping, only partial security was obtained. This begs the question of whether one can have a (two-sided) adversarial self-test to achieve ideal security for such tasks. In this work, we show that this is impossible.

Our contributions. We start by concretely defining adversarial self-testing. Consider a device specification $\mathsf{spec} := (|\psi\rangle_{AB}, \{M_a^x\}, \{M_b^y\})$ and n untrusted quantum devices purportedly consistent with spec. We denote the ith untrusted device by two boxes $\square_{A,i}$ and $\square_{B,i}$. Let Alice and Bob be two remote parties, connected by a classical channel and a quantum channel. Alice and Bob are uncorrelated initially except that Alice holds boxes $\{\square_{A,i}\}_i$ and Bob holds $\{\square_{B,i}\}_i$.

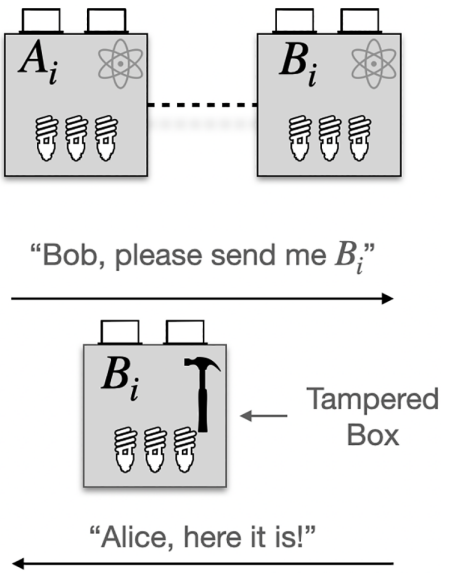

FIG. 2. If Bob is malicious, he can tamper with the boxes adaptively. For example, he can tamper with box $\square_{A,i}$ when it was created, then change the contents of $\square_{B,i}$ later before sending it to Alice.

Assume that, at any point during the protocol, boxes held by Alice cannot communicate with those held by Bob and also that the parties can choose to prevent communication among the boxes in their possession. Let $\mathcal{P}$ be a bipartite protocol among Alice and Bob, which specifies a procedure for the two parties to perform classical computations, exchange classical messages, measure, and exchange $n-1$ of the n untrusted quantum devices. Based on this, each party either outputs $\perp$ denoting abort or an index $j \in \{1, \ldots n\}$ that specifies the certified unused quantum device.

Consider the following three situations describing the various adversarial attacks we allow when the target specification is spec. In each, an honest party proceeds exactly as specified by $\mathcal{P}$.

(i) *Fully trusted.* Both parties are assumed to be honest and all n quantum devices are specified by spec.

(ii) *Trusted parties (but untrusted devices).* Both parties are assumed to be honest but all n quantum devices are created by an adversary.

(iii) *Fully distrustful.* An adversary creates the devices and controls one party, say Bob, i.e., can make Bob arbitrarily deviate from protocol $\mathcal{P}$. The only restriction on the adversary is that it cannot influence Alice's classical computations and it cannot influence any quantum box while it is held by Alice. It is similar when Alice is controlled by the adversary.

We set up some notation. We say that a device specification $(|\phi\rangle_{A'B'}, \{N_a^x\}, \{N_b^y\})$ is δ close to the target specification spec if there are local isometries $\Phi_{A'} : A' \to AA''$ and $\Phi_{B'} : B' \to BB''$ such that

$$\Phi\left(\left(N_a^x \otimes N_b^y\right)|\phi\rangle_{A'B'}\right) \approx_\delta \left(M_a^x \otimes M_b^y\right)|\psi\rangle_{AB} \otimes |\mathsf{junk}\rangle_{A''B''}$$

for all x, y, a, b, where $\Phi := \Phi_{A'} \otimes \Phi_{B'}$ and $\approx_\delta$ is used to denote that the states are at most δ far in trace distance. Then, adversarial self-testing is defined as follows.

Definition 1 (Adversarial self-test). $\mathcal{P}$ adversarially self-tests the device specification $\mathsf{spec} := (|\psi\rangle_{AB}, \{M_a^x\}, \{M_b^y\})$, if there exist decreasing vanishing functions $\epsilon, \delta \geqslant 0$ such that the following conditions hold, corresponding to the three situations above.

(i) *Correctness (Fully trusted).* Both parties output the same device index j (and neither aborts).

(ii) *Self-testing (Trusted parties).* Both parties have identical outputs and with probability at least $1-\epsilon(n)$, the protocol either aborts or, given that the protocol does not abort, the certified device $(|\phi\rangle_{A'B'}, \{N_a^x\}, \{N_b^y\})$ is $\delta(n)$ close to the target specification spec.

(iii) *Adversarial self-testing (Fully distrustful).* Suppose Alice is honest and Bob is controlled by the adversary. When Alice does not abort, we denote by $|\phi\rangle_{A'B'}$ the purification of the state in Alice's certified box and assume its purification is held by Bob. We denote by $\{N_a^x\}$ the measurements corresponding to Alice's certified box. Then, it is required that irrespective of Bob's output, the same condition as in the self-testing case above holds for some measurements $\{N_b^y\}$. The analogous condition must also hold when Bob is honest and Alice is controlled by the adversary.

We make two remarks about our definition. (i) Observe that if a specification spec can be adversarially self-tested then, in particular, spec can be self-tested in the standard setting (i.e., without exchanging boxes). (ii) A weakened variant of the third requirement, for instance, by assuming that one party, say Alice, is always honest, can be realized and has also found applications [16,18], as discussed earlier.

Consider any device specification spec that produces a product correlation, i.e., $p(ab|xy) = p(a|x)p(b|y)$ for all a, b, x, y where $p(ab|xy)$ is as in Eq. (1). This correlation can be produced locally (without shared randomness) and classically. Therefore, any guarantee from self-testing, which must be up to local isometries, becomes meaningless. Remark (i) above entails that adversarial self-testing is, consequently, also meaningless in this case.

What can one say about device specifications that produce nonproduct correlations, i.e., $p(ab|xy) \neq p(a|x)p(b|y)$ for some a, b, x, y? In [1], the authors show that for every entangled state, one can find measurements such that the resulting device specification can be self-tested. Can one extend this to adversarial self-testing? The following result shows that adversarial self-testing is impossible for any meaningful specification.

Theorem 1. Any device specification spec that produces nonproduct correlations [i.e., $p(ab|xy) \neq p(a|x) \cdot p(b|y)$ for some a, b, x, y where $p(ab|xy)$ is as in Eq. (1)] cannot be *adversarially self-tested*.

Adversarial self-testing of spec implies one can securely sample, a simpler task we define below, according to the correlation $p(ab|xy)$ [which is produced by spec as in Eq. (1)]. Clearly, if secure sampling of $p(ab|xy)$ is impossible, the proof of Theorem 1 is immediate. The remaining discussion focuses on proving the impossibility of secure sampling of nonproduct correlations.

Secure sampling. We consider secure sampling in the bipartite setting where the parties are untrusted but their quantum devices are trusted. More concretely, a valid protocol for

securely sampling from the joint distribution $p(ab|xy)$ is an interactive protocol among Alice and Bob who are given inputs x, y and produce outputs a, b (or abort). The protocol specifies local quantum computations for each party, involving exchange quantum messages, to compute their respective outputs.

As before, note that a malicious Alice may digress from the protocol. She may try to bias the marginal distribution of b. Similarly a malicious Bob may try to bias the marginal distribution of a. Note also that it does not make sense to consider the entire joint distribution $p(ab|xy)$ in the security analysis. This is because a malicious party can always output anything they wish, at the end. Thus, what makes sense is to bound the deviations away from the marginal distributions $p(a|x)$ and $p(b|y)$.

We say that $p(ab|xy)$ can be δ securely sampled for a $\delta > 0$, if there exists a protocol such that for any pair of outputs (a, b), for any input (x, y) the following hold.

(i) When both Alice and Bob are honest, they output a and b with probability $p(ab|xy)$.
(ii) The probability that Alice outputs a is at most $p(a|x) + \delta$ when Bob cheats (implying she did not abort).
(iii) The probability that Bob outputs b is at most $p(b|y) + \delta$ when Alice cheats (implying he did not abort).

In words, a malicious party can only really influence the honest party's outcome toward "cheating detected." We say that a distribution $p(ab|xy)$ can be securely sampled if for any $\delta > 0$, the distribution can be δ securely sampled. Note that, product correlations can be trivially sampled securely—the parties sample their own outputs, depending on their respective inputs. We prove that the converse also holds.

Theorem 2. Given a *correlation*[3] $p(ab|xy)$, secure sampling is possible if and only if it is a product correlation.

From the definitions, one can check that adversarial self-testing of spec that produces $p(ab|xy)$ implies there is a protocol for secure sampling from $p(ab|xy)$. Thus, Theorem 1 follows directly from Theorem 2. Turning to the proof of Theorem 2, we start with a simple fact about nonproduct correlations.

Lemma. For a nonproduct correlation $p(ab|xy)$, there exist a, b, x, and y such that

$$p(ab|xy) > p(a|x) \cdot p(b|y). \tag{2}$$

To prove this, suppose that for all a, b, x, and y we have

$$p(ab|xy) \leqslant p(a|x) \cdot p(b|y). \tag{3}$$

Then, for any fixed x and y, one can easily see that $p(ab|xy) = p(a|x) \cdot p(b|y)$ by adding over a and b on both sides, and using the fact that if $0 \leqslant \Delta_i$ and $\sum_i \Delta_i = 0$, it follows that $\Delta_i = 0$ for each i. Thus, $p(ab|xy)$ is a product correlation, a contradiction.

The above lemma says that there is some input pair (x', y') such that Alice and Bob's outcomes are correlated, i.e., not sampled from a product probability distribution. Henceforth, we focus on secure sampling of the nonproduct distribution $p(ab) := p(ab|x'y')$. This particular nonproduct distribution is exactly the issue when Alice and Bob try to adversarial self-test. It turns out that Alice or Bob can always bias the marginals of nonproduct distributions in quantum settings which we show follows from the insecurity of certain tasks in quantum two-party cryptography. The literature on this area contains many impossibility results. Some of the more popular tasks include bit commitment [19–21], strong coin flipping [22,23], die rolling [24,25], oblivious transfer [26–28], and, more generally, secure function evaluation [29,30] (many of the references above point toward their impossibility). With this said, we revisit the theme of this paper, stated in the contrapositive.

Theme, restated: The insecurity in quantum cryptography suggests the inability to self-test.

To illustrate this connection, we consider one particular task within two-party cryptography we alluded to earlier, coin flipping, where Alice and Bob wish to generate a shared uniformly random bit. In other words, they wish to securely sample from the joint distribution $p(ab) = \frac{1}{2}\delta_{a,b}$. However, there is a constant lower bound on the security of any quantum coin flipping protocol due to Kitaev [22] indicating that this particular distribution cannot be securely sampled. Can one say something more generally?

Indeed, Kitaev's lower bound states that for any quantum protocol that samples from the joint distribution $p(ab)$, we must have

$$p^*(a) \cdot p^*(b) \geqslant p(ab) \tag{4}$$

for any fixed a and b, where we use the following notation.

(i) $p(ab)$: The probability with which Alice and Bob output a and b (when both follow the protocol honestly).
(ii) $p^*(a)$: The maximum probability Bob can force Alice to output a (when she follows the protocol honestly).
(iii) $p^*(b)$: The maximum probability Alice can force Bob to output b (when he follows the protocol honestly).

Now, suppose one can securely sample from the nonproduct distribution $p(ab)$. Then, for any fixed $\delta > 0$, there exists a protocol such that $p(a) + \delta \geqslant p^*(a)$ and $p(b) + \delta \geqslant p^*(b)$. Combining with Kitaev's bound, we have

$$(p(a) + \delta)(p(b) + \delta) \geqslant p^*(a) \cdot p^*(b) \geqslant p(ab) \tag{5}$$

for any a and b. By taking limits as $\delta \to 0$, we have that $p(a) \cdot p(b) \geqslant p(ab)$ for all a and b which can only hold for product distributions from our lemma—a contradiction. Thus, $p(ab)$ cannot be securely sampled, completing the proof of Theorem 2.

Multiparty setting. We now briefly discuss the possibility of secure sampling if there are more than two parties. Consider the task where there are n parties who wish to sample from the joint distribution $p(a_1 a_2 \ldots a_n)$ where party i outputs a_i. One may wonder if there is some way to use the extra parties involved to test the devices. It turns out that this is also impossible for certain distributions. We say that a mulitpartite distribution is nontrivial if there exists a partition, such that $p(a_1 a_2 \ldots a_n)$ is nonproduct across that partition. Consider such a nontrivial multipartite distribution and call the partitions A for "Alice" and B for "Bob" (this suggestive naming convention will make sense shortly). If we also set a to be the tuple $(a_i : i \in A)$, and b to be the tuple where

[3]Recall that we only consider correlations/distributions that can arise from measuring a quantum state with local measurements.

$(a_i : i \in B)$, we have effectively reduced the multiparty setting to the two-party setting where we only have Alice and Bob. Since $p(ab)$ is nontrivial, then we cannot securely sample from this distribution. Here, when Alice or Bob cheats, we suppose that they are not bound by any locality constraints. That is, they are allowed to act as a single cheating entity. In summary, we cannot securely sample a nontrivial multiparty distribution since there exists one subset of the parties who can (collectively) cheat the rest. Thus, if we generalize adversarial self-testing to multiple parties, we see that this is impossible as well if a certain partition and choice of inputs leads to a nonproduct distribution.

Comparisons to previous work. The work [31] considers nonlocal games in a two-phase setting where, in the first phase, the two parties cooperate to play the game and in the second phase, they try to learn the other party's output. It shows that even if the other party's input is revealed, their output remains random. The multiparty case with dishonest parties has been studied in [18]. In this work, the identity of the malicious parties is known in advance. In [16], these ideas are applied to improve protocols for the cryptographic task of weak coin flipping. All these works can be interpreted as positive results as contrasted to our negative result. Indeed, they all have assumptions concerning how the parties trust each other (while we make no assumptions). This opens the question of what possible results can be obtained in this adversarial setting if one places assumptions/restrictions on the cheating parties involved.

Conclusions. In this Letter, we proved that one cannot securely sample nonproduct probability distributions, and thus adversarial self-testing of devices producing nonproduct correlations is also impossible. For future work, it would be interesting to see if a form of adversarial self-testing is possible in certain multiparty settings. Perhaps restricting the cheating subsets to only have a small number of parties would circumvent the impossibility. Another interesting research avenue would be to see how our results change if one were to add restrictions to what Alice and Bob are allowed to do when tampering with the boxes. Kitaev's lower bound is in the information-theoretic setting; it may not hold if we impose certain restrictions on Alice and Bob (e.g., Alice and Bob are computationally bounded). We believe that adversarial self-testing should be possible in this restricted setting.

Acknowledgments. We are thankful to J. Bartusek for helpful discussions. A.B. is partially supported by a Bitshares Fellowship. A.S.A. acknowledges support from IQIM, an NSF Physics Frontier Center (GBMF-1250002), MURI Grant No. FA9550-18-1-0161, and the US Department of Defense through a QuICS Hartree Fellowship. Part of the work was carried out while A.S.A. was visiting the Simons Institute for the Theory of Computing. T.V.H. acknowledges support from ParisRegionQCI, supported by Paris Region; FranceQCI, supported by the European Commission, under the Digital Europe program; and QSNP: European Union's Horizon Europe research and innovation program under the project "Quantum Security Networks Partnership." J.S. is partially supported by Commonwealth Cyber Initiative SWVA Grant No. 467489 and by Virginia Tech's Open Access Subvention Fund.

[1] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).

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

[3] S. Breiner, A. Kalev, and C. A. Miller, Parallel self-testing of the GHZ state with a proof by diagrams, EPTCS **287**, 43 (2019).

[4] 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).

[5] A. Coladangelo, Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension, Phys. Rev. A **98**, 052115 (2018).

[6] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Device-independent entanglement certification of all entangled states, Phys. Rev. Lett. **121**, 180503 (2018).

[7] C. A. Miller and Y. Shi, Optimal robust self-testing by binary nonlocal XOR games, in *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013), Guelph, Canada*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 22 (Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, 2013), pp. 254–262.

[8] J. Sikora, A. Varvitsiotis, and Z. Wei, Minimum dimension of a Hilbert space needed to generate a quantum correlation, Phys. Rev. Lett. **117**, 060401 (2016).

[9] J. Bartusek, D. Khurana, and A. Srinivasan, Secure computation with shared EPR pairs (or: How to teleport in zero-knowledge), *Annual International Cryptology Conference* (Springer, 2023), pp. 224–257.

[10] T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, Quantum **5**, 544 (2021).

[11] Z. Brakerski, A. Gheorghiu, G. D. Kahanamoku-Meyer, E. Porat, and T. Vidick, Simple tests of quantumness also certify qubits, arXiv:2303.01293.

[12] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Phys. Rev. Lett. **98**, 230501 (2007).

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

[14] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[15] U. Vazirani and T. Vidick, Fully device independent quantum key distribution, Commun. ACM **62**, 133 (2019).

[16] A. S. Arora, J. Sikora, and T. V. Himbeeck, Improving device-independent weak coin flipping protocols, arXiv:2404.17079.

[17] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, Fully distrustful quantum bit commitment and coin flipping, Phys. Rev. Lett. **106**, 220501 (2011).

[18] G. Murta and F. Baccari, Self-testing with dishonest parties and device-independent entanglement certification in quantum communication networks, Phys. Rev. Lett. **131**, 140201 (2023).

[19] D. Mayers, Unconditionally secure quantum bit commitment is impossible, Phys. Rev. Lett. **78**, 3414 (1997).

[20] H.-K. Lo and H. F. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible, Physica D **120**, 177 (1998).

[21] A. Chailloux and I. Kerenidis, Optimal bounds for quantum bit commitment, in *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, Palm Springs, CA* (IEEE Computer Society, Massachusetts Ave., Washington, DC, US, 2011), pp. 354–362.

[22] A. Kitaev, Quantum coin flipping. Unpublished result, *Talk at the 6th Annual workshop on Quantum Information Processing, Berkeley, CA* (QIP, 2003).

[23] A. Chailloux and I. Kerenidis, Optimal quantum strong coin flipping, in *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Massachusetts Ave., Washington, DC, US, 2009), pp. 527–533.

[24] N. Aharon and J. Silman, Quantum dice rolling: a multi-outcome generalization of quantum coin flipping, New J. Phys. **12**, 033027 (2010).

[25] J. Sikora, Simple, near-optimal quantum protocols for die-rolling, Cryptography **1**, 11 (2017).

[26] A. Chailloux, I. Kerenidis, and J. Sikora, Lower bounds for quantum oblivious transfer, Quantum Info. Comput. **13**, 158 (2013).

[27] A. Chailloux, G. Gutoski, and J. Sikora, Optimal bounds for semi-honest quantum oblivious transfer, Chicago J. Theor. Comput. Sci. **22**, 1 (2016).

[28] S. Kundu, J. Sikora, and E. Y.-Z. Tan, A device-independent protocol for XOR oblivious transfer, Quantum **6**, 725 (2022).

[29] S. A. Osborn and J. Sikora, A constant lower bound for any quantum protocol for secure function evaluation, in *17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 232 (Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, 2022), pp. 8:1–8:14.

[30] H. Buhrman, M. Christandl, and C. Schaffner, Complete insecurity of quantum protocols for classical two-party computation, Phys. Rev. Lett. **109**, 160501 (2012).

[31] C. A. Miller and Y. Shi, Randomness in nonlocal games between mistrustful players, Quantum Inf. Comput. **17**, 0595 (2017).