

A device-independent protocol for XOR oblivious transfer

Srijita Kundu¹, Jamie Sikora², and Ernest Y.-Z. Tan¹

¹Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada

²Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada and Virginia Polytechnic Institute and State University, Blacksburg, Virginia, USA

Oblivious transfer is a cryptographic primitive where Alice has two bits and Bob wishes to learn some function of them. Ideally, Alice should not learn Bob's desired function choice and Bob should not learn any more than what is logically implied by the function value. While decent quantum protocols for this task are known, many become completely insecure if an adversary were to control the quantum devices used in the implementation of the protocol. In this work we give a fully device-independent quantum protocol for XOR oblivious transfer.

1 Introduction

Oblivious transfer is an important cryptographic primitive in two-party computation as it can be used as a universal building block for constructing more elaborate protocols [Kil88]. Indeed, some quantum protocols for this task are known [WST08, Sch07, CKS13, CGS16]. However, it can be shown that there do not exist classical protocols with any level of information-theoretic security, and there do not exist quantum protocols with perfect security [CKS13, Lo97].

In this paper, we consider a variant of oblivious transfer called *XOR oblivious transfer (XOT)*. This is the two-party cryptographic primitive in which two spatially separated parties, Alice and Bob, wish to do the following task: Alice outputs two bits (x_0, x_1) , which are uniformly random, and Bob outputs a trit b which is uniformly random, as well as x_b where we define $x_2 = x_0 \oplus x_1$. In other words, Alice and Bob communicate and Bob learns one bit of information from Alice's two bits (either the first bit, second bit, or their XOR). When designing XOT protocols, the security goals are:

1. *Completeness*: If both parties are honest, then their outcomes are consistent (i.e., x_b is the correct value), uniformly random, and neither party aborts.
2. *Soundness against cheating Bob*: If Alice is honest, then a dishonest (i.e., cheating) Bob cannot learn both x_0 and x_1 by digressing from protocol.
3. *Soundness against cheating Alice*: If Bob is honest, then a dishonest (i.e., cheating) Alice cannot learn b by digressing from protocol.

Srijita Kundu: srijita.kundu@uwaterloo.ca

Jamie Sikora: sikora@vt.edu

Ernest Y.-Z. Tan: yzetan@uwaterloo.ca

Remark 1. One could imagine a situation where Alice already has a fixed choice of (x_0, x_1) that she wishes to input into a XOT protocol (perhaps from the result of an earlier computation). However, we can use the outcomes of an XOT protocol as described above as a one-time pad to convey the information to Bob. For more details, see [CKS13].

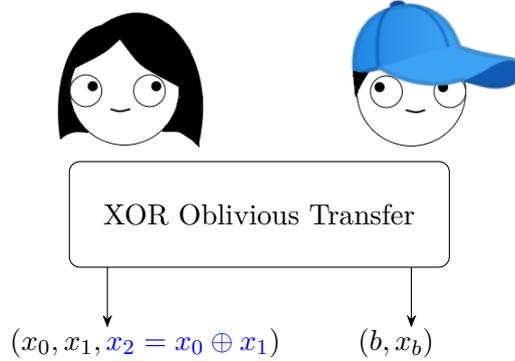


Figure 1: Desired outputs for XOR oblivious transfer (XOT).

In this paper we are concerned with *information-theoretic security*, meaning that Alice and Bob are only bounded by the laws of quantum mechanics. In other words, Alice and Bob can perform arbitrarily complicated computations, have arbitrarily large quantum memories, and so on. We shall have occasion to change how much control Alice and Bob have over the protocol, but precisely what actions are allowed to be performed by dishonest parties should be clear from context, and will be described shortly.

We focus on studying XOT protocols from the perspective of assuming perfect completeness and trying to make them as sound as possible.¹ To this end, we choose to quantify the soundness via *cheating probabilities*, which we define as follows:

- P_B^{XOT} : The maximum probability with which a dishonest Bob can learn both of honest Alice's outcome bits (x_0, x_1) and the protocol does not abort.
- P_A^{XOT} : The maximum probability with which a dishonest Alice can learn honest Bob's choice outcome b and the protocol does not abort.

Any XOT protocol with perfect completeness necessarily has $P_A^{\text{XOT}} \geq \frac{1}{3}$ and $P_B^{\text{XOT}} \geq \frac{1}{2}$, since a dishonest Alice could always guess one of three choices for Bob's outcome b uniformly at random and, similarly, dishonest Bob can follow the honest protocol to gain perfect knowledge of x_0, x_1 , or $x_0 \oplus x_1$, and then randomly guess the unknown bit in Alice's outcome (x_0, x_1) .

Remark 2. In this work, we chose to quantify soundness via cheating probabilities, but we note that such a measure of security is not necessarily composable [WW08, VPdR19]. Unfortunately, it can be very challenging to prove that a protocol is composable secure, and in some settings such protocols are in fact impossible [VPdR19]. As a first analysis of the protocol proposed in this work, we will restrict ourselves to studying the cheating probabilities only.

¹To contrast, the task of finding protocols with perfect soundness and the best possible completeness was considered in [SCK14].

Since the lowest possible bounds on P_A^{XOT} and P_B^{XOT} for perfectly complete XOT protocols are asymmetric, we shall consider them in pairs and will not concern ourselves with finding an “optimal protocol”. Instead, we motivate our work by asking the following question:

“Is it possible to create quantum protocols where both $P_A^{\text{XOT}}, P_B^{\text{XOT}} < 1$ when Alice and Bob do not even trust their own quantum devices?”

When taken literally, this question cannot be answered in the affirmative, since arbitrarily malicious devices could simply broadcast all desired information to a dishonest party. However, it turns out that there exist quantum protocols that can be proven secure using almost no assumptions other than ruling out this extreme scenario (which seems a rather necessary assumption in any case). This is the notion of *device-independent security*, which typically exploits *nonlocal games* played using entangled states. In a fully device-independent model, one only assumes that the parties’ devices do not directly broadcast certain information to the dishonest party and/or each other (we shall explain this in more detail in Section 1.4). In particular, one does not assume that the states and/or measurements implemented by the devices are known, and even the dimensions of the quantum systems are not specified. Device-independent security analyses exist for other cryptographic tasks such as quantum key distribution [PAB⁺09, AFDF⁺18], bit commitment [SCA⁺11, AMPS16], coin-flipping [ACK⁺14], and weak string erasure (in the bounded or noisy storage models) [KW16]. The approach we use in this work is somewhat similar to [ACK⁺14].

Coin flipping, bit commitment and weak string erasure are all two-party cryptographic tasks like oblivious transfer. There are classical constructions of bit commitment and coin-flipping from oblivious transfer. Since these constructions do not use trusted quantum states or measurements to perform the conversion, we think it would be possible to obtain device-independent bit commitment and coin-flipping from device-independent oblivious transfer, although the resulting cheating probabilities may not be optimal. In the reverse direction, there is a quantum construction of oblivious transfer from bit commitment as well [Unr10]. However, this construction was not designed to be device-independent (it relies on sending trusted states), hence a device-independent protocol for oblivious transfer is not implied by [SCA⁺11, AMPS16]. Weak string erasure is a task very similar to oblivious transfer, but the protocol for weak string erasure given in [KW16] assumes noisy or bounded quantum storage in addition to the standard minimal assumptions in the device-independent framework, and hence does not directly yield device-independent oblivious transfer without those assumptions.

In this work, we examine the security of quantum XOT protocols in semi-device-independent and device-independent scenarios. A semi-device-independent scenario is weaker than the fully device-independent scenario described above; specifically, the honest parties may trust the state preparation devices, or the measurement devices, or quantum operations, or some combination of these. By a slight abuse of notation, we use the same notation P_A^{XOT} and P_B^{XOT} to denote the cheating probabilities of Alice and Bob in all the different scenarios, corresponding to differently defined cheating capabilities of the dishonest party. For example, if we were to allow a dishonest Alice to control Bob’s measurements, it may lead to a different value of P_A^{XOT} . The cheating capabilities of cheating parties should be clear from context when we discuss P_A^{XOT} and P_B^{XOT} .

1.1 Trivial protocols

For readers new to oblivious transfer, we present two bad classical protocols and a simple quantum protocol.

Protocol 1 (Bad XOT Protocol 1).

1. Alice chooses (x_0, x_1) uniformly at random and sends (x_0, x_1) to Bob.
2. Bob chooses b uniformly at random.
3. Alice outputs (x_0, x_1) and Bob outputs (b, x_b) .

A moment's thought shows that Bob has full information (he clearly learns (x_0, x_1)) while Alice has no information. Therefore, we have

$$P_A^{\text{XOT}} = 1/3 \quad \text{and} \quad P_B^{\text{XOT}} = 1 \quad (1)$$

which is as insecure concerning cheating Bob as possible.

Protocol 2 (Bad XOT Protocol 2).

1. Bob chooses b uniformly at random and sends b to Alice.
2. Alice chooses (x_0, x_1) uniformly at random and sends x_b to Bob.
3. Alice outputs (x_0, x_1) and Bob outputs (b, x_b) .

Here Alice has full information while Bob has none. Therefore, we have

$$P_A^{\text{XOT}} = 1 \quad \text{and} \quad P_B^{\text{XOT}} = 1/2. \quad (2)$$

Remark 3. *These protocols are obviously device-independent since they are classical. But surprisingly, these protocols can be useful — we shall use them to construct our fully device-independent protocol. The idea is this: suppose Alice wishes to test Bob to see if he has been cheating, and aborts if and only if the test fails. Then if the test passes, the parties need a way to finish executing the protocol, which they could do using Protocol 1 (which is independent of previous steps in the tested protocol).*

1.2 A quantum protocol for XOT with no device-independent security

Here we present the oblivious transfer protocol from [CKS13] adapted to the XOT setting. For $b \in \{0, 1, 2\}$, let $|\psi_b^\pm\rangle \in \mathcal{X}\mathcal{Y}$ denote the following two-qutrit state:

$$|\psi_b^\pm\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{X}\mathcal{Y}} \pm |22\rangle_{\mathcal{X}\mathcal{Y}}) & \text{if } b = 0, \\ \frac{1}{\sqrt{2}}(|11\rangle_{\mathcal{X}\mathcal{Y}} \pm |22\rangle_{\mathcal{X}\mathcal{Y}}) & \text{if } b = 1, \\ \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{X}\mathcal{Y}} \pm |11\rangle_{\mathcal{X}\mathcal{Y}}) & \text{if } b = 2. \end{cases} \quad (3)$$

Note that for every $b \in \{0, 1, 2\}$, we have that $|\psi_b^+\rangle$ and $|\psi_b^-\rangle$ are orthogonal. We are now ready to state the protocol.

Protocol 3.

1. Bob chooses $b \in \{0, 1, 2\}$ uniformly at random, prepares the state $|\psi_b^+\rangle$ in registers $\mathcal{X}\mathcal{Y}$, and sends the register \mathcal{X} to Alice.
2. Alice chooses (x_0, x_1) uniformly at random, performs the unitary
$$U_{(x_0, x_1)} = (-1)^{x_0} |0\rangle\langle 0| + (-1)^{x_1} |1\rangle\langle 1| + |2\rangle\langle 2| \quad (4)$$
on \mathcal{X} , and then sends it back to Bob.
3. Bob performs the 2-outcome measurement $\{|\psi_b^+\rangle\langle\psi_b^+|, \mathbb{1} - |\psi_b^+\rangle\langle\psi_b^+|\}$ and records his outcome as $c = 0$ if he gets $|\psi_b^+\rangle\langle\psi_b^+|$ and $c = 1$ otherwise.
4. Alice outputs (x_0, x_1) and Bob outputs (b, c) .

Protocol 3 can be checked to be complete (i.e., Bob always gets the correct outcome). The cheating probabilities in this protocol in the cases of trusted and untrusted devices are given by Theorem 1 below. We give a proof for the trusted case in Section 3, and the relatively simple proof for the untrusted case is given below.

Theorem 1. *In Protocol 3, the cheating probabilities are as listed in the following table. (In the untrusted setting, Alice controls Bob's state preparation and Bob controls Alice's unitary.)*

	P_A^{XOT}	P_B^{XOT}
Trusted devices	1/2	3/4
Untrusted devices	1	1

Untrusted device cheating strategies. As indicated in the second row of the above table, the protocol is not secure when the devices are untrusted. To see this, assume Bob has full control over Alice's unitary. It could be a unitary which implements a superdense coding protocol:

$$U_{(x_0, x_1)}^{\text{cheat}} = \begin{cases} \mathbb{1}_{\mathcal{X}} & \text{if } (x_0, x_1) = (0, 0), \\ \sigma_X & \text{if } (x_0, x_1) = (0, 1), \\ \sigma_Y & \text{if } (x_0, x_1) = (1, 0), \\ \sigma_Z & \text{if } (x_0, x_1) = (1, 1), \end{cases} \quad (5)$$

where σ_X , σ_Y , and σ_Z are the Pauli operators. (Note that this unitary acts on a qubit, which we can assume Bob sends if he wishes, or just define the unitary to act trivially on the $|2\rangle$ subspace.) Now, if Bob creates $|\psi_2^+\rangle$ at the beginning of the protocol, he is left with a state from the Bell basis at the end of the protocol. In other words, he can perfectly learn (x_0, x_1) .

In the case of cheating Alice, she can simply control Bob's state preparation device to prepare the state $|b\rangle|0\rangle \in \mathcal{X}\mathcal{Y}$ on input b , and have Bob send the register \mathcal{X} . From this state, Alice simply measures it to learn b . Thus, we have

$$P_A^{\text{XOT}} = 1 \quad \text{and} \quad P_B^{\text{XOT}} = 1 \quad [\text{Devices are NOT trusted}]. \quad (6)$$

Thus, we need a clever way to design protocols where Alice and Bob cannot cheat in the above fashion. This motivates the need for device-independent XOT protocols and some protocol design ideas that should be avoided.

1.3 A semi-device-independent XOT protocol from magic square

Similar to device-independent protocols which exist for other cryptographic tasks, we design our protocols using nonlocal games. In this work, we shall make use of the nonlocal game known as the Mermin-Peres magic square game. In the magic square game,

- Alice and Bob receive respective inputs $a \in \{0, 1, 2\}$ and $b \in \{0, 1, 2\}$ independently and uniformly at random.
- Alice outputs three bits $(x_0, x_1, x_2) \in \{0, 1\}^3$ such that $x_0 \oplus x_1 \oplus x_2 = 0$ and Bob outputs three bits $(y_0, y_1, y_2) \in \{0, 1\}^3$ such that $y_0 \oplus y_1 \oplus y_2 = 1$.
- Alice and Bob win the game if $x_b = y_a$.

Remark 4. *We have defined the magic square game such that Alice and Bob are required to produce bits satisfying their respective parity conditions, rather than defining these parity conditions as part of the win condition. This means that we can equivalently view this as Alice and Bob each producing only the bits (x_0, x_1) and (y_0, y_1) respectively, with the third bit being completely specified by the parity conditions.*

If Alice and Bob are allowed only classical strategies (using e.g. shared randomness), the magic square game cannot be won with probability greater than $8/9$. However, there exists a quantum strategy, where Alice and Bob share prior entanglement, which wins the magic square game with probability 1. We shall refer to this strategy as the *magic square strategy* which is detailed in Section 2.

Now, suppose Alice and Bob play the magic square game according to the above description. Notice that x_2 will always be equal to $x_0 \oplus x_1$, similar to the definition of XOT, and that (x_0, x_1) is uniformly distributed (see Section 2). Also, for each of Bob's input choices, he learns either x_0 , x_1 , or $x_2 = x_0 \oplus x_1$ depending on the choice of input a for Alice. Since a is chosen uniformly at random, this is almost a proper XOT protocol (putting aside soundness for now). The only missing ingredient is that Bob knows he has x_b , but does not know which of the bits of (y_0, y_1, y_2) it is. To fix this small issue, we simply have Alice tell Bob which bit it is.

We formalize this protocol below and add in a *test* step that helps to prevent cheating. Strictly speaking, Protocol 4 should be thought of as a protocol framework, as we have not specified who creates the entangled state that Alice and Bob share — either party can. We consider different security analyses of Protocol 4, corresponding to each of these different cases. In the trusted state analysis, the honest party (whomever that may be) creates the state, and in the untrusted state analysis it is the cheating party who does so.

Protocol 4 (Quantum XOT protocol from the magic square game).

1. Alice and Bob share the bipartite state used in the magic square strategy.
2. Bob chooses $b \in \{0, 1, 2\}$ uniformly at random, performs the measurements corresponding to b in the magic square strategy on his state to get the outcome $(y_0, y_1, y_2 = y_0 \oplus y_1 \oplus 1)$, and sends (y_0, y_1, y_2) to Alice.
3. Alice chooses $a \in \{0, 1, 2\}$ uniformly at random and sends a to Bob.

4. Alice performs the measurement corresponding to a in her magic square strategy on her state to get the outcome $(x_0, x_1, x_2 = x_0 \oplus x_1)$.
5. **Test:** If $(x_0, x_1, x_2) = (0, 0, 0)$ and Bob has sent (y_0, y_1, y_2) such that $y_a = 1$, then Alice aborts.
6. Alice outputs (x_0, x_1) and Bob outputs (b, y_a) .

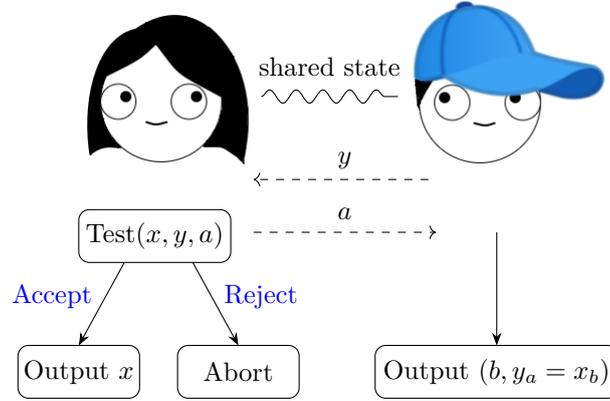


Figure 2: Schematic depiction of the messages sent in Protocol 4.

Intuitively, the test step in Protocol 4 serves as a weak test that the magic square winning condition is fulfilled (though the test only occurs with somewhat small probability). This provides a way to partially certify that Bob has measured his share of the state *before* learning Alice’s input. Note that if the test is not performed, Bob need not actually measure his state before receiving Alice’s input. So even when the states are trusted, he has the potential to perfectly learn Alice’s output after learning her input, by simply performing the same measurement as Alice on his state. However, forcing him to perform the magic square measurement “deletes” some of this information; a notion referred to as *certified deletion* in [FM18].

We note that the test is asymmetric — only Alice checks if Bob’s outputs satisfy a certain condition. This is because if we were to consider the protocol without this test, *only* Bob has any possibility of cheating: in that version Bob would not communicate at all with Alice, so she cannot learn his input (simply due to no-signalling). In our actual protocol with the test, security against Alice is no longer guaranteed via no-signalling. But as it turns out, we can still show Alice cannot perfectly learn Bob’s input from his message (if Bob’s measurement is trusted), so we do not add any further testing from Bob’s side.

It is easily verified that Protocol 4 is complete when Alice and Bob use a strategy that wins the magic square game with certainty. To prove its soundness, we compute the cheating probabilities using appropriate SDPs, as described in Section 3, for the trusted state and untrusted state cases. We summarize these cheating probabilities in the following theorem, and below it we explain why Alice and Bob can cheat perfectly if they control the other’s measurement devices.

Theorem 2. *If Alice and Bob play the “canonical” strategy for the magic square game (see Section 2), then the cheating probabilities for Alice and Bob in Protocol 4 are as shown in the table below, rounded to 5 decimal places.*

	P_A^{XOT}	P_B^{XOT}
<i>Trusted state</i>	<i>0.83333</i>	<i>0.93628</i>
<i>Untrusted state</i>	<i>0.87268</i>	<i>0.94096</i>
<i>Untrusted measurement</i>	<i>1</i>	<i>1</i>

Untrusted-measurement scenario. As the last row of the table in Theorem 2 indicates, Protocol 4 is not fully device-independent. To see this, note that if Bob were to control Alice’s measurements, he can force $(x_0, x_1) = (0, 1)$ to always occur (regardless of the state, by performing a trivial measurement), and then he will never be tested. This also fixes the value of (x_0, x_1) , so Bob knows it perfectly. Conversely, if Alice controls Bob’s measurement, she can force the output to be such that $y_b = 1$ and the other two bits are 0. Then Bob’s message fully reveals b to Alice.

1.4 A fully device-independent protocol

We now aim to find an XOT protocol based on the magic square game that is fully device-independent. We shall first clarify the premises and assumptions in such a setting. Specifically, we shall suppose that Alice and Bob each possess one of a pair of black boxes, each of which will accept a classical input in $\{0, 1, 2\}$ and return a classical output in $\{0, 1\}$ ³. We shall only require a single use of these boxes. In the honest scenario, the boxes will simply be implementing the ideal magic square states and measurements. If either party is dishonest, however, we shall suppose only that the boxes’ behaviour can be modelled as follows: the boxes share some entangled state between them, and when one of the boxes receives an input, it returns the output of some measurement (conditioned on the input) performed on its share of the quantum state, *without broadcasting either its input or output* to any party other than the one holding the box². While the honest party can only interact with the box as specified, the dishonest party is able to “open” any box they possess and perform arbitrary quantum operations or measurements on the share of the state held by that box. However, the dishonest party cannot interact with or change the behaviour of a box while it is in the honest party’s possession.

This describes the general device-independent setting. For the purposes of this work, we shall impose a small additional assumption on the states and measurements the boxes implement, namely that they are described by a tensor product of Hilbert spaces, one for each box. More general scenarios could be considered (for instance, one could require only that the two boxes’ measurements commute), but we do not consider them within this work — we shall briefly discuss this point when outlining our proof techniques below.

It would seem difficult to design a secure protocol under such weak assumptions. However, we can exploit the fact that many nonlocal games (including the magic square game) exhibit the important property of *self-testing* or *rigidity*: if the boxes win the game with probability equal to

²To take a slightly different perspective (used in e.g. [AFDF⁺18]), we could suppose that the honest party is able to “shield” their lab in a way such that signals cannot be broadcast out of it once they have supplied the input to their box.

the maximum quantum value, then they must be implementing the ideal state and measurements (up to trivial isometries). A robust version of this statement is formally expressed as Lemma 5 in the next section.

This suggests the following idea to make Protocol 4 fully device-independent: we introduce an initial step where with some probability, either party may ask to perform a single-shot test of whether the boxes win the magic square game. They do this by sending over a uniformly random input for the other party's box, and asking the other party to send over the output that they get by entering this input into their box (in the honest case). In reality a dishonest party may discard the input sent by the honest party and produce this claimed output by unknown means; but this process of obtaining the output can still be modelled by a measurement, to which we can apply a self-testing result.

To prevent a dishonest party from always calling for a test and then declaring a pass, we shall enforce that a party calling for a test must then cede all control if the test is passed, performing a trivial XOT protocol that is perfectly secure against them. Specifically, if Alice calls for the test and it passes, then Protocol 1 is performed, and if Bob calls for the test and it passes, then Protocol 2 is performed. (Here we are using several properties of Protocols 1 and 2. First, they have perfect completeness, hence ensuring that the overall protocol we construct is perfectly complete, as is the focus of this work. Second, they achieve perfect security against one party in a "trivial" device-independent sense, because they do not need trusted quantum states or measurements, albeit at the cost of being fully insecure against the other party.)³ If a test is not called, the parties simply perform Protocol 4. This idea of the parties probabilistically performing a self-test or a device-dependent protocol, and implementing a trivial protocol if the self-test passes, was also used in [ACK⁺14]. We describe this construction formally as Protocol 5 below.

Qualitatively, Protocol 5 imposes a "tradeoff" for the cheating party between passing the test (if it is called) and the extent to which they deviate from the ideal implementation of Protocol 4. More specifically, if (say) Bob is dishonest, he could cheat perfectly if Alice decides to test, by having both boxes implement the honest behaviour, and he could also cheat perfectly if Alice decides not to test, but to do so he needs to modify Alice's box's behaviour (since our device-dependent arguments show that perfect cheating is impossible when Alice's box is honest). Since Alice's box must behave differently in the two scenarios and Bob cannot change how that box behaves once the protocol starts, Alice can constrain his cheating probability by randomly choosing between testing and not testing. A similar argument applies to cheating Alice.

Note that for this reasoning to be valid, it is important that the honest party's box cannot be allowed to detect whether it is being subjected to a magic square test or whether it is being used for Protocol 4 (we are implicitly assuming that the honest party's box behaves the same way in both situations). An assumption of this nature is typically required in device-independent protocols that involve performing a test with some probability, e.g. [ACK⁺14, AFDF⁺18]. In particular, as observed in [ACK⁺14], we note that if the behaviour of the boxes could be time-dependent, then the honest party must ensure they provide the input to their box at a fixed pre-determined time, regardless of whether the box is being tested or used for Protocol 4.

³One may want to implement protocols that are better than Protocols 1 and 2 in this construction to improve its performance (for instance, protocols that achieve partial security against the tested party in addition to the perfect security against the testing party). However, proving such improved performance would require device-independent security guarantees on whatever protocols are used in place of Protocols 1 and 2, and we do not know any other device-independent protocols for XOT.

Protocol 5 (Quantum XOT protocol from the magic square game *with extra test steps*).

1. Alice flips a coin whose outcome is 0 with probability $1 - q^A$, to obtain $c^A \in \{0, 1\}$, which she sends to Bob.
2. (a) If $c^A = 0$, Bob flips a coin whose outcome is 0 with probability $1 - q^B$, to obtain $c^B \in \{0, 1\}$, which he sends to Alice.
 (b) If $c^A = 1$, Alice picks uniformly random $a^A, b^A \in \{0, 1, 2\}$, enters a^A into her box, and sends b^A to Bob.
3. (a) If $c^A = 0, c^B = 0$, Alice and Bob perform Protocol 4 henceforth.
 (b) If $c^A = 0, c^B = 1$, Bob picks uniformly random $a^B, b^B \in \{0, 1, 2\}$, enters b^B into his own box, and sends a^B to Alice.
 (c) If $c^A = 1$, Alice receives y^A from Bob, has her output x^A from her own box, and checks if they satisfy $x_{b^A}^A = y_{a^A}^A$. If not, she aborts.
4. If $c^A = 0, c^B = 1$, Bob receives x^B from Alice, has his own output y^B , and checks if they satisfy $x_{b^B}^B = y_{a^B}^B$. If not, he aborts.
5. (a) If $c^A = 1$ and Alice has not aborted, Alice and Bob perform Protocol 1 henceforth.
 (b) If $c^A = 0, c^B = 1$ and Bob has not aborted, Alice and Bob perform Protocol 2 henceforth.

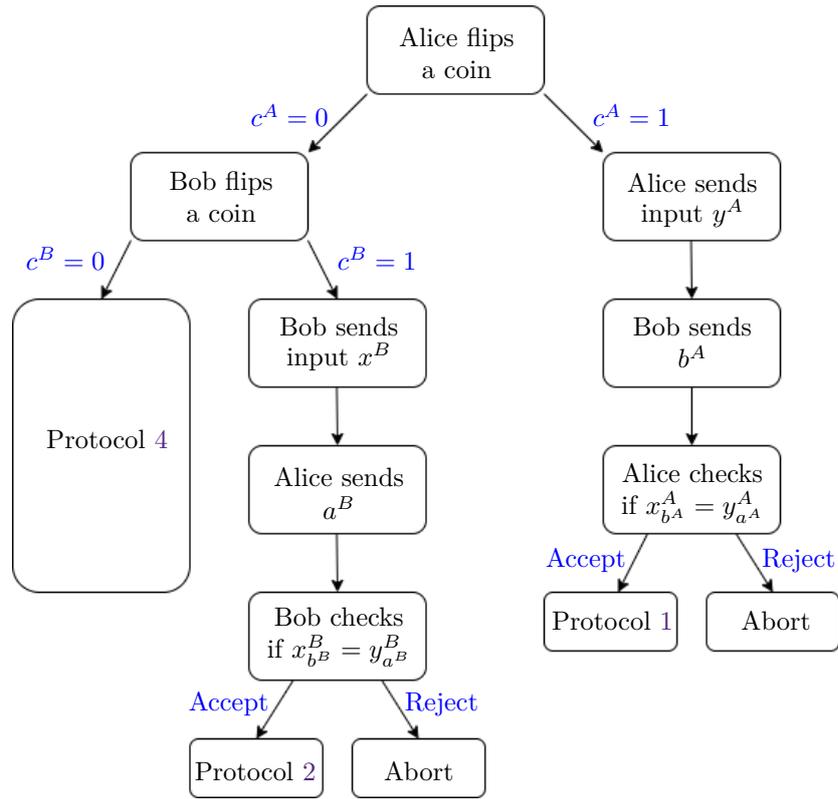


Figure 3: Flowchart for Protocol 5.

We give two soundness arguments for Protocol 5. The first consists of explicit numerical bounds on the cheating probabilities, based on the family of SDPs known as the Navascués-Pironio-Acín (NPA) hierarchy [NPA08]. We state the results as Theorem 3 below, and give the proof in Section 4. The second is an analytic proof that the cheating probabilities are bounded away from 1, based on the robust self-testing bounds for the magic square game [WBMS16, CN16]. We state this result formally as Theorem 4 below, and give the proof in Section 5.

Note that the NPA hierarchy works with commuting measurement operators rather than a tensor product structure, hence it might be possible that the first proof approach would work with the weaker assumption of commuting measurements instead. However, there is a technical issue that we begin our proofs with a reduction to projective measurements (see Appendix C), which we have not generalized to the commuting measurements case.

Theorem 3. *Upper bounds on the cheating probabilities for Protocol 5 (the fully device-independent scenario) with $q^A = 0.6$, $q^B = 0.6$ are given below, rounded to 5 decimal places.*

Upper bounds	P_A^{XOT}	P_B^{XOT}
Fully Device-Independent	0.96440	0.99204

Remark 5. *The choices for q^A and q^B in Theorem 3 were made by computing the bounds for different choices of q^A and q^B in intervals of 0.1, then simply taking the value that yields the best bounds on the cheating probabilities. We note that the result obtained for P_B^{XOT} is rather close to 1; however, the significant figures shown here are within the tolerance levels of the solver.*

Theorem 4. *For any $q^A, q^B > 0$ in Protocol 5, there exists some $\delta > 0$ such that $P_A^{\text{XOT}}, P_B^{\text{XOT}} \leq 1 - \delta$.*

1.5 Our security analysis approach

To analyze the security of the protocols for which perfect cheating is not possible, we require a way to calculate or upper bound the optimal cheating probabilities. For most of the bounds in this paper, we use the formalism of semidefinite programming to calculate optimal cheating probabilities. In the device-dependent case, i.e., in the proofs of Theorems 1 and 2, our approach is similar to the SDP-based analysis of coin-flipping in Kitaev [Kit02] and general protocols in Gutoski and Watrous [GW07].

A semidefinite program (SDP) is an optimization problem of the form

$$\begin{aligned} \text{maximize : } & \text{Tr}(AX) \\ \text{subject to : } & \Phi(X) = B \\ & X \in \text{Pos}(\mathcal{X}) \end{aligned}$$

where \mathcal{X} and \mathcal{Y} are complex Euclidean spaces, $\Phi : \text{Herm}(\mathcal{X}) \rightarrow \text{Herm}(\mathcal{Y})$ is a linear, Hermiticity-preserving transformation, and $C \in \text{Herm}(\mathcal{X})$ and $B \in \text{Herm}(\mathcal{Y})$ are Hermitian. When the spaces are clear from context, we write $X \succeq Y$ to mean that $X - Y$ is (Hermitian) positive semidefinite, noting that the special case $X \succeq 0$ simply means X is positive semidefinite. We use $X \succ Y$ to mean that $X - Y$ is positive definite.

The *dual* of the above optimization problem (called the *primal* in this context) is the problem

$$\begin{aligned} \text{minimize: } & \text{Tr}(BY) \\ \text{subject to: } & \Phi^*(Y) \succeq A \\ & Y \in \text{Herm}(\mathcal{Y}). \end{aligned}$$

Under mild conditions, for example that there exists an $X \succ 0$ that is primal feasible and a Y that is dual feasible, the optimal values of the primal and dual problems are equal.

In the device-independent case, the proof of Theorem 3 is via the NPA hierarchy, which is an infinite hierarchy of SDPs (see Appendix A). The SDP corresponding to any finite “level” of the NPA hierarchy gives an upper bound on the cheating probabilities in Theorem 3. Note however that the NPA hierarchy is inherently an optimization over all possible states *and* measurements, and thus is only suitable to be applied to device-independent protocols (where additional test steps are included to certify the state and/or measurements). Indeed, if we were to attempt to use the NPA hierarchy to bound the cheating probabilities of Protocols 3 and 4, we would get the trivial value of 1. This is why we set up specialized (and finite) SDPs for Theorems 1 and 2 instead.⁴

Finally, although our cheating probabilities are obtained by numerically solving SDPs, we note the following points:

- First, since each value is computed as an SDP, the dual SDPs yield certified upper bounds on the cheating probabilities. (The primal and dual values of all SDPs we solved are identical to more significant figures than displayed in our theorem statements.) Should there be concerns about floating-point errors, one could in principle find rational approximations to the dual solutions and thus obtain a bound certified by exact arithmetic, but this process is tedious and will not be included in this work.
- Second, we provide the code used (see below) so the SDP implementation may be verified and/or applied for any protocol modifications of interest.
- Third, the “punchline” of this work is that there exists a fully device-independent protocol where Alice and Bob’s cheating probabilities are bounded away from 1. We show this theoretically and also provide the numerical upper bounds to give an idea of what the cheating probabilities may look like.

Computational platform

The optimal value of most semidefinite programs can be approximated to within any constant precision efficiently. In particular, our computations were performed using the MATLAB packages QETLAB [Joh16] and YALMIP [Löf04] with solver MOSEK [MOS19]. Some of the calculations reported here were performed using the Euler cluster at ETH Zürich. The code used to compute the SDPs will be maintained at

<https://github.com/ernesttyz/dixot>.

⁴Strictly speaking, although Protocol 4 is used as an intermediate protocol to construct Protocol 5, our proof of Theorem 3 via the NPA hierarchy does not require Theorem 2. However, we designed Protocol 5 after making sure that the device-dependent component of it is secure, and thus Theorem 2 is a useful intermediate step: the analytical proof of Theorem 4, which does require Theorem 2, reflects this.

1.6 Paper organization

The next section details the magic square game and a rigidity result which is needed for this work. In Section 3, we use semidefinite programming to bound the cheating probabilities of Protocols 3 and 4. The security of our device-independent protocol is analyzed numerically in Section 4, and we refer the reader to Appendix A for background on the NPA hierarchy which we use in the analysis. We conclude in Section 5 with the analytical bounds on the device-independent protocol.

2 The magic square game strategy and a rigidity lemma

In this section, we discuss the optimal magic square game strategy and present a rigidity result required for this work.

The optimal quantum strategy for magic square can be described as follows. Alice and Bob share the state

$$|\Psi^{\text{MS}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{X}_0\mathcal{Y}_0} + |11\rangle_{\mathcal{X}_0\mathcal{Y}_0}) \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{X}_1\mathcal{Y}_1} + |11\rangle_{\mathcal{X}_1\mathcal{Y}_1}) \quad (7)$$

with Alice holding the registers $\mathcal{X}_0\mathcal{X}_1$, and Bob holding the registers $\mathcal{Y}_0\mathcal{Y}_1$. The measurements of Alice and Bob are given in Table 1.

$a \backslash b$	0	1	2
0	$\Pi_{00}^0 = 0\rangle\langle 0 \otimes \mathbb{1}$ $\Pi_{00}^1 = 1\rangle\langle 1 \otimes \mathbb{1}$	$\Pi_{01}^0 = \mathbb{1} \otimes 0\rangle\langle 0 $ $\Pi_{01}^1 = \mathbb{1} \otimes 1\rangle\langle 1 $	$\Pi_{02}^0 = 0\rangle\langle 0 \otimes 0\rangle\langle 0 $ $\quad + 1\rangle\langle 1 \otimes 1\rangle\langle 1 $ $\Pi_{02}^1 = 0\rangle\langle 0 \otimes 1\rangle\langle 1 $ $\quad + 1\rangle\langle 1 \otimes 0\rangle\langle 0 $
1	$\Pi_{10}^0 = \mathbb{1} \otimes +\rangle\langle + $ $\Pi_{10}^1 = \mathbb{1} \otimes -\rangle\langle - $	$\Pi_{11}^0 = +\rangle\langle + \otimes \mathbb{1}$ $\Pi_{11}^1 = -\rangle\langle - \otimes \mathbb{1}$	$\Pi_{12}^0 = +\rangle\langle + \otimes +\rangle\langle + $ $\quad + -\rangle\langle - \otimes -\rangle\langle - $ $\Pi_{12}^1 = +\rangle\langle + \otimes -\rangle\langle - $ $\quad + -\rangle\langle - \otimes +\rangle\langle + $
2	$\Pi_{20}^0 = 1\rangle\langle 1 \otimes +\rangle\langle + $ $\quad + 0\rangle\langle 0 \otimes -\rangle\langle - $ $\Pi_{20}^1 = 0\rangle\langle 0 \otimes +\rangle\langle + $ $\quad + 1\rangle\langle 1 \otimes -\rangle\langle - $	$\Pi_{21}^0 = +\rangle\langle + \otimes 1\rangle\langle 1 $ $\quad + -\rangle\langle - \otimes 0\rangle\langle 0 $ $\Pi_{21}^1 = +\rangle\langle + \otimes 0\rangle\langle 0 $ $\quad + -\rangle\langle - \otimes 1\rangle\langle 1 $	$\Pi_{22}^0 = +i\rangle\langle +i \otimes +i\rangle\langle +i $ $\quad + -i\rangle\langle -i \otimes -i\rangle\langle -i $ $\Pi_{22}^1 = +i\rangle\langle +i \otimes -i\rangle\langle -i $ $\quad + -i\rangle\langle -i \otimes +i\rangle\langle +i $

Table 1: Possible measurements for either party in the quantum strategy for magic square.

On input a , Alice simultaneously performs the three 2-outcome measurements $\{(\Pi_{ab}^0, \Pi_{ab}^1)\}_b$ in the row indexed by a in Table 1 (it can be checked that the three measurements in every row are compatible, so they can be performed simultaneously) on her registers $\mathcal{X}_0\mathcal{X}_1$. Her output (x_0, x_1, x_2) is the output of the three measurements (in order). Similarly, on input b , Bob simultaneously performs the three 2-outcome measurements $\{(\Pi_{ab}^0, \Pi_{ab}^1)\}_a$ in the column indexed by b

(the three measurements in every column are also compatible) on his registers $\mathcal{Y}_0\mathcal{Y}_1$, and gives the outcomes of the three measurements as his output (y_0, y_1, y_2) .

Clearly, the measurement Alice performs to output x_b is the same as the measurement Bob performs to output y_a . Since these measurements are performed on maximally entangled states, one can show Alice and Bob always get the same outcome for x_b and y_a . Also, it can be verified that these measurements always produce outcomes satisfying the parity conditions $x_0 \oplus x_1 \oplus x_2 = 0$ and $y_0 \oplus y_1 \oplus y_2 = 1$ (this holds regardless of the state). It can be shown that the output distribution is uniform over all combinations that win the magic square game, i.e. $\Pr(xy|ab) = 1/8$ if $x_b = y_a$ (and x, y satisfy the parity conditions), and $\Pr(xy|ab) = 0$ otherwise.

The above description views Alice and Bob as performing 8-outcome measurements (via a sequence of three 2-outcome measurements). However, since for *any* state the measurements always produce outputs satisfying the parity conditions, we can equivalently suppose Alice and Bob measure to determine only (x_0, x_1) and (y_0, y_1) , with the last bit for each determined by the parity conditions. (This is consistent with the way we defined the magic square game earlier.) These are 4-outcome measurements that can be expressed in terms of the Π operators from Table 1 as

$$M_{x_0x_1|a}^{\text{MS}} = \Pi_{a0}^{x_0} \Pi_{a1}^{x_1} \quad N_{y_0y_1|b}^{\text{MS}} = \Pi_{0b}^{y_0} \Pi_{1b}^{y_1}. \quad (8)$$

It can be checked that each $M_{x_0x_1|a}^{\text{MS}}$ and $N_{y_0y_1|b}^{\text{MS}}$ is a rank-1 projector. Since the measurements for x_0 and x_1 (resp. y_0 and y_1) commute for every a (resp. b), the product of the Π operators in each case can be taken in either order.

Certain nonlocal games exhibit the property that the quantum strategies achieving their optimal values are essentially unique. That is, if a quantum strategy wins with probability within ε of the optimal probability, that strategy must be $\delta(\varepsilon)$ -close to the ideal strategy for the game, up to certain local operations. This property of rigidity or self-testing was described first in [MY98], and has been shown for a variety of nonlocal games since.

[WBMS16] originally gave a proof of the rigidity of a version of the magic square game which is slightly different from ours. [CN16] showed that the rigidity statement also holds for the version of the magic square game we use. However, both of these results show the self-testing of some operators that are related to Alice and Bob's measurement operators in the magic square game, but not the measurement operators themselves. It is not immediately clear how to self-test the measurement operators themselves from their results. In Appendix B we derive the following lemma for self-testing of the measurement operators of the magic square strategy.

Lemma 5. *Consider any state $|\rho\rangle$ on registers $\mathcal{X}\mathcal{Y}$ and projective measurements $M_{x|a}, N_{y|b}$ such that $M_{x|a}$ acts only on \mathcal{X} and $N_{y|b}$ acts only on \mathcal{Y} . If this state and measurements win the magic square game with probability $1 - \varepsilon$, then there exist local isometries $V_A : \mathcal{X} \rightarrow \mathcal{X}_0\mathcal{X}_1\mathcal{J}_A$ and $V_B : \mathcal{Y} \rightarrow \mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B$ and a state $|\text{junk}\rangle$ on $\mathcal{J}_A\mathcal{J}_B$ such that for all a, b, x, y , we have*

$$\begin{aligned} & \left\| (V_A \otimes V_B) |\rho\rangle - |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2 \leq O(\varepsilon^{1/4}), \\ & \left\| (V_A \otimes V_B)(M_{x|a} \otimes \mathbb{1}) |\rho\rangle - ((M_{x|a}^{\text{MS}} \otimes \mathbb{1}) |\Psi^{\text{MS}}\rangle) \otimes |\text{junk}\rangle \right\|_2 \leq O(\varepsilon^{1/4}), \\ & \left\| (V_A \otimes V_B)(\mathbb{1} \otimes N_{y|b}) |\rho\rangle - ((\mathbb{1} \otimes N_{y|b}^{\text{MS}}) |\Psi^{\text{MS}}\rangle) \otimes |\text{junk}\rangle \right\|_2 \leq O(\varepsilon^{1/4}), \end{aligned}$$

where $|\Psi^{\text{MS}}\rangle$, $M_{x|a}^{\text{MS}}$, and $N_{y|b}^{\text{MS}}$ denote the ideal state and measurements in the magic square game, as described above.

3 On the security of Protocol 3 and Protocol 4

In this section we formulate the cheating probabilities as SDPs and solve them numerically to get their values.

3.1 Security analysis of Protocol 3

In this section, we prove that when the devices are trusted in Protocol 3, then $P_A^{\text{XOT}} = 1/2$ and $P_B^{\text{XOT}} = 3/4$. Before continuing, recall that Protocol 3 is an adaptation of the protocol in [CKS13] where Alice's actions are the exact same and so are the intentions of a dishonest Bob. Therefore, we can import $P_B^{\text{XOT}} = 3/4$ directly from the security analysis of that protocol.

The rest of this subsection is devoted to proving $P_A^{\text{XOT}} = 1/2$. Since Bob never aborts, all we need to ascertain is the ability for Alice to learn b from her information contained in the first message. To do this, she must infer b from the ensemble

$$\left\{ \left(\frac{1}{3}, \rho_b = \text{Tr}_Y(|\psi_b^+\rangle\langle\psi_b^+|) \right) : b \in \{0, 1, 2\} \right\}. \quad (9)$$

This is known as the *quantum state discrimination problem*, and the optimal guessing probability can be written as the following SDP:

Primal problem	Dual problem
maximize: $\frac{1}{3} \sum_{b \in \{0,1,2\}} \text{Tr}(E_b \rho_b)$	minimize: $\text{Tr}(\sigma)$
subject to: $\sum_{b \in \{0,1,2\}} E_b = \mathbb{1}_{\mathcal{X}}$	subject to: $\forall b \frac{1}{3} \rho_b \preceq \sigma$
$\forall b E_b \in \text{Pos}(\mathcal{X})$	$\sigma \in \text{Herm}(\mathcal{X})$.

Note that the success probability can be seen to be given by this SDP as it is a maximization over POVMs and the objective function is the probability of that POVM measurement producing the correct guess for b .

Now, if Alice uses the POVM

$$\{E_0, E_1, E_2\} = \{|0\rangle\langle 0| + |2\rangle\langle 2|, |1\rangle\langle 1|, 0\}, \quad (10)$$

we can see that

$$P_A^{\text{XOT}} \geq \frac{1}{3} \sum_{b \in \{0,1,2\}} \text{Tr}(E_b \rho_b) = \frac{1}{3} + \frac{1}{3} \cdot \frac{1}{2} + 0 = \frac{1}{2}. \quad (11)$$

Effectively what this measurement does is measure in the computational basis, then assign the outcomes $|0\rangle$ and $|2\rangle$ to the guess $b = 0$ and the outcome $|1\rangle$ to the guess $b = 1$. Note that $b = 2$ is never guessed in this strategy. All that remains to show is that $P_A^{\text{XOT}} \leq 1/2$. For this, we use the dual problem. Consider the dual feasible solution

$$\sigma = \frac{1}{6} \mathbb{1}_{\mathcal{X}}. \quad (12)$$

It can be checked that σ satisfies the dual constraints, i.e., $\sigma \succeq \frac{1}{3} \rho_b$ for all $b \in \{0, 1, 2\}$. Since $\text{Tr}(\sigma) = 1/2$, we have that $P_A^{\text{XOT}} \leq 1/2$ by weak duality.

3.2 Security analysis of Protocol 4

We split this section up into the four cases, depending on whether or not the state is trusted at the beginning, and each cheating party. The cheating probabilities in Theorem 2 are obtained by solving the SDPs obtained in each case.

Cheating strategy formulation set-up. Recall that Alice and Bob’s ideal measurement operators in the magic square game are denoted by $M_{x_0x_1|a}^{\text{MS}}$ and $N_{y_0y_1|b}^{\text{MS}}$. The measurement corresponding to a may be performed by applying a unitary that takes the $\{M_{x_0x_1|a}^{\text{MS}}\}_{x_0x_1}$ basis to the computational basis, and then measuring in the computational basis. We denote this unitary by U_a for each input a to Alice. Similarly, the measurement corresponding to b can be performed by applying U_b and then measuring in the computational basis.

3.2.1 Untrusted state, cheating Bob

In Protocol 4, Bob cheats successfully if he is able to output (x_0, x_1) at the end of the protocol and Alice does not abort in step 5. The steps of Protocol 4 that are relevant for determining whether Bob cheats successfully can then be described as follows:

1. Alice holds a state on two qubit registers $\mathcal{X}_0\mathcal{X}_1$.
2. Bob sends two qubit registers $\mathcal{Y}_0\mathcal{Y}_1$ to Alice (encoding his claimed outcomes (y_0, y_1)).
3. Alice prepares the state

$$|\phi_3\rangle_{\mathcal{A}\mathcal{A}'} = \frac{1}{\sqrt{3}}(|00\rangle_{\mathcal{A}\mathcal{A}'} + |11\rangle_{\mathcal{A}\mathcal{A}'} + |22\rangle_{\mathcal{A}\mathcal{A}'}), \quad (13)$$

and sends \mathcal{A}' to Bob.

4. Bob produces a guess g_B for (x_0, x_1) in the two-qubit register \mathcal{G}_B .
5. The event of Bob cheating successfully is now determined by a joint measurement on the registers $\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B$ (see Eq. (18) below).

We remark that in the actual protocol, the registers $\mathcal{A}\mathcal{A}'\mathcal{Y}_0\mathcal{Y}_1\mathcal{G}_B$ are classical, but in the above description we have treated them as quantum. The cheating probability is unaffected by this change, because of the following observation: in principle, the classicality condition could be enforced by applying a pinching channel in the computational basis immediately after each of those registers is generated. Since no further operations are performed on these registers before the final measurement in step 5,⁵ we can defer these pinching channels to the point just before that measurement is performed. However, that measurement (Eq. (18)) is diagonal in the computational basis of the registers $\mathcal{A}\mathcal{Y}_0\mathcal{Y}_1\mathcal{G}_B$, thus its outcome probabilities remain invariant regardless of whether those pinching channels were explicitly implemented beforehand. Hence those channels can be omitted entirely without changing the cheating probability.

⁵Strictly speaking, this is not true for \mathcal{A}' , which Bob could operate on. Fortunately, the classicality condition for \mathcal{A}' can be enforced by applying a pinching channel to \mathcal{A} alone in the state (13), without acting on \mathcal{A}' . This pinching channel on \mathcal{A} can indeed be deferred as desired.

Let ρ_1 and ρ_2 be Alice's states at the end of steps 2 and 4 respectively in the above description. These states are on registers $\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1$ and $\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B$ respectively. Since Alice does not perform any operations on the registers she holds between these steps, we must have

$$\text{Tr}_{\mathcal{G}_B}(\rho_2) = \text{Tr}_{\mathcal{A}'}(\rho_1 \otimes |\phi_3\rangle\langle\phi_3|) = \rho_1 \otimes \frac{\mathbb{1}_{\mathcal{A}}}{3}. \quad (14)$$

The measurement in step 5 can be described as follows. First, Alice performs a controlled unitary on registers $\mathcal{A}\mathcal{X}_0\mathcal{X}_1$ given by

$$U_{\mathcal{A}\mathcal{X}_0\mathcal{X}_1} = \sum_{a \in \{0,1,2\}} |a\rangle\langle a|_{\mathcal{A}} \otimes (U_a)_{\mathcal{X}_0\mathcal{X}_1}. \quad (15)$$

A computational-basis measurement is then performed on $\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B$ to determine whether Bob cheats successfully. Letting $P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}}$ denote the projector

$$\begin{aligned} P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}} = & |10\rangle\langle 10|_{\mathcal{Y}_0\mathcal{Y}_1} \otimes |0\rangle\langle 0|_{\mathcal{A}} + |01\rangle\langle 01|_{\mathcal{Y}_0\mathcal{Y}_1} \otimes |1\rangle\langle 1|_{\mathcal{A}} \\ & + |00\rangle\langle 00|_{\mathcal{Y}_0\mathcal{Y}_1} \otimes |2\rangle\langle 2|_{\mathcal{A}} + |11\rangle\langle 11|_{\mathcal{Y}_0\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{A}}, \end{aligned} \quad (16)$$

the projector corresponding to Bob cheating successfully is $\mathbb{1} - E_{\text{rej}}$, where

$$\begin{aligned} E_{\text{rej}} = & |00\rangle\langle 00|_{\mathcal{X}_0\mathcal{X}_1} \otimes \left(P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}} \otimes \mathbb{1}_{\mathcal{G}_B} + (\mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}} - P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}}) \otimes \sum_{(x'_0, x'_1) \neq (0,0)} |x'_0 x'_1\rangle\langle x'_0 x'_1|_{\mathcal{G}_B} \right) \\ & + \sum_{\substack{(x_0, x_1) \neq (0,0) \\ (x'_0, x'_1) \neq (x_0, x_1)}} |x_0 x_1\rangle\langle x_0 x_1|_{\mathcal{X}_0\mathcal{X}_1} \otimes \mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}} \otimes |x'_0 x'_1\rangle\langle x'_0 x'_1|_{\mathcal{G}_B}. \end{aligned} \quad (17)$$

The first term in E_{rej} corresponds to Alice's outputs being $x_0 x_1 = 00$, in which case Bob may fail if he either fails to pass Alice's test correctly, or if his guess $x'_0 x'_1$ is not equal to $x_0 x_1$. The second term corresponds to Alice's output being anything other than 00, in which case Alice does not conduct a test, and Bob only fails if he fails to guess $x_0 x_1$ correctly. The projector $P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}}$ has a term for all the cases in which Bob fails Alice's test when $x_0 x_1 = 00$. For example, if $y_0 y_1 = 01$ (and correspondingly $y_2 = 1$), then the test fails if $a = 0$ in the \mathcal{A} register; if $y_0 y_1 = 11$ (and correspondingly $y_2 = 1$), then the test always fails, since none of them can be equal to any x_a . $\mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}} - P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}}$ then corresponds to Bob not failing the test, and this case he still fails overall when $x'_0 x'_1 \neq 00$, which is reflected in the operator on \mathcal{G}_B that $\mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}} - P_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{A}}$ is tensored with.

The cheating probability is thus given by $\text{Tr}((\mathbb{1} - E_{\text{rej}})U_{\mathcal{A}\mathcal{X}_0\mathcal{X}_1}\rho_2 U_{\mathcal{A}\mathcal{X}_0\mathcal{X}_1}^\dagger)$. To describe it using a single measurement, we can write this as $\text{Tr}(E'_{\text{acc}}\rho_2)$, where

$$E'_{\text{acc}} = U_{\mathcal{A}\mathcal{X}_0\mathcal{X}_1}^\dagger (\mathbb{1} - E_{\text{rej}}) U_{\mathcal{A}\mathcal{X}_0\mathcal{X}_1}. \quad (18)$$

Hence we conclude Bob's maximum cheating probability is bounded above by the following SDP:

<u>Primal problem</u>	<u>Dual problem</u>
maximize: $\text{Tr}(E'_{\text{acc}}\rho_2)$	minimize: η
subject to: $\text{Tr}_{\mathcal{G}_B}(\rho_2) = \rho_1 \otimes \frac{\mathbb{1}_{\mathcal{A}}}{3}$	subject to: $\frac{1}{3} \text{Tr}_{\mathcal{A}}(Q) \preceq \eta \mathbb{1}_{\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1}$
$\text{Tr}(\rho_1) = 1$	$E'_{\text{acc}} \preceq Q \otimes \mathbb{1}_{\mathcal{G}_B}$
$\rho_1 \in \text{Pos}(\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1)$	$\eta \in \mathbb{R}$
$\rho_2 \in \text{Pos}(\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B)$	$Q \in \text{Herm}(\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1)$.

For the purposes of numerically solving the primal, one can enforce that the registers $\mathcal{A}\mathcal{Y}_0\mathcal{Y}_1\mathcal{G}_B$ are classical (by applying pinching channels in the computational basis), since the objective function and constraints are unaffected by applying such a channel to ρ_1, ρ_2 . This allows dramatically faster solving of the SDP, since it eliminates many variables. In addition, the optimization variables can be assumed to have real-valued entries, since the constraints and objective function are described by real-valued coefficients.

Solving the SDP numerically yields a value of 0.94096.

To show that this bound is tight, we shall argue that every feasible solution to the (primal) SDP corresponds to an attack Bob can physically perform. Consider any feasible states ρ_1, ρ_2 in the SDP, and let $|\rho_1\rangle_{\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{R}}, |\rho_2\rangle_{\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B\mathcal{R}'}$ be any purifications of these states onto some registers $\mathcal{R}, \mathcal{R}'$ respectively. The main constraint in the SDP implies that

$$\mathrm{Tr}_{\mathcal{G}_B\mathcal{R}'}(|\rho_2\rangle\langle\rho_2|) = \mathrm{Tr}_{\mathcal{A}'\mathcal{R}}(|\rho_1\rangle\langle\rho_1| \otimes |\phi_3\rangle\langle\phi_3|). \quad (19)$$

By Uhlmann's theorem, this implies (expanding the dimension of \mathcal{R}' if necessary) there exists an isometry $V : \mathcal{A}'\mathcal{R} \rightarrow \mathcal{G}_B\mathcal{R}'$ that sends $|\rho_1\rangle_{\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{R}} \otimes |\phi_3\rangle_{\mathcal{A}\mathcal{A}'}$ to $|\rho_2\rangle_{\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B\mathcal{R}'}$. Bob can hence implement the following attack: in the initial steps, Bob prepares the state $|\rho_1\rangle_{\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{R}}$ and keeps the purification \mathcal{R} . Then after receiving \mathcal{A}' from Alice, he implements the isometry V on $\mathcal{A}'\mathcal{R}$ to produce $\mathcal{G}_B\mathcal{R}'$. Discarding the purification \mathcal{R}' , this produces the feasible state ρ_2 in the SDP, achieving the desired cheating probability. (To be precise, one should again incorporate appropriate pinching channels to fulfill the classicality requirements for a physical attack, but as argued above, these channels can indeed be implemented without changing the cheating probability.)

3.2.2 Trusted state, cheating Bob

The fact that the state is trusted implies an extra constraint on ρ_1 , namely $\mathrm{Tr}_{\mathcal{Y}_0\mathcal{Y}_1}(\rho_1) = \frac{\mathbb{1}_{\mathcal{X}_0\mathcal{X}_1}}{4}$. Note that this automatically takes care of the $\mathrm{Tr}(\rho_1) = 1$ constraint. The rest of the argument applies in exactly the same way, so Bob's cheating probability in this case is bounded by the following SDP:

<u>Primal problem</u>	<u>Dual problem</u>
maximize: $\mathrm{Tr}(E'_{\mathrm{acc}}\rho_2)$	minimize: $\frac{1}{4} \mathrm{Tr}(Q_2)$
subject to: $\mathrm{Tr}_{\mathcal{G}_B}(\rho_2) = \rho_1 \otimes \frac{\mathbb{1}_{\mathcal{A}}}{3}$	subject to: $\frac{1}{3} \mathrm{Tr}_{\mathcal{A}}(Q_1) \preceq Q_2 \otimes \mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1}$
$\mathrm{Tr}_{\mathcal{Y}_0\mathcal{Y}_1}(\rho_1) = \frac{\mathbb{1}_{\mathcal{X}_0\mathcal{X}_1}}{4}$	$E'_{\mathrm{acc}} \preceq Q_1 \otimes \mathbb{1}_{\mathcal{G}_B}$
$\rho_1 \in \mathrm{Pos}(\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1)$	$Q_2 \in \mathrm{Herm}(\mathcal{X}_0\mathcal{X}_1)$
$\rho_2 \in \mathrm{Pos}(\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1\mathcal{G}_B)$	$Q_1 \in \mathrm{Herm}(\mathcal{A}\mathcal{X}_0\mathcal{Y}_0\mathcal{X}_1\mathcal{Y}_1)$.

Solving this SDP numerically yields a value of 0.93628. This value is a bit smaller than the case when the state is untrusted, as should be expected.

To see that this bound is tight, we follow the same argument as before, together with the fact that the new constraint completely captures the fact that the whole initial state is trusted (not just Alice's side). This is because the initial state is pure, and Bob is allowed to apply arbitrary operations on his side. This lets him produce any extension of Alice's side of the state, hence there is no loss of tightness by only imposing a constraint on Alice's side.

3.2.3 Untrusted state, cheating Alice

In this section, for brevity we will use \mathcal{Y} to denote the registers $\mathcal{Y}_0\mathcal{Y}_1$ together, and label it using a single index $y = (y_0, y_1)$. Alice sends some state in register \mathcal{Y} (possibly while retaining a purification of the state in a register \mathcal{Y}') to Bob, who carries out the measurement $\{N_{y|b}^{\text{MS}}\}_y$ on it, and sends the outcome y back to Alice in the computational basis of a register \mathcal{Z} .⁶ So honest Bob performs one of the three channels

$$\Phi_b(\sigma) = \sum_y \text{Tr}(N_{y|b}^{\text{MS}}\sigma) |y\rangle\langle y|_{\mathcal{Z}}, \quad (20)$$

each with probability $\frac{1}{3}$, and cheating Alice wants to learn which channel he has performed. In order to do this, Alice in general can start with a pure state $|\nu\rangle\langle\nu|$ in $\mathcal{Y}\mathcal{Y}'$ of which she sends register \mathcal{Y} to Bob, so the overall channel being performed on $|\nu\rangle\langle\nu|$ is $\Phi_b \otimes \mathbb{1}_{\mathcal{Y}'}$. Note that by considering the Schmidt decomposition, we can always assume \mathcal{Y}' has the same dimension as \mathcal{Y} (as long as we allow Alice to perform general POVMs later). After Bob has performed the channel, Alice can carry out a POVM measurement $\{E_b\}$ on $\mathcal{Z}\mathcal{Y}'$ to find out which channel was performed, with the POVM operator E_b corresponding to Alice guessing channel b . Conditioned on channel Φ_b being performed, the probability of Alice guessing b (i.e. being correct) is $\text{Tr}(E_b(\Phi_b \otimes \mathbb{1}_{\mathcal{Y}'}(|\nu\rangle\langle\nu|)))$. Hence Alice wants to maximize over pure states $|\nu\rangle\langle\nu|$ in $\mathcal{Y}\mathcal{Y}'$ and three-outcome measurements $\{E_b\}$ the following quantity:

$$\frac{1}{3} \sum_{b \in \{0,1,2\}} \text{Tr}(E_b(\Phi_b \otimes \mathbb{1}_{\mathcal{Y}'}(|\nu\rangle\langle\nu|))) \quad (21)$$

and the maximal value thereof is her maximum cheating probability.

We claim that the maximum cheating probability is given by the optimal value of the following primal-dual SDP pair, which is a slight generalization of the SDP for distance between channels due to [Wat09, GW07]:

Primal problem	Dual problem
maximize: $\frac{1}{3} \sum_{b \in \{0,1,2\}} \text{Tr}(Q_b J(\Phi_b))$	minimize: λ
subject to: $\sum_{b \in \{0,1,2\}} Q_b = \mathbb{1}_{\mathcal{Z}} \otimes \sigma$	subject to: $\text{Tr}_{\mathcal{Z}}(R) \preceq \lambda \mathbb{1}_{\mathcal{Y}'}$
$\text{Tr}(\sigma) = 1$	$\forall b \frac{1}{3} J(\Phi_b) \preceq R$
$\sigma \in \text{Pos}(\mathcal{Y}'), \forall b Q_b \in \text{Pos}(\mathcal{Z}\mathcal{Y}')$	$\lambda \in \mathbb{R}, R \in \text{Herm}(\mathcal{Z}\mathcal{Y}'),$

where $J(\Phi_b)$ is the Choi-Jamiołkowski matrix for Φ_b , which is in $\text{Herm}(\mathcal{Z}\mathcal{Y}')$ and given by

$$J(\Phi_b) = \Phi_b \otimes \mathbb{1}_{\mathcal{Y}'} (|\Omega\rangle\langle\Omega|) = \sum_y |y\rangle\langle y|_{\mathcal{Z}} \otimes N_{y|b}^{\text{MS}}, \quad (22)$$

where $|\Omega\rangle = \sum_y |yy\rangle_{\mathcal{Y}\mathcal{Y}'}$ is the (unnormalized) maximally entangled state between registers $\mathcal{Y}\mathcal{Y}'$, with respect to the computational basis of \mathcal{Y} .

⁶In previous sections, we used the registers $\mathcal{Y}_0\mathcal{Y}_1$ themselves to encode the outcome, but the subsequent proof is easier to follow with a new register storing the outcome.

To see that the optimization for Alice's discrimination probability is equivalent to the above SDP, note that Alice's initial state $|\nu\rangle_{\mathcal{Y}\mathcal{Y}'}$ can always be written in the form

$$|\nu\rangle_{\mathcal{Y}\mathcal{Y}'} = \sum_{y,y'} \nu_{yy'} |y\rangle_{\mathcal{Y}} |y'\rangle_{\mathcal{Y}'}, \quad (23)$$

for some coefficients $\nu_{yy'}$. Define the matrix $K_\nu \in L(\mathcal{Y}')$ as

$$K_\nu = \sum_{y,y'} \nu_{yy'} |y'\rangle\langle y|. \quad (24)$$

(This is the operator-vector isomorphism, up to a transpose.) It is easily verified by direct calculation that $|\nu\rangle = (\mathbb{1}_{\mathcal{Y}} \otimes K_\nu) |\Omega\rangle$, which implies

$$\Phi_b \otimes \mathbb{1}_{\mathcal{Y}'} (|\nu\rangle\langle\nu|) = (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu) J(\Phi_b) (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu^\dagger). \quad (25)$$

Therefore, the quantity Alice wants to maximize (Eq. (21)) can be written as

$$\sum_b \text{Tr}(E_b(\Phi_b \otimes \mathbb{1}_{\mathcal{Y}'} (|\nu\rangle\langle\nu|))) = \sum_b \text{Tr}\left((\mathbb{1}_{\mathcal{Z}} \otimes K_\nu^\dagger) E_b (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu) J(\Phi_b)\right). \quad (26)$$

Furthermore, note that Eq. (24) describes a bijective mapping between normalized initial states $|\nu\rangle$ and operators $K_\nu \in L(\mathcal{Y}')$ satisfying $\|K_\nu\|_2 = 1$. Hence Alice's optimal discrimination probability can be written as

$$\sup_{\{Q'_b\}_{b \in \mathcal{S}'}} \frac{1}{3} \sum_b \text{Tr}(Q'_b J(\Phi_b)), \quad (27)$$

where \mathcal{S}' is the set

$$\mathcal{S}' = \left\{ \{(\mathbb{1}_{\mathcal{Z}} \otimes K_\nu^\dagger) E_b (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu)\}_{b \in \{0,1,2\}} : E_b \in \text{Pos}(\mathcal{Z}\mathcal{Y}'), \sum_b E_b = \mathbb{1}_{\mathcal{Z}\mathcal{Y}'}, K_\nu \in L(\mathcal{Y}'), \|K_\nu\|_2 = 1 \right\}. \quad (28)$$

In comparison, the primal problem stated above is

$$\sup_{\{Q_b\}_{b \in \mathcal{S}}} \frac{1}{3} \sum_b \text{Tr}(Q_b J(\Phi_b)) \quad (29)$$

where \mathcal{S} is the set

$$\mathcal{S} = \left\{ \{Q_b\}_{b \in \{0,1,2\}} : Q_b \in \text{Pos}(\mathcal{Z}\mathcal{Y}'), \sum_b Q_b = \mathbb{1}_{\mathcal{Z}} \otimes \sigma, \sigma \in \text{Pos}(\mathcal{Y}'), \text{Tr}(\sigma) = 1 \right\}. \quad (30)$$

We shall show that \mathcal{S}' and \mathcal{S} are the same set (thus the optimizations are the same), by proving that every element of the former lies in the latter, and vice versa. First, every element of \mathcal{S}' is a tuple $\{(\mathbb{1}_{\mathcal{Z}} \otimes K_\nu^\dagger) E_b (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu)\}_{b \in \{0,1,2\}}$ defined by some E_b and K_ν satisfying the conditions in (28). It is easily verified that this tuple satisfies the conditions in (30), with

$$Q_b = (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu^\dagger) E_b (\mathbb{1}_{\mathcal{Z}} \otimes K_\nu), \quad \sigma = K_\nu^\dagger K_\nu, \quad (31)$$

and hence it lies in \mathcal{S} . As for the other direction, every element of \mathcal{S} is a tuple $\{Q_b\}_{b \in \{0,1,2\}}$ defined by some Q_b and σ satisfying the conditions in (30). It can be verified that this tuple is of a form satisfying the conditions in (28), with

$$E_b = (\mathbb{1}_{\mathcal{Z}} \otimes \sigma^{-1/2}) Q_b (\mathbb{1}_{\mathcal{Z}} \otimes \sigma^{-1/2}) + \frac{\mathbb{1}_{\mathcal{Z}} \otimes \Pi_\sigma^\perp}{3}, \quad K_\nu = \sigma^{1/2}, \quad (32)$$

where $\sigma^{-1/2}$ denotes the pseudoinverse of $\sigma^{1/2}$, and Π_σ^\perp denotes the projector onto the kernel of σ . Hence this tuple lies in \mathcal{S}' , as desired.

Solving the SDP numerically yields a value of 0.87268.

This bound is tight because the cheating probability is given by exactly the channel discrimination task we described, and the SDP (by construction) yields exactly the maximum discrimination probability.

3.2.4 Trusted state, cheating Alice

Since the initial state is trusted, this means Alice initially holds the $\mathcal{X}_0\mathcal{X}_1$ registers of the state $|\Psi^{\text{MS}}\rangle$, while Bob performs the measurement corresponding to input b on his registers $\mathcal{Y}_0\mathcal{Y}_1$, then receives an outcome which he sends to Alice by encoding it in the computational basis of a register \mathcal{Z} . The state Alice then holds is

$$\rho_b = \sum_{y_0 y_1} \text{Tr}_{\mathcal{Y}_0 \mathcal{Y}_1} ((\mathbb{1} \otimes N_{y_0 y_1 | b}^{\text{MS}}) |\Psi^{\text{MS}}\rangle\langle\Psi^{\text{MS}}| (\mathbb{1} \otimes N_{y_0 y_1 | b}^{\text{MS}})) \otimes |y_0 y_1\rangle\langle y_0 y_1|_{\mathcal{Z}}. \quad (33)$$

Alice has to distinguish these states (for the three possible values of b), and hence her cheating probability is given by the state discrimination SDP from Section 3.1:

Primal problem	Dual problem
maximize: $\frac{1}{3} \sum_{b \in \{0,1,2\}} \text{Tr}(E_b \rho_b)$	minimize: $\text{Tr}(\sigma)$
subject to: $\sum_{b \in \{0,1,2\}} E_b = \mathbb{1}_{\mathcal{X}_0 \mathcal{X}_1 \mathcal{Z}}$	subject to: $\forall b \frac{1}{3} \rho_b \preceq \sigma$
$\forall b E_b \in \text{Pos}(\mathcal{X}_0 \mathcal{X}_1 \mathcal{Z})$	$\sigma \in \text{Pos}(\mathcal{X}_0 \mathcal{X}_1 \mathcal{Z}).$

Solving the SDP numerically yields a value of 0.83333. This value is a bit smaller than the case when the state is untrusted, as should be expected.

Again, this bound is tight because the cheating probability is given by exactly the state discrimination task we described.

4 Numerically bounding the cheating probabilities for Protocol 5

In this section, we obtain expressions for Alice and Bob's cheating probabilities in Protocol 5, which can be optimized using the NPA hierarchy. Throughout the section we shall often omit some tensor factors of $\mathbb{1}$ for brevity (e.g. for an operator M on Alice's system and an operator N on Bob's system, MN implicitly means $(M \otimes \mathbb{1})(\mathbb{1} \otimes N)$).

Without loss of generality, we assume the state shared by the two parties is pure, by giving the dishonest party the purification of any mixed state. We shall also henceforth assume that all measurements are projective: in the case of cheating Alice, our analysis involves a standard Bell-nonlocality scenario, in which case it is a known result (see Appendix C for a brief discussion) that measurements can be assumed to be projective. For cheating Bob, however, some of the measurements are sequential and hence more care is needed, since it was found in [BMKG13] that

there exist sequential correlations that *cannot* be described by projective measurements. (It would be convenient if Protocol 4 did not involve Alice sending her input to Bob, thereby more closely resembling a standard nonlocal game. However, it would seem this step was necessary to allow an honest Bob to know which bit of his output he should use, as previously mentioned regarding Protocol 4.) We prove that the measurements can also be assumed to be projective in the case of cheating Bob in Lemma 10 in Appendix C.

Cheating Bob. Bob never calls for a test if he is dishonest, since if he does so then he must either abort or perform a protocol perfectly secure against him. Hence we can consider only two families of measurement choices that dishonest Bob may perform — one family that is used if Alice calls for a test, and one family that is used in the subroutine running Protocol 4. As noted previously, dishonest Bob may not be physically supplying the test input Alice provides to his box and reporting the corresponding output. However, it is still true that the process of him producing a reply b^A to Alice’s message y^A can be modelled as a measurement process described by some operators acting on his share of the state, and it is these operators that we will be calling $N_{y^A|b^A}^{\text{test}}$ in the proof. (An alternative perspective is that any operation dishonest Bob might perform on his share of the state might as well have been “encoded” in the box directly.) Still, we highlight that it is important here that y^A was chosen by honest Alice rather than self-reported by dishonest Bob — this ensures that it was indeed uniformly chosen.

Since Alice is honest, the possible measurements performed by her box are the same in both situations, although Bob could have preprogrammed what measurement is performed by Alice’s box for a given input. We have used a^A, b^A, x^A, y^A to denote the inputs and outputs when Alice runs the test; here we shall use a, b, x, y to denote the variables when the Protocol 4 subroutine is run.

Let Alice and Bob’s shared pure state be $|\rho\rangle$, and let $\rho = |\rho\rangle\langle\rho|$. Let Alice’s measurement operators on her system for input a and output x be denoted by $M_{x|a}$ and Bob’s test measurement operators on his system for input b^A and output y^A be denoted by $N_{y^A|b^A}^{\text{test}}$. The probability of outputs x^A, y^A on inputs a^A, b^A by Alice during the test is given by $\|M_{x^A|a^A} N_{y^A|b^A}^{\text{test}} |\rho\rangle\|_2 = \text{Tr}(M_{x^A|a^A} N_{y^A|b^A}^{\text{test}} \rho)$, since we assumed the measurements are projective. Bob’s cheating probability when Alice runs the test is just his probability of passing the test, since he can guess x perfectly if he passes the test. Since honest Alice picks the testing inputs a^A, b^A uniformly, Bob’s probability of passing the test is given by

$$P_B^{\text{test}} = \frac{1}{9} \sum_{a^A, b^A} \sum_{x^A, y^A: x_{b^A}^A = y_{a^A}^A} \text{Tr}(M_{x^A|a^A} N_{y^A|b^A}^{\text{test}} \rho). \quad (34)$$

Let Bob’s measurement operators when Alice does not run the test be denoted by N^{prot} . There are two kinds of measurement operators here — Bob performs a measurement with no input to generate the y that he sends to Alice in step 2 of the Protocol 4 subroutine; these measurement operators will be denoted by N_y^{prot} . The subnormalized shared state after Bob performs this measurement is given by $N_y^{\text{prot}} \rho N_y^{\text{prot}}$. After receiving Alice’s input a as a message from Alice, Bob performs another measurement to produce his guess g for Alice’s output x . Since the only information he learns from Alice is a , he uses this as his input and applies a measurement operator $N_{g|a}^{\text{prot}}$. The probability of Alice outputting x on input a and Bob outputting g on input a and sending y at the beginning is given by $\|M_{x|a} N_{g|a}^{\text{prot}} N_y^{\text{prot}} |\rho\rangle\|_2 = \text{Tr}(M_{x|a} N_{g|a}^{\text{prot}} N_y^{\text{prot}} \rho N_y^{\text{prot}})$. Alice picks

her input a uniformly at random and Bob cheats successfully in this case if y, a and x are compatible (in the Protocol 4 subroutine) and his guess satisfies $g = x$. Hence Bob's cheating probability is given by

$$P_B^{\text{prot}} = \frac{1}{3} \text{Tr} \left(M_{00|0} N_{00|0}^{\text{prot}} (N_{00}^{\text{prot}} \rho N_{00}^{\text{prot}} + N_{01}^{\text{prot}} \rho N_{01}^{\text{prot}}) + M_{00|1} N_{00|1}^{\text{prot}} (N_{00}^{\text{prot}} \rho N_{00}^{\text{prot}} + N_{10}^{\text{prot}} \rho N_{10}^{\text{prot}}) \right. \\ \left. + M_{00|2} N_{00|2}^{\text{prot}} (N_{01}^{\text{prot}} \rho N_{01}^{\text{prot}} + N_{10}^{\text{prot}} \rho N_{10}^{\text{prot}}) + \sum_a \sum_{x \neq 00} \sum_y M_{x|a} N_{x|a}^{\text{prot}} N_y^{\text{prot}} \rho N_y^{\text{prot}} \right). \quad (35)$$

Using the fact that $M_{x|a}$ and N_y^{prot} act on different systems, the terms in the above expression can be rewritten in the form $\text{Tr}(M_{x|a} N_y^{\text{prot}} N_{x|a}^{\text{prot}} N_y^{\text{prot}} \rho)$, which are terms in the NPA matrix. Bob's overall cheating probability is given by the maximum value (over all possible states and measurements as described above) of

$$q^A P_B^{\text{test}} + (1 - q^A) P_B^{\text{prot}}. \quad (36)$$

Cheating Alice. Here we similarly assume dishonest Alice has measurement operators M^{prot} that are applied in her box when the Protocol 4 subroutine is run, and measurement operators M^{test} that are applied when Bob calls for the test. Bob's measurement operators $N_{y|b}$ are the same throughout. As in Bob's case, Alice's cheating probability when Bob runs the test is given by

$$P_A^{\text{test}} = \frac{1}{9} \sum_{a^A, b^A} \sum_{x^A, y^A: x_{b^A}^A = y_{a^A}^A} \text{Tr}(M_{x^A|a^A}^{\text{test}} N_{y^A|b^A} \rho). \quad (37)$$

The only information Alice gets from Bob in the Protocol 4 subroutine is Bob's output y . She uses this to choose a measurement to perform on her state, which produces an output g that is her guess for Bob's input. This corresponds to a measurement operator $M_{g|y}^{\text{prot}}$, and the probability of Bob producing output y on input b and Alice producing output g on message y from Bob is given by $\text{Tr}(M_{g|y}^{\text{prot}} N_{y|b} \rho)$. Since honest Bob chooses his input b uniformly, and Alice cheats successfully if her guess satisfies $g = b$, her cheating probability in this case is given by

$$P_A^{\text{prot}} = \frac{1}{3} \sum_b \sum_y \text{Tr}(M_{b|y}^{\text{prot}} N_{y|b} \rho). \quad (38)$$

Alice's overall cheating probability is given by the maximum value of

$$q^B P_A^{\text{test}} + (1 - q^B) P_A^{\text{prot}}. \quad (39)$$

Using the NPA hierarchy. The bound on P_A^{XOT} in Theorem 3 was computed by using NPA local level 1 (see Appendix A) to optimize Eq. (39).⁷ For P_B^{XOT} , we need to optimize Eq. (36), and higher-order moments are required due to the sequential measurements. Hence we choose the index set O (see Appendix A) to be

$$O = (\{\mathbb{1}\} \cup \{M_{x|a}\}) \circ (\{\mathbb{1}\} \cup \{N_{y|b}^{\text{test}}\} \cup \{N_{g|m}^{\text{prot}}\} \cup \{N_y^{\text{prot}}\} \cup \{N_{g|m}^{\text{prot}} N_y^{\text{prot}}\}), \quad (40)$$

⁷In principle, it could have been simpler to compute a bound using only the no-signalling constraints, as was done in part of the security proof in [SCA⁺11]. However, here we encountered the issue that non-signalling strategies that perfectly win the magic square game are not unique, and can even produce deterministic outcomes for one input pair.

where \circ means all pairwise word concatenations between the two sets in order (and $\mathbb{1}$ is the empty word). However, this matrix is very large if measurement operators for all outcomes are included, and hence we omitted one projector per measurement by using the relation $\sum_x M_{x|a} = \sum_y N_{y|b} = \mathbb{1}$ to eliminate $M_{11|a}, N_{11|b}$ from the objective function. Omitting these terms from the index set O as well, its size is reduced to a more manageable $|O| = (1+9)(1+9+9+3+27) = 490$.

The results from solving these SDPs numerically are stated in Theorem 3.

5 Analytically bounding the cheating probabilities away from 1 for Protocol 5

We shall show the security proof for cheating Bob only (the proof for cheating Alice is analogous, though simpler because there are no sequential measurements by Alice). We start by first proving the following lemma, which formalizes the intuition that in order to show P_B^{XOT} is bounded away from 1 in Protocol 5, it would be sufficient to argue that if Bob passes Alice's test with high probability, then he cannot cheat perfectly in the "protocol branch".

Lemma 6. *Consider any $q^A \in (0, 1)$. Suppose there exists some $\varepsilon > 0$ such that the value of*

$$\begin{aligned} & \text{maximize: } P_B^{\text{prot}} \\ & \text{subject to: } P_B^{\text{test}} \geq 1 - \varepsilon \end{aligned}$$

is upper-bounded by $1 - \varepsilon/(1 - q^A)$, where $P_B^{\text{prot}}, P_B^{\text{test}}$ are defined as in Eqs. (34)–(35), and the supremum is taken over all states and measurements. Then for Protocol 5 performed with that choice of q^A , we have

$$P_B^{\text{XOT}} \leq 1 - q^A \varepsilon.$$

Proof. Suppose to the contrary that $P_B^{\text{XOT}} > 1 - q^A \varepsilon$. Then by Eq. (36), this must be achieved by Bob implementing a strategy such that

$$P_B^{\text{test}} > \frac{1 - q^A \varepsilon - (1 - q^A)P_B^{\text{prot}}}{q^A} \geq \frac{1 - q^A \varepsilon - (1 - q^A)(1)}{q^A} = 1 - \varepsilon. \quad (41)$$

By hypothesis, this implies that $P_B^{\text{prot}} \leq 1 - \varepsilon/(1 - q^A)$. But this would imply

$$P_B^{\text{XOT}} \leq q^A(1) + (1 - q^A) \left(1 - \frac{\varepsilon}{1 - q^A}\right) = 1 - \varepsilon < 1 - q^A \varepsilon, \quad (42)$$

contradicting the supposition that $P_B^{\text{XOT}} > 1 - q^A \varepsilon$. \square

We now use the rigidity properties of the magic square game to prove (for any fixed choice of q^A) there indeed exists some $\varepsilon > 0$ fulfilling the conditions of this lemma, and thus P_B^{XOT} is bounded by some constant strictly less than 1. To do so, we first note that our device-dependent arguments directly yield the following lemma, which we shall use later.

Lemma 7. *Let $|\Psi^{\text{MS}}\rangle$ and $M_{x|a}^{\text{MS}}$ be the ideal state and measurements (for Alice) in the magic square game. If Alice and Bob share a state of the form $|\rho\rangle = |\Psi^{\text{MS}}\rangle_{\mathcal{X}_0\mathcal{X}_1\mathcal{Y}_0\mathcal{Y}_1} \otimes |\text{junk}\rangle_{\mathcal{J}_A\mathcal{J}_B}$, and Alice's measurements on $\mathcal{X}_0\mathcal{X}_1\mathcal{J}_A$ are of the form $M_{x|a} = M_{x|a}^{\text{MS}} \otimes \mathbb{1}_{\mathcal{J}_A}$, then for any measurements $N_{g|m}^{\text{prot}}, N_y^{\text{prot}}$ by Bob on $\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B$, we have*

$$P_B^{\text{prot}} \leq 0.93628,$$

where P_B^{prot} is defined as in Eq. (35).

Proof. Since Alice’s measurements act as the identity on \mathcal{J}_A , we may as well suppose Bob holds that system. Recall that our device-dependent arguments allowed the cheating party to perform arbitrary operations on their state. In particular, cheating Bob could append an ancilla $|\text{junk}\rangle_{\mathcal{J}_A\mathcal{J}_B}$ and perform a joint measurement across this ancilla and his part of the state. Hence our bounds for the trusted-state-and-measurements scenario apply to the situation described here. \square

Consider an arbitrary $\varepsilon > 0$, and consider any cheating strategy for Bob in Protocol 5 that achieves $P_B^{\text{test}} \geq 1 - \varepsilon$. Then by Lemma 5, we have

$$\left\| (V_A M_{x|a} \otimes V_B) |\rho\rangle - ((M_{x|a}^{\text{MS}} \otimes \mathbb{1}) |\Psi^{\text{MS}}\rangle) \otimes |\text{junk}\rangle \right\|_2 \leq O(\varepsilon^{1/4}). \quad (43)$$

Before proceeding further, we give an informal overview of our subsequent argument. Qualitatively, Eq. (43) means the (subnormalized) true post-Alice-measurement states are close to the ideal post-Alice-measurement states of the magic square game, up to local isometries/ancillas. We shall hence argue that after Bob performs his true measurements $N_{g|m}^{\text{prot}}, N_y^{\text{prot}}$ on the true post-Alice-measurement states, the resulting states are close (up to local isometries/ancillas) to those that would result from Bob performing some other measurements $\tilde{N}_{g|m}^{\text{prot}}, \tilde{N}_y^{\text{prot}}$ on the ideal post-Alice-measurement states, upon which our desired result quickly follows by observing that the latter is precisely a situation where Lemma 7 applies. Roughly speaking, these measurements $\tilde{N}_{g|m}^{\text{prot}}, \tilde{N}_y^{\text{prot}}$ will be constructed from the true measurements $N_{g|m}^{\text{prot}}, N_y^{\text{prot}}$ by simply “inverting” the isometries mapping the true states to the ideal ones, giving us measurements that act on the ideal systems rather than the true ones. However, since isometries are not in general invertible, we shall need to account for some technical details while doing so.⁸

We now give the rigorous proof. As previously described, we take the input and output spaces of all the true measurement operators to be the same. In that case, we can define measurement operators $\tilde{N}_y^{\text{prot}}, \tilde{N}_{g|m}^{\text{prot}}$ on $\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B$ via

$$\tilde{N}_y^{\text{prot}} = V_B N_y^{\text{prot}} V_B^\dagger + \frac{\Pi_{V_B}}{2} \quad \text{and} \quad \tilde{N}_{g|m}^{\text{prot}} = V_B N_{g|m}^{\text{prot}} V_B^\dagger + \frac{\Pi_{V_B}}{2} \quad (44)$$

where $\Pi_{V_B} = \mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B} - V_B V_B^\dagger$. It is easy to verify that Π_{V_B} is a projector and satisfies $V_B^\dagger \Pi_{V_B} = 0$, $\Pi_{V_B} V_B = 0$. The operators $\tilde{N}_y^{\text{prot}}$ form a valid set of measurement operators on $\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B$, since

$$\tilde{N}_y^{\text{prot} \dagger} \tilde{N}_y^{\text{prot}} = \left(V_B N_y^{\text{prot} \dagger} V_B^\dagger + \frac{\Pi_{V_B}}{2} \right) \left(V_B N_y^{\text{prot}} V_B^\dagger + \frac{\Pi_{V_B}}{2} \right) = V_B N_y^{\text{prot} \dagger} N_y^{\text{prot}} V_B^\dagger + \frac{\Pi_{V_B}}{4}, \quad (45)$$

which implies they sum to the identity on $\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B$. Similarly, for each m , the operators $\tilde{N}_{g|m}^{\text{prot}}$ form a valid set of measurement operators.

The “sequential operators” $\tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}$ thus also form a valid set of measurement operators, i.e. we have $\sum_{gy} (\tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}})^\dagger \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}} = \mathbb{1}_{\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_B}$ (for all m). This implies that for any (not necessarily normalized) $|\nu\rangle \in \mathcal{X}_0\mathcal{X}_1\mathcal{Y}_0\mathcal{Y}_1\mathcal{J}_A\mathcal{J}_B$, we have $\left\| (\mathbb{1}_{\mathcal{X}_0\mathcal{X}_1\mathcal{J}_A} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}) |\nu\rangle \right\|_2 \leq \|\nu\|_2$. Additionally, we note that

$$\tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}} V_B = \left(V_B N_{g|m}^{\text{prot}} V_B^\dagger + \frac{\Pi_{V_B}}{2} \right) \left(V_B N_y^{\text{prot}} V_B^\dagger + \frac{\Pi_{V_B}}{2} \right) V_B = V_B N_{g|m}^{\text{prot}} N_y^{\text{prot}}. \quad (46)$$

⁸An alternate perspective that may be helpful is that an isometry simply defines an embedding of Hilbert spaces, i.e. we can choose bases such that $V|\phi\rangle = |\phi\rangle \oplus \mathbf{0}$ in explicit components. We can thus think of Eq. (43) as the statement $\left\| ((M_{x|a} \otimes \mathbb{1}) |\rho\rangle) \oplus \mathbf{0} - ((M_{x|a}^{\text{MS}} \otimes \mathbb{1}) |\Psi^{\text{MS}}\rangle) \otimes |\text{junk}\rangle \right\|_2 \leq O(\varepsilon^{1/4})$ in some choice of coordinates, in which case the subsequent construction is fairly intuitive.

Applying these properties to Eq. (43), followed by the reverse triangle inequality, we finally obtain the following (denoting $M_{x|a}^{\text{MS}} \otimes \mathbb{1}_{\mathcal{J}_A} = \tilde{M}_{x|a}^{\text{MS}}$):

$$\begin{aligned}
O(\varepsilon^{1/4}) &\geq \left\| (V_A M_{x|a} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}} V_B) |\rho\rangle - (\tilde{M}_{x|a}^{\text{MS}} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}) |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2 \\
&= \left\| (V_A M_{x|a} \otimes V_B N_{g|m}^{\text{prot}} N_y^{\text{prot}}) |\rho\rangle - (\tilde{M}_{x|a}^{\text{MS}} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}) |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2 \\
&\geq \left\| (V_A M_{x|a} \otimes V_B N_{g|m}^{\text{prot}} N_y^{\text{prot}}) |\rho\rangle \right\|_2 - \left\| (\tilde{M}_{x|a}^{\text{MS}} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}) |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2 \\
&= \left\| (M_{x|a} \otimes N_{g|m}^{\text{prot}} N_y^{\text{prot}}) |\rho\rangle \right\|_2 - \left\| (\tilde{M}_{x|a}^{\text{MS}} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}) |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2. \quad (47)
\end{aligned}$$

Recall that P_B^{prot} is a sum of terms of the form $\left\| (M_{x|a} \otimes N_{g|m}^{\text{prot}} N_y^{\text{prot}}) |\rho\rangle \right\|_2$. Let $\tilde{P}_B^{\text{prot}}$ be the value obtained by replacing these terms with $\left\| (\tilde{M}_{x|a}^{\text{MS}} \otimes \tilde{N}_{g|m}^{\text{prot}} \tilde{N}_y^{\text{prot}}) |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2$ instead. Since this is the sum of finitely many terms, Eq. (47) implies that $P_B^{\text{prot}} \leq \tilde{P}_B^{\text{prot}} + O(\varepsilon^{1/4})$. In addition, Lemma 7 implies that $\tilde{P}_B^{\text{prot}} \leq 0.93628$. Hence we conclude that by choosing sufficiently small $\varepsilon > 0$, we would have $P_B^{\text{prot}} \leq 0.93628 + O(\varepsilon^{1/4}) \leq 1 - \varepsilon/(1 - q^A)$, which satisfies the conditions of Lemma 6.

Remark 6. *In principle, this approach can yield analytical bounds on P_B^{XOT} by explicitly tracking the constants in the $O(\varepsilon^{1/4})$ bound. However, the results of [WBMS16] show that this $O(\varepsilon^{1/4})$ self-testing bound becomes trivial at very small values of ε (less than 10^{-4} , for our definition of ε). We found that if the optimization in Lemma 6 is solved numerically using the NPA hierarchy instead of using this analytical bound, the results appear much more robust — for instance, at $\varepsilon = 10^{-3}$ we still get a nontrivial bound of $P_B^{\text{prot}} \leq 0.97365$. Hence this indicates that the analytical approach here yields bounds that are quite far from tight. (Solving the analogous optimization for cheating Alice yields tighter bounds as compared to cheating Bob; e.g. $P_A^{\text{prot}} \leq 0.85855$ at $\varepsilon = 10^{-3}$ and $P_A^{\text{prot}} \leq 0.83590$ at $\varepsilon = 10^{-5}$.)*

6 Discussion

The protocol in this work is a somewhat “minimal” construction, in that it only involves a small number of rounds, and each check that Alice and/or Bob conducts appears critical for achieving any nontrivial bound on the cheating probabilities. However, a natural question to investigate in future work would be whether having more rounds of communication or larger entangled states could yield better protocols. For instance, our protocol yields different cheating probabilities for Alice and Bob, but it seems unclear whether it is simply due to the asymmetric nature of the task, or whether having further checks by each party could result in more symmetric bounds. As for trying to achieve better security by using more states, there are various self-testing results for devices playing many parallel instances of nonlocal games [McK16, McK17, CN16, Col17], although it is not immediately clear whether they are sufficiently robust to be converted into a protocol of this form. Another approach could be to design protocols based on sequential rounds of nonlocal games, such as in [AMPS16, KW16].

It may also be interesting to try converting the XOT protocol in this work into a protocol for OT, or other tasks such as bit commitment and coin flipping as mentioned in the introduction. As a starting point, it is fairly straightforward to design a conversion to OT that maintains perfect completeness (in the following, we use (x'_0, x'_1) to denote Alice’s final OT output and (b', y') to denote Bob’s):

Protocol 6 (Converting XOT to OT).

1. Alice and Bob perform an XOT protocol so that Alice has (x_0, x_1, x_2) and Bob has $(b, y = x_b)$.
2. Bob picks $c \in \{0, 1, 2\}$ uniformly at random such that $c \neq b$, and sends it to Alice.
3.
 - If $c = 0$, Alice outputs $(x'_0, x'_1) = (x_1, x_0 \oplus x_1)$, and Bob outputs $(b', y') = (b+2 \bmod 3, y)$.
 - If $c = 1$, Alice outputs $(x'_0, x'_1) = (x_0 \oplus x_1, x_0)$, and Bob outputs $(b', y') = (b+1 \bmod 3, y)$.
 - If $c = 2$, Alice outputs $(x'_0, x'_1) = (x_0, x_1)$, and Bob outputs $(b', y') = (b, y)$.

However, analyzing the soundness of the resulting OT protocol (using the protocol in this work to achieve the XOT part) would require further developing an appropriate SDP and/or self-testing analysis — it does not seem straightforward to directly apply the final cheating-probability bounds for our XOT protocol, as they do not impose particularly detailed constraints on the nature of the dishonest party’s side-information. We leave this for future work.

Acknowledgements

We thank Jean-Daniel Bancal, Andrea Coladangelo, Lidia del Rio, Honghao Fu, Anand Natarajan, Christopher Portmann, Xingyao Wu and Vilasini Venkatesh for helpful discussions. We also thank the reviewers for their feedback and suggestions for improvement.

Research at Perimeter Institute is supported in part by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Economic Development, Job Creation and Trade.

Research at the Institute for Quantum Computing is supported by Innovation, Science and Economic Development (ISED) Canada. S. K. and E. T. acknowledge support from the NSERC Canada Discovery Grants Program, and S. K. from Fujitsu Labs America.

Part of this work was done when S. K. was at the Centre for Quantum Technologies, National University of Singapore, Singapore (partially funded by the Singapore Ministry of Education and the National Research Foundation, Prime Minister’s Office, Singapore), and E. T. was at the Institute for Theoretical Physics, ETH Zürich, Switzerland (funded by the Swiss National Science Foundation via the National Center for Competence in Research for Quantum Science and Technology (QSIT), the Air Force Office of Scientific Research (AFOSR) via grant FA9550-19-1-0202, and the QuantERA project eDICT).

References

- [ACK⁺14] Nati Aharon, André Chailloux, Iordanis Kerenidis, Serge Massar, Stefano Pironio, and Jonathan Silman. [Weak coin flipping in a device-independent setting](#). In *Theory of Quantum Computation, Communication, and Cryptography*, pages 1–12, 2014.
- [AFDF⁺18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. [Practical device-independent quantum cryptography via entropy accumulation](#). *Nature Communications*, 9(1):459, 2018.

- [AMPS16] Nati Aharon, Serge Massar, Stefano Pironio, and Jonathan Silman. [Device-independent bit commitment based on the CHSH inequality](#). *New Journal of Physics*, 18(2):025014, 2016.
- [BMKG13] Costantino Budroni, Tobias Moroder, Matthias Kleinmann, and Otfried Gühne. [Bounding temporal quantum correlations](#). *Physical Review Letters*, 111:020403, 2013.
- [CGS16] André Chailloux, Gus Gutoski, and Jamie Sikora. [Optimal bounds for semi-honest quantum oblivious transfer](#). *Chicago Journal of Theoretical Computer Science*, 13:1–17, 2016.
- [CKS13] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. [Lower bounds for quantum oblivious transfer](#). *Quantum Information & Computation*, 13(1-2):158–177, 2013.
- [CN16] Matthew Coudron and Anand Natarajan. [The parallel-repeated Magic Square game is rigid](#). arXiv preprint, 2016.
- [Col17] Andrea Coladangelo. [Parallel self-testing of \(tilted\) EPR pairs via copies of \(tilted\) CHSH and the magic square game](#). *Quantum Information and Computation*, 17(9&10):831–865, 2017.
- [FM18] Honghao Fu and Carl A. Miller. [Local randomness: Examples and application](#). *Physical Review A*, 97:032324, 2018.
- [GW07] Gus Gutoski and John Watrous. [Toward a general theory of quantum games](#). In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 565–574, 2007.
- [Joh16] Nathaniel Johnston. [QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9](#), 2016.
- [Kil88] Joe Kilian. [Founding cryptography on oblivious transfer](#). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 20–31, 1988.
- [Kit02] Alexei Kitaev. [Quantum coin-flipping](#). Unpublished result. Talk in the 6th Annual workshop on Quantum Information Processing, QIP 2003, Berkeley, CA, USA, 2002.
- [KW16] Jędrzej Kaniewski and Stephanie Wehner. [Device-independent two-party cryptography secure against sequential attacks](#). *New Journal of Physics*, 18(5):055004, 2016.
- [Lo97] Hoi-Kwong Lo. [Insecurity of quantum secure computations](#). *Physical Review A*, 56:1154–1162, 1997.
- [Löf04] Johan Löfberg. [YALMIP : A toolbox for modeling and optimization in MATLAB](#). In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.
- [McK16] Matthew McKague. [Self-testing in parallel](#). *New Journal of Physics*, 18(4):045013, 2016.
- [McK17] Matthew McKague. [Self-testing in parallel with CHSH](#). *Quantum*, 1:1, 2017.
- [MOS19] MOSEK ApS. [The MOSEK optimization toolbox for MATLAB manual. Version 8.1.](#), 2019.
- [MY98] Dominic Mayers and Andrew Yao. [Quantum cryptography with imperfect apparatus](#). In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS '98*, pages 503–509, 1998.
- [NC10] Michael A. Nielsen and Isaac L. Chuang. [Quantum Computation and Quantum Information](#). Cambridge University Press, 2010.

- [NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. [A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations](#). *New Journal of Physics*, 10(7):073013, 2008.
- [PAB⁺09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. [Device-independent quantum key distribution secure against collective attacks](#). *New Journal of Physics*, 11(4):045021, 2009.
- [PT15] V. I. Paulsen and I. G. Todorov. [Quantum chromatic numbers via operator systems](#). *The Quarterly Journal of Mathematics*, 66(2):677–692, 2015.
- [SCA⁺11] Jonathan Silman, André Chailloux, Nati Aharon, Iordanis Kerenidis, Stefano Pironio, and Serge Massar. [Fully distrustful quantum bit commitment and coin flipping](#). *Physical Review Letters*, 106:220501, 2011.
- [Sch07] Christian Schaffner. [Cryptography in the bounded-quantum-storage model](#). arXiv preprint, 2007.
- [SCK14] Jamie Sikora, André Chailloux, and Iordanis Kerenidis. [Strong connections between quantum encodings, nonlocality, and quantum cryptography](#). *Physical Review A*, 89:022334, 2014.
- [Unr10] Dominique Unruh. [Universally Composable Quantum Multi-party Computation](#). In *Advances in Cryptology – EUROCRYPT 2010*, pages 486–505, 2010.
- [VPdR19] Vilasini Venkatesh, Christopher Portmann, and Lidia del Rio. [Composable security in relativistic quantum cryptography](#). *New Journal of Physics*, 21(4):043057, 2019.
- [Wat09] John Watrous. [Semidefinite programs for completely bounded norms](#). *Theory of Computing*, 5(11):217–238, 2009.
- [WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. [Device-independent parallel self-testing of two singlets](#). *Physical Review A*, 93:062121, 2016.
- [WST08] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. [Cryptography from noisy storage](#). *Physical Review Letters*, 100:220502, 2008.
- [WW08] Stephanie Wehner and Jürg Wullschleger. [Composable security in the bounded-quantum-storage model](#). In *International Colloquium on Automata, Languages, and Programming*, pages 604–615, 2008.

A Background: The NPA hierarchy

In this appendix, we briefly explain the NPA hierarchy as used in Section 4. The NPA hierarchy [NPA08] is a method to characterize the set of *quantum behaviours*, which are defined to be distributions that can be written as

$$\Pr(xy|ab) = \langle \nu | M_{x|a} N_{y|b} | \nu \rangle, \quad (48)$$

where $|\nu\rangle$ is a state in a Hilbert space \mathcal{H} and $\{M_{x|a}\}_{x \in X, a \in A}, \{N_{y|b}\}_{y \in Y, b \in B}$ are sets of operators on \mathcal{H} satisfying the following properties:

$$\begin{aligned}
M_{x|a}^\dagger &= M_{x|a} \text{ and } N_{y|b}^\dagger = N_{y|b}, \\
M_{x|a}M_{x'|a} &= \delta_{xx'}M_{x|a} \text{ and } N_{y|b}N_{y'|b} = \delta_{yy'}N_{y|b}, \\
\sum_{x \in X} M_{x|a} &= \mathbb{1} \text{ and } \sum_{y \in Y} N_{y|b} = \mathbb{1} \quad \forall a, b, \\
[M_{x|a}, N_{y|b}] &= 0 \quad \forall x, y, a, b.
\end{aligned} \tag{49}$$

Such distributions can be produced, for instance, by projective measurements on the subsystems of a tensor product of two Hilbert spaces⁹, as we are studying in this work. The NPA hierarchy consists of an infinite sequence of SDP conditions on $\Pr(xy|ab)$ which are all satisfied if and only if it is a quantum behaviour.

Specifically, let O denote any finite list of finite-length words formed by letters from the alphabet $\{M_{x|a}\}_{x \in X, a \in A} \cup \{N_{y|b}\}_{y \in Y, b \in B}$, and let O_j denote the j^{th} element of O . It is not hard to show that if we have a state and operators satisfying the conditions in Eq. (49), then any $|O| \times |O|$ matrix Γ with entries given by

$$\Gamma_{jk} = \langle \nu | O_j^\dagger O_k | \nu \rangle, \tag{50}$$

interpreting the words as the corresponding operators on \mathcal{H} , must be positive semidefinite. In particular, if $\Pr(xy|ab)$ is a quantum behaviour, then some of the entries of Γ correspond to values of $\Pr(xy|ab)$, hence imposing an SDP constraint on this distribution. Additional constraints on Γ can be imposed based on the relations in Eq. (49).

We hence see that any choice of O yields an SDP characterization of a superset of the set of quantum behaviours (this is sufficient to yield upper bounds on the cheating probabilities we consider in this work). A sequence of increasingly tight bounds can be obtained via appropriate choices of O . Specifically, if O is chosen to be the set of all words of length at most k , this will be referred to as *global level k* of the NPA hierarchy. It was shown in [NPA08] that if a distribution $\Pr(xy|ab)$ satisfies the SDP constraint at global level k for all k , then it must be a quantum behaviour. Hence the hierarchy describes a sequence of increasingly smaller sets that eventually converge to the set of quantum behaviours.

As a slight variation, one can also consider *local level k* , which refers to taking O to be the set of all words with at most k letters from $\{M_{x|a}\}_{x \in X, a \in A}$ and at most k letters from $\{N_{y|b}\}_{y \in Y, b \in B}$. (Basically, local level k defines a slightly smaller O than global level $2k$.) Our results are based on local level 1 of the hierarchy or slight extensions thereof (see Section 4). In addition, in our work we need to consider sequential measurements, which are not directly covered by the above description. However, as we discuss in Section 4, the probabilities produced by such measurements can also be expressed as elements of the matrix Γ and can be assumed projective, hence we can bound them using this approach.

⁹While every distribution achievable on such a tensor-product space can easily be expressed in the form (48), the converse is not necessarily true. However, the former property implies the NPA hierarchy characterizes a superset of the distributions we consider, which is sufficient for our goal of upper bounding the cheating probabilities — though the bounds may not be tight.

B Proof of Lemma 5

In this appendix we prove the rigidity lemma needed for the proof of our fully device-independent protocol. Again, in this section we often leave some tensor factors of $\mathbb{1}$ implicit.

Following [CN16], we define the following operators from the ideal measurements of the magic square game

$$\begin{aligned}
X_1^{\text{MS}} &= \sum_{x_0 x_1} (-1)^{x_1} M_{x_0 x_1|1}^{\text{MS}}, & X_2^{\text{MS}} &= \sum_{x_0 x_1} (-1)^{x_0} M_{x_0 x_1|1}^{\text{MS}}, \\
Z_1^{\text{MS}} &= \sum_{x_0 x_1} (-1)^{x_0} M_{x_0 x_1|0}^{\text{MS}}, & Z_2^{\text{MS}} &= \sum_{x_0 x_1} (-1)^{x_1} M_{x_0 x_1|0}^{\text{MS}}, \\
X_3^{\text{MS}} &= \sum_{y_0 y_1} (-1)^{y_1} N_{y_0 y_1|1}^{\text{MS}}, & X_4^{\text{MS}} &= \sum_{y_0 y_1} (-1)^{y_1} N_{y_0 y_1|0}^{\text{MS}}, \\
Z_3^{\text{MS}} &= \sum_{y_0 y_1} (-1)^{y_0} N_{y_0 y_1|0}^{\text{MS}}, & Z_4^{\text{MS}} &= \sum_{y_0 y_1} (-1)^{y_0} N_{y_0 y_1|1}^{\text{MS}}, \\
W_1^{\text{MS}} &= \sum_{x_0 x_1} (-1)^{x_0} M_{x_0 x_1|2}^{\text{MS}}, & W_2^{\text{MS}} &= \sum_{x_0 x_1} (-1)^{x_1} M_{x_0 x_1|2}^{\text{MS}}, \\
W_3^{\text{MS}} &= \sum_{y_0 y_1} (-1)^{y_0} N_{y_0 y_1|2}^{\text{MS}}, & W_4^{\text{MS}} &= \sum_{y_0 y_1} (-1)^{y_1} N_{y_0 y_1|2}^{\text{MS}}.
\end{aligned} \tag{51}$$

X_k, Z_k, W_k are defined similarly from the actual measurement operators $M_{x_0 x_1|a}, N_{y_0 y_1|b}$ (assumed projective, as declared in the Lemma 5 conditions) used by Alice and Bob.

Both [WBMS16] and [CN16] use the following lemma due to McKague, which we shall also need.

Lemma 8 ([McK16] Lemma 6). *Suppose $|\rho\rangle$ is a state on $\mathcal{X}\mathcal{Y}$ and $\{X_1, X_2\}, \{Z_1, Z_2\}$ are sets of Hermitian, unitary, commuting operators acting only on \mathcal{X} , and $\{X_3, X_4\}, \{Z_3, Z_4\}$ are sets of Hermitian, unitary, commuting operators acting only on \mathcal{Y} , such that for all $k \neq l$,*

$$\begin{aligned}
\|(X_k Z_l - Z_l X_k) |\rho\rangle\|_2 &\leq \delta \\
\|(X_k - Z_{k+2}) |\rho\rangle\|_2 &\leq \delta \\
\|(X_k Z_k + Z_k X_k) |\rho\rangle\|_2 &\leq \delta.
\end{aligned}$$

For $p, q \in \{0, 1\}^4$, let $X^p = \prod_{i=1}^4 X_i^{p_i}$ and let $Z^q, (X^{\text{MS}})^p, (Z^{\text{MS}})^q$ be defined similarly. Then, there exist isometries $V_A : \mathcal{X} \rightarrow \mathcal{X}_0 \mathcal{X}_1 \mathcal{J}_A$ and $V_B : \mathcal{Y} \rightarrow \mathcal{Y}_0 \mathcal{Y}_1 \mathcal{J}_B$ such that for any $p, q \in \{0, 1\}^4$,

$$\left\| (V_A \otimes V_B)(X^p Z^q) |\rho\rangle - (X^{\text{MS}})^p (Z^{\text{MS}})^q |\Psi^{\text{MS}}\rangle \otimes |\text{junk}\rangle \right\|_2 \leq O(\sqrt{\delta}).$$

Suppose the state $|\rho\rangle$ and measurements $M_{x|a}, N_{y|b}$ win the magic square game with probability $1 - \varepsilon$. Let p_{ab} denote the probability that this strategy wins when Alice and Bob's inputs are a and b . Since the inputs are uniformly distributed, this means that $\frac{1}{9} \sum_{a,b} p_{ab} = 1 - \varepsilon$. Since every probability is upper bounded by 1, for any fixed a, b we have,

$$p_{ab} = 9(1 - \varepsilon) - \sum_{(a', b') \neq (a, b)} p_{a' b'} \geq 9(1 - \varepsilon) - 8 \geq 1 - 9\varepsilon. \tag{52}$$

This implies that

$$\langle \nu | X_1 X_3 | \nu \rangle = \sum_{x_0 x_1 y_0 y_1} (-1)^{x_1 + y_1} \langle \nu | M_{x_0 x_1|1} N_{y_0 y_1|1} | \nu \rangle = p_{11} - (1 - p_{11}) \geq 1 - 18\varepsilon. \tag{53}$$

Similarly, using the lower bound on p_{ab} for other values of a, b we get

$$\langle \rho | X_2 X_4 | \rho \rangle \geq 1 - 18\varepsilon \quad (54)$$

$$\langle \rho | X_1 X_2 W_4 | \rho \rangle \geq 1 - 18\varepsilon \quad (55)$$

$$\langle \rho | Z_1 Z_3 | \rho \rangle \geq 1 - 18\varepsilon \quad (56)$$

$$\langle \rho | Z_2 Z_4 | \rho \rangle \geq 1 - 18\varepsilon \quad (57)$$

$$\langle \rho | Z_1 Z_2 W_3 | \rho \rangle \geq 1 - 18\varepsilon \quad (58)$$

$$-\langle \rho | W_1 X_4 Z_3 | \rho \rangle \geq 1 - 18\varepsilon \quad (59)$$

$$-\langle \rho | W_2 X_3 Z_4 | \rho \rangle \geq 1 - 18\varepsilon \quad (60)$$

$$-\langle \rho | W_1 W_2 W_3 W_4 | \rho \rangle \geq 1 - 18\varepsilon. \quad (61)$$

Using these relations, we can show that $\|(X_1 Z_1 + Z_1 X_1) | \rho \rangle\|_2 \leq O(\sqrt{\varepsilon})$, following [WBMS16, CN16]. (The argument basically relies on a sequence of bounds obtained in the same way as Eq. (66) below.) Similarly, we can show that all the conditions for Lemma 8 hold for the X_k, Z_k operators, and hence the conclusion of the lemma holds with a bound of $O(\varepsilon^{1/4})$.

Now, consider the cases $p = 1000, 0100, 1100$ with q being 0000 in all cases in the statement of the lemma. Using the definitions of X_1 and X_2 we have,

$$\begin{aligned} & \|(V_A \otimes V_B)((M_{00|1} - M_{01|1} + M_{10|1} - M_{11|1}) \otimes \mathbb{1}) | \rho \rangle \\ & - ((M_{00|1}^{\text{MS}} - M_{01|1}^{\text{MS}} + M_{10|1}^{\text{MS}} - M_{11|1}^{\text{MS}}) \otimes \mathbb{1}) | \Psi^{\text{MS}} \rangle \otimes |\text{junk}\rangle\|_2 \leq O(\varepsilon^{1/4}) \end{aligned} \quad (62)$$

$$\begin{aligned} & \|(V_A \otimes V_B)((M_{00|1} + M_{01|1} - M_{10|1} - M_{11|1}) \otimes \mathbb{1}) | \rho \rangle \\ & - ((M_{00|1}^{\text{MS}} + M_{01|1}^{\text{MS}} - M_{10|1}^{\text{MS}} - M_{11|1}^{\text{MS}}) \otimes \mathbb{1}) | \Psi^{\text{MS}} \rangle \otimes |\text{junk}\rangle\|_2 \leq O(\varepsilon^{1/4}) \end{aligned} \quad (63)$$

$$\begin{aligned} & \|(V_A \otimes V_B)((M_{00|1} - M_{01|1} - M_{10|1} + M_{11|1}) \otimes \mathbb{1}) | \rho \rangle \\ & - ((M_{00|1}^{\text{MS}} - M_{01|1}^{\text{MS}} - M_{10|1}^{\text{MS}} + M_{11|1}^{\text{MS}}) \otimes \mathbb{1}) | \Psi^{\text{MS}} \rangle \otimes |\text{junk}\rangle\|_2 \leq O(\varepsilon^{1/4}) \end{aligned} \quad (64)$$

where in the last inequality we have simplified $X_1 X_2$ using the fact that the $M_{x_0 x_1 | 1}, M_{x_0 x_1 | 1}^{\text{MS}}$ operators are orthogonal projectors. Moreover, both the $M_{x_0 x_1 | 1}$ and $M_{x_0 x_1 | 1}^{\text{MS}}$ operators must sum to the identity on their respective spaces, which implies (via the $p = q = 0000$ case) that

$$\begin{aligned} & \|(V_A \otimes V_B)((M_{00|1} + M_{01|1} + M_{10|1} + M_{11|1}) \otimes \mathbb{1}) | \rho \rangle \\ & - ((M_{00|1}^{\text{MS}} + M_{01|1}^{\text{MS}} + M_{10|1}^{\text{MS}} + M_{11|1}^{\text{MS}}) \otimes \mathbb{1}) | \Psi^{\text{MS}} \rangle \otimes |\text{junk}\rangle\|_2 \leq O(\varepsilon^{1/4}). \end{aligned} \quad (65)$$

Eqs. (62)–(65) involve linearly independent combinations of the $M_{x_0 x_1 | 1}$ operators (and the corresponding ones for $M_{x_0 x_1 | 1}^{\text{MS}}$). Hence from linear combinations of these we can self-test the $M_{x_0 x_1 | 1}$ operators, by applying the triangle inequality.

Similarly, $M_{x_0 x_1 | 0}^{\text{MS}}$ measurement can be self-tested by taking $p = 0000$ with $q = 1000, 0100, 1100$, and using the fact that $M_{x_0 x_1 | 0}^{\text{MS}}$ sum to identity. For self-testing $N_{y_0 y_1 | 1}^{\text{MS}}$ we take the equations for $(p = 0010, q = 0000), (p = 0000, q = 0001), (p = 0010, q = 0001)$, with the identity condition. And finally for $N_{y_0 y_1 | 0}^{\text{MS}}$ we take $(p = 0001, q = 0000), (p = 0000, q = 0010), (p = 0001, q = 0010)$ with the identity condition.

To self-test the $N_{y_0 y_1 | 2}$ operators, note that from Eq. (55),

$$\begin{aligned} \|(W_4 - X_1 X_2) | \rho \rangle\|_2^2 &= \langle \rho | W_4^2 | \rho \rangle + \langle \rho | (X_1 X_2)^2 | \rho \rangle - \langle \rho | W_4 X_1 X_2 | \rho \rangle - \langle \rho | X_1 X_2 W_4 | \rho \rangle \\ &= 2 - 2\langle \rho | X_1 X_2 W_4 | \rho \rangle \leq 2 - 2(1 - 18\varepsilon) = 36\varepsilon, \end{aligned} \quad (66)$$

where we have used the fact that W_4 and X_1X_2 square to identity by construction, and they also commute due to acting on only Alice and Bob's registers respectively. Using Eq. (58) similarly we have,

$$\|(W_3 - Z_1Z_2) |\rho\rangle\|_2 \leq O(\sqrt{\varepsilon}) \quad (67)$$

$$\|(W_4 - X_1X_2) |\rho\rangle\|_2 \leq O(\sqrt{\varepsilon}). \quad (68)$$

Now, using the fact that $\|W_3\|_\infty, \|X_1X_2\|_\infty = 1$, and W_3, W_4 commute with X_1, X_2, Z_1, Z_2 ,

$$\begin{aligned} \|(W_3W_4 - X_1X_2Z_1Z_2) |\rho\rangle\|_2 &\leq \|W_3(W_4 - X_1X_2) |\rho\rangle\|_2 + \|(W_3X_1X_2 - X_1X_2Z_1Z_2) |\rho\rangle\|_2 \\ &\leq \|(W_4 - X_1X_2) |\rho\rangle\|_2 + \|X_1X_2(W_3 - Z_1Z_2) |\rho\rangle\|_2 \\ &\leq \|(W_4 - X_1X_2) |\rho\rangle\|_2 + \|(W_3 - Z_1Z_2) |\rho\rangle\|_2 \\ &\leq O(\sqrt{\varepsilon}). \end{aligned} \quad (69)$$

We have already seen the self-testing of the X_1X_2 and Z_1Z_2 operators. Taking $(p = 1100, q = 1100)$ in Lemma 8 lets us self-test $X_1X_2Z_1Z_2$. Moreover, since the ideal magic square state and measurements win the magic square game perfectly, they must satisfy analogous relations with $\varepsilon = 0$, i.e. we have

$$\begin{aligned} Z_1^{\text{MS}} Z_2^{\text{MS}} |\Psi^{\text{MS}}\rangle &= W_3^{\text{MS}} |\Psi^{\text{MS}}\rangle, & X_1^{\text{MS}} X_2^{\text{MS}} |\Psi^{\text{MS}}\rangle &= W_4^{\text{MS}} |\Psi^{\text{MS}}\rangle, \\ X_1^{\text{MS}} X_2^{\text{MS}} Z_1^{\text{MS}} Z_2^{\text{MS}} |\Psi^{\text{MS}}\rangle &= W_3^{\text{MS}} W_4^{\text{MS}} |\Psi^{\text{MS}}\rangle. \end{aligned} \quad (70)$$

Using these, Eqs. (67)–(69) and the fact that the $N_{y_0y_1|2}$ operators add to identity lets us self-test this measurement.

Finally, to self-test the $M_{x_0x_1|2}$ operators, we note that using Eqs. (59)–(61) we get,

$$\|(W_1 + X_4Z_3) |\rho\rangle\|_2 \leq O(\sqrt{\varepsilon}) \quad (71)$$

$$\|(W_2 + X_3Z_4) |\rho\rangle\|_2 \leq O(\sqrt{\varepsilon}) \quad (72)$$

$$\|(W_1W_2 + W_3W_4) |\rho\rangle\|_2 \leq O(\sqrt{\varepsilon}). \quad (73)$$

The ideal magic square state and measurements satisfy

$$\begin{aligned} X_4^{\text{MS}} Z_3^{\text{MS}} |\Psi^{\text{MS}}\rangle &= -W_1^{\text{MS}} |\Psi^{\text{MS}}\rangle & X_3^{\text{MS}} Z_4^{\text{MS}} |\Psi^{\text{MS}}\rangle &= -W_2^{\text{MS}} |\Psi^{\text{MS}}\rangle \\ W_3^{\text{MS}} W_4^{\text{MS}} |\Psi^{\text{MS}}\rangle &= -W_1^{\text{MS}} W_2^{\text{MS}} |\Psi^{\text{MS}}\rangle. \end{aligned} \quad (74)$$

Using these, Eqs. (71)–(73), the statement of Lemma 8 for $(p = 0001, q = 0010), (p = 0010, q = 0001)$, the self-testing of W_3W_4 that we have already seen, and the identity condition for $M_{x_0x_1|2}$, we can self-test this measurement. This completes the list of all self-testing statements in Lemma 5.

C Dilation to projective measurements

In this appendix, we prove the claim in Section 4 that we can assume the measurements are projective without loss of generality. As mentioned previously, such reductions are already known for standard Bell-nonlocality scenarios — for instance, the proof for tensor product measurements is just a simpler version of the construction here. (The proof for commuting measurements is more complicated [PT15], and we do not aim to consider that model in this work.) However, our proof here accommodates some forms of sequential measurements, as required for our protocol.

First, to handle a dilation of isometries to unitaries that we will need if the systems are infinite-dimensional, we prove a useful lemma based on the Sz.-Nagy dilation for an isometry.

Lemma 9. Consider a set of isometries $V_j : \mathcal{H}_0 \rightarrow \mathcal{H}_j$ for $j = 1, 2, \dots, n$, and another set of isometries $V'_k : \mathcal{H}_n \rightarrow \mathcal{K}_k$ for $k = 1, 2, \dots, m$. Let $\mathcal{L} = \bigoplus_{j=0}^n \mathcal{H}_j \oplus \bigoplus_{k=1}^m \mathcal{K}_k$, and view all \mathcal{H}_j and \mathcal{K}_k as subspaces of \mathcal{L} . Then there exist unitaries $\{U_j\}_{j=1}^n$ on \mathcal{L} such that for any $|\nu\rangle \in \mathcal{H}_0$, we have $V_j |\nu\rangle = U_j |\nu\rangle \in \mathcal{H}_j$. There also exist unitaries $\{U'_k\}_{k=1}^m$ on \mathcal{L} such that for any $|\mu\rangle \in \mathcal{H}_n$, we have $V'_k |\mu\rangle = U'_k |\mu\rangle \in \mathcal{K}_k$.

Proof. For brevity, we only prove the case for $n = m = 2$; the construction for more isometries is precisely analogous. For any isometry V with some domain \mathcal{H} , we define the operator $\Pi_V = \mathbb{1}_{\mathcal{H}} - VV^\dagger$, which can be easily shown to be a projector satisfying $V^\dagger \Pi_V = \Pi_V V = 0$. Let

$$\begin{aligned} U_1 &= \begin{pmatrix} 0_{\mathcal{H}_0} & -V_1^\dagger & & & & \\ V_1 & \Pi_{V_1} & & & & \\ & & \mathbb{1}_{\mathcal{H}_2} & & & \\ & & & \mathbb{1}_{\mathcal{K}_1 \oplus \mathcal{K}_2} & & \end{pmatrix}, & U_2 &= \begin{pmatrix} 0_{\mathcal{H}_0} & & -V_2^\dagger & & & \\ & \mathbb{1}_{\mathcal{H}_1} & & & & \\ V_2 & & \Pi_{V_2} & & & \\ & & & \mathbb{1}_{\mathcal{K}_1 \oplus \mathcal{K}_2} & & \end{pmatrix}, \\ U'_1 &= \begin{pmatrix} \mathbb{1}_{\mathcal{H}_0 \oplus \mathcal{H}_1} & & & & & \\ & 0_{\mathcal{H}_2} & -V_1'^\dagger & & & \\ & V_1' & \Pi_{V_1'} & & & \\ & & & \mathbb{1}_{\mathcal{K}_2} & & \end{pmatrix}, & U'_2 &= \begin{pmatrix} \mathbb{1}_{\mathcal{H}_0 \oplus \mathcal{H}_1} & & & & & \\ & 0_{\mathcal{H}_2} & & -V_2'^\dagger & & \\ & & \mathbb{1}_{\mathcal{K}_1} & & & \\ & V_2' & & \Pi_{V_2'} & & \end{pmatrix}, \end{aligned} \quad (75)$$

where blank blocks in the matrices are taken to be filled with zero operators. A direct calculation shows that these operators are indeed unitary and satisfy the desired property, e.g. for U_1 we have

$$\begin{aligned} U_1^\dagger U_1 &= \begin{pmatrix} 0_{\mathcal{H}_0} & V_1^\dagger & & & & \\ -V_1 & \Pi_{V_1} & & & & \\ & & \mathbb{1}_{\mathcal{H}_2} & & & \\ & & & \mathbb{1}_{\mathcal{K}_1 \oplus \mathcal{K}_2} & & \end{pmatrix} \begin{pmatrix} 0_{\mathcal{H}_0} & -V_1^\dagger & & & & \\ V_1 & \Pi_{V_1} & & & & \\ & & \mathbb{1}_{\mathcal{H}_2} & & & \\ & & & \mathbb{1}_{\mathcal{K}_1 \oplus \mathcal{K}_2} & & \end{pmatrix} \\ &= \begin{pmatrix} 0_{\mathcal{H}_0} + V_1^\dagger V_1 & 0_{\mathcal{H}_0} + V_1^\dagger \Pi_{V_1} & & & & \\ 0_{\mathcal{H}_0} + \Pi_{V_1} V_1 & V_1 V_1^\dagger + \Pi_{V_1} & & & & \\ & & \mathbb{1}_{\mathcal{H}_2} & & & \\ & & & \mathbb{1}_{\mathcal{K}_1 \oplus \mathcal{K}_2} & & \end{pmatrix} \\ &= \mathbb{1}_{\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_2 \oplus \mathcal{K}_1 \oplus \mathcal{K}_2} \end{aligned} \quad (76)$$

and

$$U_1 |\nu\rangle = \begin{pmatrix} 0_{\mathcal{H}_0} & -V_1^\dagger & & & & \\ V_1 & \Pi_{V_1} & & & & \\ & & \mathbb{1}_{\mathcal{H}_2} & & & \\ & & & \mathbb{1}_{\mathcal{K}_1 \oplus \mathcal{K}_2} & & \end{pmatrix} \begin{pmatrix} |\nu\rangle \\ \mathbf{0}_{\mathcal{H}_1} \\ \mathbf{0}_{\mathcal{H}_2} \\ \mathbf{0}_{\mathcal{K}_1 \oplus \mathcal{K}_2} \end{pmatrix} = \begin{pmatrix} \mathbf{0}_{\mathcal{H}_0} \\ V_1 |\nu\rangle \\ \mathbf{0}_{\mathcal{H}_2} \\ \mathbf{0}_{\mathcal{K}_1 \oplus \mathcal{K}_2} \end{pmatrix}. \quad (77)$$

□

Remark 7. The construction in the above proof easily generalizes in several ways, for instance if one allows some of the isometries to have the same codomain, or if another set of isometries could be applied after V'_k .

We now prove the claim that the measurements can be assumed projective without loss of generality, stated as the following lemma:

Lemma 10. For any state ρ and POVMs attaining some value for Bob's cheating probability (as expressed in Eq. (36)), there is another state $\bar{\rho}$ and projective measurements (PVMs) that attain the same value. An analogous statement holds for Alice's cheating probability (as expressed in Eq. (39)).

Proof. We describe the proof for cheating Bob only (the proof for cheating Alice is analogous, though simpler since there are no sequential measurements in that case).

First, let us denote Alice and Bob's measurement operators as $M_{x|a}$, $N_{y^A|b^A}^{\text{test}}$, N_y^{prot} and $N_{g|m}^{\text{prot}}$, as described previously, but here we shall not assume they are projective. Note that this is intended to denote the Kraus operators of the measurements, rather than the POVM elements. More specifically, taking $M_{x|a}$ (for a fixed a) as an example, this denotes a set of operators satisfying $\sum_x M_{x|a}^\dagger M_{x|a} = \mathbb{1}$, such that the (subnormalized) state after performing the measurement on a state ρ and getting outcome x is $M_{x|a}\rho M_{x|a}^\dagger$. (This is slightly more detailed than specifying POVM elements $E_{x|a} \succeq 0$ such that $\sum_x E_{x|a} = \mathbb{1}$ and $P(x) = \text{Tr}(E_{x|a}\rho)$, because it incorporates an explicit description of the post-measurement state. This allows, for instance, defining $M_{x|a}$ such that the measurement outcome and choice of measurement is encoded into the post-measurement state, which is important for sequential measurements.) For projective measurements, the two notions coincide and hence we did not need to specify this distinction previously.

Without loss of generality, we can assume the codomains of all the measurement operators are the same (if they were different, we could simply view all of them as being embedded in a common Hilbert space; for instance the direct sum of all the Hilbert spaces¹⁰). Let \mathcal{Y}' and \mathcal{Y}'' be 4-dimensional Hilbert spaces with orthonormal bases $\{|y'\rangle\}$ and $\{|y''\rangle\}$. We first define the following isometries:

$$\begin{aligned} V_{b^A}^{\text{test}} |\nu\rangle_{\mathcal{Y}} &= \sum_{y^A} |y^A\rangle_{\mathcal{Y}'} N_{y^A|b^A}^{\text{test}} |\nu\rangle_{\mathcal{Y}}, \\ V^{\text{prot}} |\nu\rangle_{\mathcal{Y}} &= \sum_y |y\rangle_{\mathcal{Y}'} N_y^{\text{prot}} |\nu\rangle_{\mathcal{Y}}, \\ V_m^{\text{prot}} |g'\rangle_{\mathcal{Y}'} |\nu\rangle_{\mathcal{Y}} &= \sum_g |g y'\rangle_{\mathcal{Y}''\mathcal{Y}'} N_{g|m}^{\text{prot}} |\nu\rangle_{\mathcal{Y}}. \end{aligned} \quad (78)$$

We apply Lemma 9 with $V_{b^A}^{\text{test}}$ being the isometries $\{V_j\}_{j=1}^{n-1}$, V^{prot} being the isometry V_n , and V_m^{prot} being the isometries $\{V_k\}_{k=1}^m$. This gives us corresponding unitaries on a Hilbert space \mathcal{L} , which we now take as the space in which all subsequent expressions are embedded. (In the finite-dimensional case, one can perform a simpler construction in which $\mathcal{Y}''\mathcal{Y}'\mathcal{Y}$ itself is the common Hilbert space, see e.g. [NC10].) These unitaries match the actions of the isometries on their respective subspaces, i.e. $U_{b^A}^{\text{test}} |\nu\rangle_{\mathcal{Y}} = V_{b^A}^{\text{test}} |\nu\rangle_{\mathcal{Y}}$, $U^{\text{prot}} |\nu\rangle_{\mathcal{Y}} = V^{\text{prot}} |\nu\rangle_{\mathcal{Y}}$ and $U_m^{\text{prot}} |\mu\rangle_{\mathcal{Y}''\mathcal{Y}'} = V_m^{\text{prot}} |\mu\rangle_{\mathcal{Y}''\mathcal{Y}'}$.

For each isometry V , let $\mathcal{L}_{\setminus V}$ denote the subspace of \mathcal{L} given by omitting the codomain of V from the direct sum used to construct \mathcal{L} (we introduce this technical detail just to ensure the PVM sets we construct below indeed sum to the identity on \mathcal{L}). We then define projectors

$$\begin{aligned} \Pi_{y^A|b^A}^{\text{test}} &= U_{b^A}^{\text{test}\dagger} ((|y^A\rangle\langle y^A|_{\mathcal{Y}'} \otimes \mathbb{1}_{\mathcal{Y}}) \oplus \delta_{y^A,0} \mathbb{1}_{\mathcal{L}_{\setminus V_{b^A}^{\text{test}}}}) U_{b^A}^{\text{test}}, \\ \Pi_y^{\text{prot}} &= U^{\text{prot}\dagger} ((|y\rangle\langle y|_{\mathcal{Y}'} \otimes \mathbb{1}_{\mathcal{Y}}) \oplus \delta_{y,0} \mathbb{1}_{\mathcal{L}_{\setminus V^{\text{prot}}}}) U^{\text{prot}}, \\ \Pi_{g|m}^{\text{prot}} &= U_m^{\text{prot}\dagger} U_m^{\text{prot}\dagger} ((|g\rangle\langle g|_{\mathcal{Y}''} \otimes \mathbb{1}_{\mathcal{Y}'}) \oplus \delta_{g,0} \mathbb{1}_{\mathcal{L}_{\setminus V_m^{\text{prot}}}}) U_m^{\text{prot}} U_m^{\text{prot}}, \end{aligned} \quad (79)$$

where $\delta_{j,k}$ denotes the Kronecker delta. It is easily seen that these form valid PVM sets. Importantly, these projectors have the useful property (omitting the $\mathbb{1}_{\mathcal{L}_{\setminus V}}$ terms for brevity)

$$\Pi_{g|m}^{\text{prot}} \Pi_y^{\text{prot}} = U_m^{\text{prot}\dagger} U_m^{\text{prot}\dagger} (|g\rangle\langle g|_{\mathcal{Y}''} \otimes \mathbb{1}_{\mathcal{Y}'}) U_m^{\text{prot}} (|y^A\rangle\langle y^A|_{\mathcal{Y}'} \otimes \mathbb{1}_{\mathcal{Y}}) U^{\text{prot}}. \quad (80)$$

¹⁰Technically, the operators $N_{g|m}^{\text{prot}}$ must be modified to ensure the POVM elements still sum to the identity on this space, but this is fairly straightforward (similar to the construction in Eq. (79)).

We construct unitaries U_a and projectors $\Pi_{x|a}$ analogously for Alice, though for that we only need to introduce a single ancillary system \mathcal{X}' . As for the state, we can simply take $|\bar{\rho}\rangle = |\rho\rangle$, though with the understanding that it is now embedded in a larger Hilbert space. Using Eq. (80), we now compute some probabilities resulting from these projective measurements:

$$\begin{aligned} \left\| \Pi_{x^A|a^A} \Pi_{y^A|b^A}^{\text{test}} |\rho\rangle \right\|_2 &= \left\| U_{a^A}^\dagger U_{b^A}^{\text{test}\dagger} \left(|x y^A\rangle M_{x^A|a^A} N_{y^A|b^A}^{\text{test}} |\rho\rangle \right) \right\|_2 \\ &= \left\| M_{x^A|a^A} N_{y^A|b^A}^{\text{test}} |\rho\rangle \right\|_2, \end{aligned} \quad (81)$$

$$\begin{aligned} \left\| \Pi_{x|a} \Pi_{g|m}^{\text{prot}} \Pi_y^{\text{prot}} |\rho\rangle \right\|_2 &= \left\| U_a^\dagger U_m^{\text{prot}\dagger} U_y^{\text{prot}\dagger} \left(|x g y\rangle M_{x|a} N_{g|m}^{\text{prot}} N_y^{\text{prot}} |\rho\rangle \right) \right\|_2 \\ &= \left\| M_{x|a} N_{g|m}^{\text{prot}} N_y^{\text{prot}} |\rho\rangle \right\|_2, \end{aligned} \quad (82)$$

since the 2-norm is unitarily invariant. These probabilities include all terms appearing in the cheating probability¹¹, and are equal to those attained by the original POVMs on $|\rho\rangle$. \square

¹¹We have exploited the fact that in our scenario, the measurements $M_{g|m}^{\text{prot}}$ are always only applied after the measurement M_y^{prot} . If there had been another possible measurement (including a trivial measurement, i.e. identity operation) to perform before measuring $M_{g|m}^{\text{prot}}$, it might not always be possible to ensure that the equivalent of Eq. (80) holds for that measurement as well. (In particular, when applying the NPA hierarchy, the projective measurements we constructed may not give the same value for all the Γ matrix elements as the original POVMs. However, this is not an issue because the reduction to projective measurements occurs *before* applying the NPA hierarchy.)