Imperfect 1-Out-of-2 Quantum Oblivious Transfer: Bounds, a Protocol, and its Experimental Implementation

Ryan Amiri,[1] Robert Stárek,[2] David Reichmuth,[1] Ittoop V. Puthoor,[1] Michal Mičuda,[2] Ladislav Mišta, Jr.,[2] Miloslav Dušek,[2] Petros Wallden,[3,*] and Erika Andersson[1]

[1] *SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

[2] *Department of Optics, Palacky University, 779 00 Olomouc, Czech Republic*

[3] *LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*

(Received 16 July 2020; accepted 15 January 2021; published 1 March 2021)

Oblivious transfer is an important primitive in modern cryptography. Applications include secure multiparty computation, oblivious sampling, *e*-voting, and signatures. Information-theoretically secure perfect 1-out-of 2 oblivious transfer is impossible to achieve. Imperfect variants, where both participants' ability to cheat is still limited, are possible using quantum means while remaining classically impossible. Precisely what security parameters are attainable remains unknown. We introduce a theoretical framework for studying semirandom quantum oblivious transfer, which is shown to be equivalent to regular oblivious transfer in terms of cheating probabilities. We then use it to derive bounds on cheating. We also present a protocol with lower cheating probabilities than previous schemes, together with its optical realization. We show that a lower bound of $\frac{2}{3}$ on the minimum achievable cheating probability can be directly derived for semirandom protocols using a different method and definition of cheating than used previously. The lower bound increases from $\frac{2}{3}$ to approximately 0.749 if the states output by the protocol are pure and symmetric. The oblivious transfer scheme we present uses unambiguous state elimination measurements and can be implemented with the same technological requirements as standard quantum cryptography. In particular, it does not require honest participants to prepare or measure entangled states. The cheating probabilities are $\frac{3}{4}$ and approximately 0.729 for sender and receiver, respectively, which is lower than in existing protocols. Using a photonic testbed, we have implemented the protocol with honest parties, as well as optimal cheating strategies. Because of the asymmetry of the receiver's and sender's cheating probabilities, the protocol can be combined with a "trivial" protocol to achieve an overall protocol with lower average cheating probabilities of approximately 0.74 for both sender and receiver. This demonstrates that, interestingly, protocols where the final output states are pure and symmetric are not optimal in terms of average cheating probability.

DOI: 10.1103/PRXQuantum.2.010335

I. INTRODUCTION

Following the discovery of quantum key distribution in 1984 [1], there arose a general optimism that quantum mechanics may provide a means to perform multiparty computations with information-theoretic security. Despite this early confidence, the history of secure two-party computations is characterized by mainly negative results. Mayers and Lo [2,3] proved that all one-sided two-party computations are insecure in the quantum setting, meaning that it is impossible to perform important protocols such as bit commitment and oblivious transfer (OT) with information-theoretic security. Nevertheless, imperfect variants of these protocols remain possible, and it has been an interesting and productive open question to determine the optimal security parameters achievable for some important two-party computations.

For many cryptographic primitives, this question has been definitively answered. For strong coin flipping, Kitaev [4] introduced the semidefinite programming formalism to show that the product of Alice's and Bob's cheating probabilities must be greater than $\frac{1}{2}$, implying that the minimum cheating probability is at least $1/\sqrt{2}$. For weak coin flipping, Mochon [5] showed that the minimum

*petros.wallden@ed.ac.uk

cheating probability is at least $\frac{1}{2} + \epsilon$ for any $\epsilon > 0$. In the same paper a protocol achieving this bound is presented, showing that the bound is tight. Chailloux and Kerenidis [6] used these results on weak coin flipping to generate a protocol for strong coin flipping achieving Kitaev's bound. Lastly, for quantum bit commitment, Chailloux and Kerenidis [7] proved that the minimum cheating probability is 0.739, and presented a protocol achieving this bias. Thus, for bit commitment, weak coin flipping, and strong coin flipping, the achievability bounds are tight with the known protocols.

For OT on the other hand, the situation is not as clear. Classically, it is impossible to achieve even limited security for OT in the information-theoretic setting, since one party can always cheat with certainty. On the other hand, quantum mechanics allows for imperfect protocols, in which the participants are able to cheat but their abilities are limited.

OT is a fundamental primitive in cryptography. Its importance stems from the fact that it can be used as the foundation for secure two-party computations; with oblivious transfer, all secure two-party computations are possible [8,9]. OT exists in many different flavors, all with slightly different definitions and notions of security. It was first introduced informally in 1970 by Wiesner as "a means for transmitting two messages either but not both of which may be received" [10], and subsequently formalized as 1-out-of-2 oblivious transfer (1-2 OT) in Ref. [11]. In related work, Rabin [12] introduced a protocol (now called Rabin OT), which was later shown by Crépeau [13] to be classically equivalent to 1-2 OT, in the sense that if it is possible to do one, it is possible to use this to implement the other. Various "weaker" variants of OT have also been proposed, most notably generalized OT, XOR OT, and universal OT [14], but all have been shown to be equivalent to 1-2 OT [15] in the classical setting. The equivalence is believed to also hold in the quantum setting, but the reduction proofs may need to be revised. There is also work by Damgård *et al.* [16], who defined OT in a slightly different way, and characterized security in terms of information leakage. With these definitions (and their quantum counterparts), the authors described a 1-2 OT protocol that is secure in the bounded quantum storage model. Spacetime-constrained quantum OT protocols have also been proposed [17–19], requiring agents at different locations in spacetime, giving constraints on where in spacetime bit values can be obtained. Recently, a device-independent quantum XOR oblivious transfer protocol was proposed [20]. The protocol uses a shared entangled state to reveal cheating. Another version of "imperfect" oblivious transfer was considered and experimentally implemented in Ref. [21], where the authors could achieve vanishing cheating advantage for both sides, at the expense of having a protocol that sometimes fails during honest execution.

In this paper we consider standalone quantum protocols for 1-2 OT, including an experimental implementation of such a protocol, and are concerned only with information-theoretic security. As mentioned above, perfect security in this setting is impossible. The best known lower bound on the achievable bias in 1-2 OT protocols is due to Chailloux *et al.* [22], who showed that the minimum cheating probability is at least $\frac{2}{3}$ if participants are "semihonest." With the definition of cheating used in Ref. [22], with "semihonest" participants, this bound is tight. However, the best known OT protocol has a cheating probability of 0.75 if parties are not assumed to be semihonest [23], meaning that there is a gap between what is known to be achievable, and what is known to be impossible. Narrowing this gap either way—obtaining higher and thus tighter lower bounds on cheating probabilities, or finding concrete protocols with smaller cheating probabilities, leading to lower upper bounds—is the main target of this paper. In order to obtain lower upper bounds, we consider general classes of protocols (either completely general or with some restrictions), but limit the capabilities of adversaries. This therefore provides only lower bounds on cheating probabilities, applicable to *all* protocols within the considered class. To obtain upper bounds on cheating probabilities, we give a specific protocol, and then consider the most general attacks. This therefore provides an upper bound on achievable cheating probabilities, in the sense that the best protocol can perform at least as well as the specific protocol we give. There is also a subtlety regarding the requirement of semihonesty, and related to this, to what extent dishonest parties can always obtain the information they would have obtained if they had been honest especially when considering variants of oblivious transfer that are not deterministic. We return to this below.

Our paper contains four main contributions.

1. We introduce the concept of semirandom OT and prove a functional equivalence with respect to the cheating probabilities between 1-2 OT and semirandom OT. We further describe a general framework for semirandom OT.
2. We use this framework to show that the minimum achievable bound on the cheating probability is $\frac{2}{3}$. This agrees with the result in Ref. [22] for regular (deterministic) oblivious transfer, but in our case we do not assume that parties are semihonest. We also increase the lower bound on the minimum achievable cheating probability for 1-2 quantum OT protocols to 0.749 if the states in the final round of the protocol when the parties are honest are pure and symmetric. We parameterize Alice's and Bob's ability to cheat in terms of a single variable F, related to the fidelity of the protocol output states. This parametrization suggests how to construct schemes

when either sender or receiver dishonesty is prioritized. That is, sender and receiver can have different cheating probabilities, and one can derive bounds for such situations. Such a scenario arises in the context of quantum signature schemes [24,25], and the derived bounds may prove useful for understanding the potential application of imperfect OT to signatures.

3. We illustrate our construction by giving an OT protocol relying on unambiguous state elimination measurements. The protocol improves on previous protocols in the sense that it decreases the cheating probability of the receiver and is easier to implement. It also highlights the connection between unambiguous state elimination measurements and 1-2 OT, and provides a new application for this relatively seldom used type of measurement. The security parameters achieved are almost tight with the bounds for protocols using pure symmetric states proven in this paper. In this protocol, one party has a smaller cheating probability than the other. This is not captured by the overall cheating probability, defined as the maximum of the cheating probabilities of either party. Such protocols might however be used for applications where restricting cheating by one party is prioritized. Such a protocol can also be combined with a "trivial" protocol, to achieve a protocol with lower average cheating probability, where both sender and receiver can cheat with probability at most 0.74. This is lower than the bound for protocols using pure symmetric states and constitutes an improvement on previously known protocols.
4. Last, but not least, we present an optical realization of the protocol we have given. In principle, an implementation of the protocol needs only the same components used for standard BB84 [1] quantum key distribution. Each of the two qubits can be encoded into a single photon, sent individually to Bob, and measured using the same components as in BB84 quantum key distribution. That is, to implement our protocol, one only needs the components used for standard quantum key distribution. Our setup is however slightly different, because we want not only to test the protocol with the honest parties, but also experimentally implement the optimal cheating strategies and verify the predicted cheating probabilities. It is obvious that, for any (e.g., commercial) application, the evaluation of the feasibility and practicality of the protocol considers the components required for an honest execution. Realizing cheating strategies is still of interest to evaluate how secure is the protocol in practice (cf. quantum hacking). To implement these optimal cheating strategies requires usage of a nontrivial entangled state. We therefore encode two qubits into a single photon, and employ a linear optical quantum gate to prepare an entangled state where these two qubits are entangled with a third qubit retained by Alice, which is encoded in a separate second photon. The experimental results for both honest and cheating parties agree well with theoretical values, demonstrating that the protocol is feasible also when realized in this way.

The paper is organized as follows. We begin in Sec. II by defining 1-2 OT and semirandom OT, stating an equivalence between the cheating probabilities for each. In Sec. III we describe a general framework for semirandom OT protocols and consider specific undetectable cheating strategies always available to Alice and Bob. We analyze these strategies to lower bound the achievable cheating probabilities for unbounded adversaries in 1-2 OT. In Sec. IV we first introduce unambiguous measurements, in particular unambiguous state elimination measurements, and motivate their use in cryptography. We describe a semirandom OT protocol that employs unambiguous state elimination measurements and analyze its security in the asymptotic limit. In Sec. V, we present the experimental implementation of this protocol.

II. DEFINITIONS

Intuitively, 1-2 OT is a two-party protocol in which Alice chooses two input bits, x_0 and x_1, and Bob chooses a single input bit b. The protocol outputs x_b to Bob with the guarantees that Alice does not know b and that Bob does not know $x_{b\oplus 1}$. A cheating Alice aims to find the value of b, while a cheating Bob aims to correctly guess both x_0 and x_1.

At this point it is worth stressing that, whenever we speak of the cheating probability of one party, we assume that the other party executes the protocol honestly. This is a standard assumption in all cryptographic protocols with two competing parties (such as coin flip, bit commitment, and all versions of oblivious transfer) and we adopt it throughout the paper. The reason for this assumption is twofold. First, one is interested in ensuring that the "interests" of honest parties are secured, while it is less relevant to give guarantees to a cheating party. The second reason is that even defining what constitutes a cheating requires the other party to behave (at least to a point) honestly. For example, how can Bob cheat (guessing both x_0 and x_1) if Alice has not even chosen two bits?

Definition 1 (Ref. [23])**.** *A* 1-2 *quantum OT protocol is a protocol between two parties, Alice and Bob, such that the following statements hold.*

(a) *Alice has inputs* $x_0, x_1 \in \{0,1\}$ *and Bob has input* $b \in \{0,1\}$. *At the beginning of the protocol, Alice*

has no information about b and Bob has no information about (x_0, x_1).

(b) *At the end of the protocol, Bob outputs y or abort and Alice can either abort or not.*

(c) *If Alice and Bob are honest, they never abort,* $y = x_b$*, Alice has no information about b, and Bob has no information about* $x_{b\oplus 1}$.

(d) $A_{OT} := \sup\{\Pr[$*Alice correctly guesses b* $\wedge$ *Bob does not abort*$]\} = \frac{1}{2} + \epsilon_A$.

(e) $B_{OT} := \sup\{\Pr[$*Bob correctly guesses* (x_0, x_1) $\wedge$ *Alice does not abort*$]\} = \frac{1}{2} + \epsilon_B$.

The suprema are taken over all cheating strategies available to Alice and Bob. We note that there are also less common variants of the definition of B_{OT}, all with subtly different cheating implications. Sikora *et al.* [26] defined cheating in terms of Bob being able to guess the XOR of Alice's bits, while Chailloux *et al.* [22] defined cheating in terms of Bob's ability to guess both bits, while also requiring that Bob can always retrieve a single bit with certainty. The choice of which definition is most appropriate will be largely application dependent.

We define $p_C := \max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\}$ to be the *cheating probability* of the protocol. The maximum cheating probability characterizes the performance of an OT protocol since protocols with $(A_{\mathrm{OT}} = 1, B_{\mathrm{OT}} = 0.5)$ are easy to construct. However, for certain applications, keeping track of cheating probabilities for both parties may be relevant. For example, it is conceivable that there are applications for which a protocol with cheating probabilities $(0.76, 0.5)$ may be better than that with $(0.75, 0.75)$, and that protocols with the same maximum cheating probability could be ordered with respect to the smaller cheating probability. Note also that our definition of security, while commonly used, differs from that in some other works, for example, Ref. [27], where security is characterized in terms of the information leakage, or in terms of Bob's ability to guess the output of some function $f(x_0, x_1)$. Nevertheless, our simpler definition makes sense if we are interested only in lower bounds on the cheating probability, since the ability to guess (x_0, x_1) automatically implies the ability to guess $f(x_0, x_1)$ for any f.

In this paper we define a variant of OT, semirandom OT, which differs from the above 1-2 OT in that Bob does not have any inputs and randomly obtains one of Alice's bit values. More concretely, semirandom OT is defined below.

Definition 2. *A* 1-2 *quantum semirandom OT, or simply semirandom OT, is a protocol between two parties, Alice and Bob, such that the following statements hold.*

(a) *Alice chooses two input bits* $(x_0, x_1) \in \{0, 1\}$ *or abort.*

(b) *Bob outputs two bits* (c, y) *or abort.*

(c) *If Alice and Bob are honest, they never abort,* $y = x_c$*, Alice has no information about c, and Bob has no information on* $x_{c\oplus 1}$*. Furthermore,* x_0, x_1 *and c are uniformly random bits [28].*

(d) $A_{OT} := \sup\{\Pr[$*Alice correctly guesses c* $\wedge$ *Bob does not abort*$]\} = \frac{1}{2} + \epsilon_A$.

(e) $B_{OT} := \sup\{\Pr[$*Bob correctly guesses* (x_0, x_1) $\wedge$ *Alice does not abort*$]\} = \frac{1}{2} + \epsilon_B$.

The reason for introducing semirandom OT is that we have found it simpler to work with than 1-2 OT, and the ability to perform semirandom OT with cheating probabilities A_{OT} and B_{OT} implies being able to perform 1-2 quantum OT with the same cheating probabilities using additional classical communication and processing (see Appendix A). Moreover, in spite of the equivalence in the above sense, semirandom protocols where Bob does not choose which bit he obtains can be subtly different from protocols where Bob can choose his input, in the following sense. In a semirandom protocol, such as the example protocol we give in Sec. IV, Bob obtains Alice's first or second bit at random [29]. In other words, the protocol is not deterministic, even when parties honestly follow the protocol, and it generally involves a destructive quantum measurement. In order to obtain his "honest" output, Bob needs to irreversibly disturb the quantum state he possesses. In earlier papers [3,22] it is assumed, correctly for their framework, that Bob can always make a nondestructive measurement to obtain the bit of his choice. Bounds derived in this way then do not directly apply to semirandom OT protocols, where such a measurement does not exist. Nevertheless, semirandom OT can be used to implement "regular" OT, using classical postprocessing, as described in Appendix A. There are subtle differences when considering how such postprocessing affects lower and upper bounds on cheating. Here we directly obtain the same bound as in Ref. [22], but by considering semirandom protocols. Our new technique also enables us to both increase the lower bound for protocols that use symmetric pure states, and to lower the upper bound by constructing a protocol with smaller cheating probabilities averaged over both parties.

III. GENERIC PROTOCOL

In this section we introduce a general framework for semirandom OT and use it to prove lower bounds on p_C. We present undetectable cheating strategies available to Alice and Bob and analyze them to lower bound their cheating probabilities A_{OT} and B_{OT}, respectively. We show that, for protocols within this framework, it holds that

$$p_C = \max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\} \geq \tfrac{2}{3}. \tag{1}$$

Furthermore, if the states output to Bob by the protocol, when both parties are honest, are pure and symmetric, then

$$p_C = \max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\} \gtrsim 0.749. \tag{2}$$

We prove this by bounding Alice's and Bob's cheating probabilities with respect to a single parameter, F, which is related to the fidelity of the output states of the protocol when it is honestly executed. (When either of the parties are dishonest, the output states may naturally be different.) From this we find that there is always a trade-off; as Alice's ability to cheat decreases, Bob's ability increases, and vice versa.

For this special case of pure symmetric output states, our result can be improved, giving an increased lower bound on the cheating probabilities. For protocols with pure symmetric output states, this nearly closes the gap between the known lower bounds, and the upper bounds resulting from existing protocols. We note that all 1-2 OT protocols we have seen proposed have output states that are pure and symmetric. Although there is no reason why this must be the case in general, protocols would intuitively often have this property. As we later show, however, there exist protocols with lower average cheating probabilities than what is possible for protocols where the output states are pure and symmetric.

A. Protocol framework

We now describe the general framework for semirandom OT protocols with N rounds of communication between Alice and Bob. This framework is based on Kitaev's construction for strong coin flipping [4] and is useful for analyzing the security of semirandom OT. In Appendix A, we further motivate why this framework is general for semirandom OT.

1. Bob starts with the state ρ_{BM} and Alice starts with an auxiliary system A initialized to $|0\rangle\langle 0|_A$. The overall state is $\rho_{BMA} := \rho_{BM} \otimes |0\rangle\langle 0|_A$. We further suppose that Alice and Bob share the counter variable i, initialized to 1, which tracks the round number of the protocol.
2. Alice randomly selects an element $x_0x_1 \in \{00, 01, 11, 10\}$.
3. Bob sends system M to Alice.
4. Based on her choice in step 2, Alice performs the unitary operation $U_{MA}^{x_0x_1,i} \in \{U_{MA}^{00,i}, U_{MA}^{01,i}, U_{MA}^{11,i}, U_{MA}^{10,i}\}$.
5. Alice sends system M back to Bob.
6. Bob performs the unitary operation $V_{BM}^{(i)}$.
7. The index i is incremented by 1. If $i = N + 1$, the protocol proceeds to step 8; otherwise, it returns to step 3.
8. The final output held by Bob is

$$\sigma_{BM}^{x_0x_1} := \mathrm{Tr}_A(\eta_{BMA}^{x_0x_1}), \tag{3}$$

where

$$\eta_{BMA}^{x_0x_1} := V_{BM}^{(n)} U_{MA}^{x_0x_1,n} \cdots V_{BM}^{(1)} U_{MA}^{x_0x_1,1} \circ \rho_{BMA} \tag{4}$$

and we have used the convention that $U \circ \rho = U\rho\, U^\dagger$.

9. Bob performs a positive operator-valued measurement (POVM) with elements $\{\Pi_{BM}^{0*}, \Pi_{BM}^{1*}, \Pi_{BM}^{*0}, \Pi_{BM}^{*1}\}$ to obtain the value of c and x_c. The position of the asterisk "$*$" determines the value of c, i.e., $c = 0$ for $0*$ and $1*$, while $c = 1$ for $*0$ and $*1$. The value of the "nonasterisk" entry is the actual value of x_c. For example, the outcome Π_{BM}^{1*} denotes that $c = 0$ and $x_0 = 1$.

The steps of the framework above describe the actions of Alice and Bob if they are honest, together with the associated outputs, assuming that all measurements are deferred to the end. Of course, Alice's and Bob's actual actions may deviate from the honest protocol description if they are dishonest, but we will see that to obtain our lower bound, this framework is useful.

B. Alice and Bob both honest

For the protocol to be correct if both Alice and Bob are honest, we require the following conditions to hold:

$$\mathrm{Tr}(\Pi_{BM}^{j*}\sigma_{BM}^{kl}) = \begin{cases} \frac{1}{2} & \text{if } j = k, \\ 0 & \text{if } j \neq k. \end{cases} \quad \text{for } c = 0, \tag{5}$$

$$\mathrm{Tr}(\Pi_{BM}^{*j}\sigma_{BM}^{kl}) = \begin{cases} \frac{1}{2} & \text{if } j = l, \\ 0 & \text{if } j \neq l. \end{cases} \quad \text{for } c = 1. \tag{6}$$

These conditions imply that Bob receives either one of Alice's two chosen bits with equal probability and that the bit received by Bob is correct.

C. Security against Bob

We assume that Bob acts honestly throughout the protocol, until step 9, where he deviates in the final measurement. This is clearly not the most general way of cheating for Bob, but any cheating probability that Bob can achieve by cheating in this restricted way can also be achieved by an unrestricted Bob. We will therefore be able to derive a lower bound on Bob's general cheating probability. Bob, at the beginning of step 9 (measurement), then holds either σ_{BM}^{00}, σ_{BM}^{01}, σ_{BM}^{11}, or σ_{BM}^{10}. In order to cheat, Bob wants to guess the exact value of x_0 *and* x_1. That is, he wants to know which of the four σ states he holds. To do this, his optimal strategy would be to perform a minimum-error measurement. However, the minimum-error measurement will vary according to the states chosen by any specific

implementation of semirandom OT. Instead, to provide a lower bound on Bob's optimal cheating probability for *all* protocols described by the framework, we assume that Bob performs a square-root measurement (SRM) [30]. This may not be his optimal strategy, but it is a valid cheating strategy, and a strategy that Bob can employ without even being caught (since Alice has no way of knowing which measurement Bob performs). Bob's cheating probability is then at least as large as the success probability of the SRM, which is bounded as [31]

$$p_{\text{succ}}^{\text{SRM}} \geq 1 - \frac{1}{8} \sum_{jk \neq lm} F(\sigma_{BM}^{jk}, \sigma_{BM}^{lm}), \tag{7}$$

where $jk, lm \in \{00, 01, 11, 10\}$ and F is the fidelity, defined as

$$F(\rho, \sigma) := \text{Tr}\left(\sqrt{\rho^{1/2} \sigma \rho^{1/2}}\right). \tag{8}$$

Equations (5) and (6) imply that $F(\sigma_{BM}^{jk}, \sigma_{BM}^{j\oplus 1, k\oplus 1}) = 0$ (since these states can be perfectly distinguished). Without loss of generality, suppose that σ_{BM}^{00} and σ_{BM}^{01} are the pair of states with the highest fidelity. Define

$$F := F(\sigma_{BM}^{00}, \sigma_{BM}^{01}). \tag{9}$$

Then it follows that

$$B_{\text{OT}} \geq 1 - F. \tag{10}$$

This result is limited somewhat by the bound on the success probability of the SRM for general states given in Eq. (7). Placing restrictions on the output states of the protocol allows us to tighten this bound. In particular, if $\{\sigma_{BM}^{00}, \sigma_{BM}^{01}, \sigma_{BM}^{11}, \sigma_{BM}^{10}\}$ forms a symmetric set [32] of pure states for which $0 \leq F \leq \frac{1}{2}$ then, as we show in Appendix B, Bob's SRM is successful with probability [33]

$$\tilde{p}_{\text{succ}}^{\text{SRM}} \geq \tfrac{1}{4}\left(1 + \tfrac{1}{2}\sqrt{1 - 2F} + \tfrac{1}{2}\sqrt{1 + 2F}\right)^2, \tag{11}$$

which gives the tighter bound $B_{\text{OT}}^{\text{pure}} = \tilde{p}_{\text{succ}}^{\text{SRM}} \geq$ the rhs of Eq. (11). (As we will see below, $F > \frac{1}{2}$ would mean that Alice's cheating probability is greater than $\frac{3}{4}$.)

If Bob's ability to cheat does not depend on Alice's random choice of input, it seems likely that most protocols would output symmetric states, and this tighter bound would apply. However, the example protocol we present in Sec. IV, which uses symmetric pure states, can be combined with a trivial protocol, to obtain overall average cheating probabilities that are lower than the bound for protocols using symmetric pure states. This shows that, interestingly, protocols using symmetric pure states are not optimal for semirandom OT in general.

D. Security against Alice

Suppose that Alice is dishonest and aims to guess the value of the c output to Bob. In this section we present a cheating strategy that is always available to Alice, and which is always undetectable. We derive Alice's cheating probability given that she performs this specific strategy, and use this to obtain a lower bound for Alice's achievable cheating probability given that she performs some optimal strategy, in the same way we restricted Bob's attacks to obtain a lower bound for his cheating probability.

The strategy that Alice employs intuitively is the following. She chooses the two classical two-bit inputs that correspond to the pair of states among the σ_{BM}^{jk} with the highest fidelity, which we called F above. Then she performs the protocol operations corresponding to either classical input, conditioned on an ancillary qubit that is prepared in a superposition state, and that she keeps. In other words, the global state (before Bob's measurement) will be an entangled superposition, involving the pair of output states σ_{BM}^{jk} with the highest fidelity on Bob's side. Bob then makes the measurement he makes if honest. Conditioned on his outcome, Alice's ancillary qubit is prepared in one of two states. Alice can distinguish between the two states with a success probability determined by the fidelity F between the two states on Bob's side. (Her success probability is greater than $\frac{1}{2}$, which would correspond to a random guess by Alice.) This leads us to a bound on Alice's cheating probability that involves the same quantity F as our bound on Bob's cheating probability.

More specifically, Alice can proceed as follows. Let $|\Psi\rangle_{BMAE}$ be a purification of ρ_{BMA}, where E denotes the environment. Alice also prepares an additional state $|+\rangle_D = (|0\rangle_D + |1\rangle_D)/\sqrt{2}$ for use as a control qubit to perform her strategy. Since we consider information-theoretic security, Alice can do anything allowed within quantum mechanics, including this. The overall state is

$$\frac{1}{\sqrt{2}}(|\Psi\rangle_{BMAE}\,|0\rangle_D + |\Psi\rangle_{BMAE}\,|1\rangle_D), \tag{12}$$

with Alice in complete control of systems A, E, and D. Without loss of generality, we again assume that the two σ states with the highest fidelity are σ_{BM}^{00} and σ_{BM}^{01}. A valid cheating strategy available to Alice is as follows. In each step 4 of the protocol, rather than performing a unitary $U_{MA}^{x_0 x_1, i}$, Alice instead performs

$$U_{MA}^{00,i} \otimes |0\rangle\langle 0|_D + U_{MA}^{01,i} \otimes |1\rangle\langle 1|_D. \tag{13}$$

Defining Alice's overall operations as $\mathcal{U} = V_{BM}^{(N)} U_{MA}^{00,N} \cdots V_{BM}^{(1)} U_{MA}^{00,1}$ and $\mathcal{V} = V_{BM}^{(N)} U_{MA}^{01,N} \cdots V_{BM}^{(1)} U_{MA}^{01,1}$, Alice's strategy

leads to an output state

$$|\chi\rangle := \frac{1}{\sqrt{2}}(\mathcal{U}\,|\Psi\rangle_{BMAE}\,|0\rangle_D + \mathcal{V}\,|\Psi\rangle_{BMAE}\,|1\rangle_D)$$
$$:= \frac{1}{\sqrt{2}}(|\psi^{00}\rangle_{BMAE}\,|0\rangle_D + |\psi^{01}\rangle_{BMAE}\,|1\rangle_D). \quad (14)$$

This strategy is not detectable by Bob, since without access to system D it is as if Alice has performed the honest operations for either $x = 00$ or $x = 01$, each with probability $\frac{1}{2}$. The states $|\psi^{jk}\rangle$ are purifications of σ^{jk}_{BM}, and all purifications are related by a unitary operation acting on the purifying system alone. Alice further performs the unitary operation

$$W^{(1)}_{AE} \otimes |0\rangle\langle 0|_D + W^{(2)}_{AE} \otimes |0\rangle\langle 0|_D, \quad (15)$$

where $W^{(1)}_{AE}$ and $W^{(2)}_{AE}$ are chosen to transform $|\psi^{00}\rangle$ and $|\psi^{01}\rangle$ into $|\phi^{00}\rangle$ and $|\phi^{01}\rangle$, such that the latter two states are the purifications of σ^{00}_{BM} and σ^{01}_{BM} with the highest overlap. This operation is performed so that we can later use Uhlmann's theorem to express Alice's cheating probability in terms of F, as we shall see. The resulting state is

$$|\Phi\rangle := \frac{1}{\sqrt{2}}(|\phi^{00}\rangle_{BMAE}\,|0\rangle_D + |\phi^{01}\rangle_{BMAE}\,|1\rangle_D). \quad (16)$$

In step 8 of the protocol, Bob performs the POVM $\{\Pi^z_{BM}\}_z$ on $|\Phi\rangle$, where $z \in \{0*, 1*, *0, *1\}$. Our aim is to discover how well Alice can distinguish between the outcomes $c = 0$ and $c = 1$ using a measurement on her D system. The state of system D following Bob's POVM is

$$\mu_D = \frac{1}{2}\sum_{i,j,z} \langle\phi^{0i}|\,\Pi^z_{MB}\,|\phi^{0j}\rangle\,|j\rangle\,\langle i|_D\,, \quad (17)$$

where $i, j \in \{0, 1\}$, $z \in \{0*, 1*, *0, *1\}$.

Equations (5) and (6) can be used to evaluate terms of the form $\langle\phi^{jk}|\Pi^z_{BM}|\phi^{jk}\rangle$, since

$$\langle\phi^{jk}|\Pi^z_{BM}|\phi^{jk}\rangle = \mathrm{Tr}_{BMAE}(\Pi^z_{BM}|\varphi^{jk}\rangle\langle\varphi^{jk}|)$$
$$= \mathrm{Tr}_{BM}(\Pi^z_{BM}\sigma^{jk}_{BM}). \quad (18)$$

The expression for μ_D can be further simplified using the following lemma.

Lemma 1. *For all values of $z \in \{0*, 1*, *0, *1\}$ and $jk \in \{00, 01, 11, 10\}$ such that $Tr_{BM}(\Pi^z_{BM}\sigma^{jk}_{BM}) = 0$, it holds that*

$$(\Pi^z_{BM} \otimes \mathbb{1}_{AE})\,|\phi^{jk}\rangle_{BMAE} = 0. \quad (19)$$

Proof. Since $\Pi^z_{BM} \otimes \mathbb{1}_{AE}$ is a positive semidefinite operator, we can write its spectral decomposition as

$$\Pi^z_{BM} \otimes \mathbb{1}_{AE} = \sum_n c_n \rho c_n, \quad (20)$$

where the c_n are positive real numbers. Therefore, using Eq. (18),

$$\mathrm{Tr}_{BM}(\Pi^z_{BM}\sigma^{jk}_{BM}) = 0 \implies \langle\phi^{jk}|\Pi^z_{BM} \otimes \mathbb{1}_{AE}|\phi^{jk}\rangle = 0$$
$$\implies \langle c_i|\phi^{jk}\rangle = 0 \quad \text{for all } i, \quad (21)$$

and the result follows. ∎

Using this lemma, μ_D simplifies to

$$\mu_D = \tfrac{1}{2}\big[\tfrac{1}{2}|0\rangle\langle 0|_D + \langle\phi^{01}|\Pi^{0*}_{MB}|\phi^{00}\rangle|0\rangle\langle 1|_D$$
$$+ \langle\phi^{00}|\Pi^{0*}_{MB}|\phi^{01}\rangle|1\rangle\langle 0|_D + \tfrac{1}{2}|1\rangle\langle 1|_D\big]$$
$$+ \tfrac{1}{2}\big[\tfrac{1}{2}|0\rangle\langle 0|_D + \tfrac{1}{2}|1\rangle\langle 1|_D\big]$$
$$= \tfrac{1}{2}\mu_D^{c=0} + \tfrac{1}{2}\mu_D^{c=1}, \quad (22)$$

where the first square bracket corresponds to Bob obtaining an outcome $c = 0$ (i.e., Π^{0*} or Π^{1*}) and the second square bracket corresponds to Bob obtaining an outcome $c = 1$ (i.e., Π^{*0} or Π^{*1}). Lastly, we must evaluate $\langle\phi^{01}|\Pi^{0*}_{MB}|\phi^{00}\rangle$.

To satisfy no signaling, the density matrix in system D must be the same regardless of whether or not Bob actually performs his measurement [34–38]. If Bob performs no measurement, using Eq. (16), the state of system D is

$$\tfrac{1}{2}[|0\rangle\langle 0|_D + \langle\phi^{01}|\phi^{00}\rangle|0\rangle\langle 1|_D$$
$$+ \langle\phi^{00}|\phi^{01}\rangle|1\rangle\langle 0|_D + |1\rangle\langle 1|_D]. \quad (23)$$

Comparing Eqs. (22) and (23), we must have $\langle\phi^{01}|\Pi^{0*}_{MB}|\phi^{00}\rangle = \langle\phi^{01}|\phi^{00}\rangle$. The trace distance between $\mu_D^{c=0}$ and $\mu_D^{c=1}$ is therefore $|\langle\phi^{01}|\phi^{00}\rangle|$, meaning that Alice can distinguish $c = 0$ from $c = 1$ with probability

$$p = \tfrac{1}{2}(1 + |\langle\phi^{01}|\phi^{00}\rangle|)$$
$$= \tfrac{1}{2}[1 + F(\sigma^{00}_{BM}, \sigma^{01}_{BM})]$$
$$:= \tfrac{1}{2}(1 + F), \quad (24)$$

where the second equality follows from Uhlmann's theorem [39] since $|\phi^{00}\rangle$ and $|\phi^{01}\rangle$ are the purifications of σ^{00}_{BM} and σ^{01}_{BM} with maximum overlap. It therefore holds that

$$A_{\mathrm{OT}} \geq \tfrac{1}{2}(1 + F). \quad (25)$$

E. Result

Previously, the best known lower bound for the cheating probabilities in 1-2 quantum OT was [22]

$$\max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\} \geq \tfrac{2}{3}. \tag{26}$$

Our results in the previous section reproduce this bound since

$$\begin{aligned} A_{\mathrm{OT}} \geq \tfrac{1}{2}(1+F) \quad \text{and} \quad B_{\mathrm{OT}} \geq 1-F \\ \implies \quad \min_F(\max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\}) = \tfrac{2}{3}. \end{aligned} \tag{27}$$

Our way to obtain this bound differs substantially from Ref. [22] in two ways, and this means (as we show later) that, when imposing further restrictions on the class of protocols, we can increase the lower bound.

If we consider protocols where the output states, during an honest execution, are pure and symmetric, then we obtain a tighter lower bound (which cannot be obtained using the technique in Ref. [22]). Specifically, we can use Eq. (11) to obtain the tighter bound

$$\min_F(\max\{A_{\mathrm{OT}}, B_{\mathrm{OT}}\}) \approx 0.749. \tag{28}$$

Protocols using symmetric states may be preferable due to theoretical or experimental simplicity, and, intuitively, one might expect optimal protocols to employ symmetric states.

Finally, another important feature of our bounding method is that our construction quantifies the trade-offs possible between A_{OT} and B_{OT}, something of importance for applications where one is more interested in a smaller value for one of the two. This exact situation arises in the context of quantum signatures [25], where, in the distribution stage, signing keys are partially distributed in a manner reminiscent of 1-2 OT. In these protocols A_{OT} is prioritized, and it is important that $A_{\mathrm{OT}} \approx 0.5$ to protect against repudiation attempts. On the other hand, to protect against forging attempts is much simpler, and the requirements on B_{OT} are less strict. The parametrization of A_{OT} in terms of F suggests that in order to create an imperfect 1-2 OT schemes with a small ϵ_A, it is necessary to have a protocol that, in the honest case, outputs states that are almost orthogonal. Unfortunately, given $A_{\mathrm{OT}} \approx 0.5$, our results show that it is necessary to have $B_{\mathrm{OT}} \approx 1$. This mirrors a similar result for two-party computation [40].

IV. A PROTOCOL FOR OBLIVIOUS TRANSFER

In this section we present a protocol for imperfect quantum oblivious transfer that achieves cheating probabilities of $\frac{3}{4}$ and approximately 0.729 for sender and receiver, respectively. The protocol uses unambiguous quantum state elimination.

A. Unambiguous measurements

Suppose that a quantum system is prepared in one of the states ρ^x, where $x \in \mathcal{X}$, with prior probabilities p_x. When retrieving the information stored in ρ^x using an "optimal" measurement, what is "optimal" depends heavily on the application. For communication protocols, a minimum-error measurement—one that identifies the state with the smallest probability of error—is just one possibility. For cryptographic protocols, the optimal measurement is often one that returns the largest possible amount of information while simultaneously disturbing the system less than a threshold amount.

A particular class of measurements we are interested in is unambiguous measurements. These measurements give "perfect" information in the sense that, given a successful measurement outcome, one can be certain that the decoded classical information is correct. Unambiguous measurements come in two main flavors: unambiguous state discrimination (USD), and unambiguous state elimination (USE). A successful USD measurement on ρ^x would identify x with certainty, but the measurement is generally not successful with probability 1. When the measurement is unsuccessful, it does not uniquely determine the state.

USE measurements [41–49] on the other hand can more often be successful with probability 1, but only guarantee that $x \notin \mathcal{Y} \subset \mathcal{X}$, i.e., the measurement rules out states rather than definitively identifying the state. Intuitively, it seems that unambiguous measurements are well suited to cryptographic applications—their ability to provide "perfect yet partial" information on the states being sent is often exactly what is needed. More concretely, USD can be seen as very similar to Rabin OT, in which it is desired that the receiver obtains the sender's message with probability $\frac{1}{2}$, and otherwise receives nothing with probability $\frac{1}{2}$. On the other hand, USE measurements seem closely related to the more common 1-2 OT, in which incomplete but correct information is gained with certainty. Since OT plays a central role in secure two-party computation, it seems likely that unambiguous measurements could also play a role in this developing field.

B. Semirandom OT using unambiguous state elimination

In this section, we present an application of USE measurements. We describe a protocol for implementing many runs of semirandom OT and analyze its security in the asymptotic limit. We again work in the information-theoretic security setting but this time prove *upper* bounds on the cheating probabilities achievable for Alice and Bob. We show that our protocol performs better than previous protocols, and is almost optimal with respect to the bounds for symmetric pure states derived in the previous section. The protocol proceeds as follows.

1. Alice uniformly, randomly, and independently selects $\mathcal{N}$ elements from the set $\mathcal{X} = \{00, 01, 11, 10\}$. She encodes elements as $00 \to |00\rangle$, $01 \to |++\rangle$, $11 \to |11\rangle$, and $10 \to |--\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.
2. Alice sends the $\mathcal{N}$ two-qubit states to Bob.
3. Bob randomly selects $\sqrt{\mathcal{N}}$ out of the $\mathcal{N}$ states he has received and asks Alice to reveal their identity [50]. If Alice declares $|++\rangle$ or $|--\rangle$, then Bob measures both qubits in the X basis; otherwise, he measures both qubits in the Z basis. The protocol aborts if any measurement result does not match Alice's declaration.
4. The $\sqrt{\mathcal{N}}$ states used in the previous step are discarded.
5. For each of the $\mathcal{N} - \sqrt{\mathcal{N}}$ remaining states, Bob measures the first qubit in the Z basis and the second qubit in the X basis. These measurements constitute two USE measurements (for example, an outcome of $|0\rangle$ on the first qubit rules out $|11\rangle$). Following these measurements, Bob can with certainty rule out one element from the set $\mathcal{Y}_0 = \{00, 11\}$ and one from the set $\mathcal{Y}_1 = \{01, 10\}$. In this way, for each of the remaining states, he can know with certainty exactly one of x_0 and x_1, but not both.

The result of this protocol is that Alice and Bob have performed $\mathcal{N} - \sqrt{\mathcal{N}}$ runs of semirandom OT, each of which could be used to implement a single instance of 1-2 OT, as per the construction in Appendix A. Below we analyze the cheating probabilities achieved by each instance of semirandom OT generated by this protocol.

At this point it is important to note that in our analysis we assume that *all* $\sqrt{\mathcal{N}}$ tests have passed successfully. This is important to simplify the subsequent analysis, by restricting to "undetectable" strategies, as we explain below. It is worth noting, however, that in realistic scenarios, even honest parties would fail some tests due to imperfections and noise. Therefore, an important further work is to weaken the condition to allow for a small fraction of tests to fail, in order to make our protocol robust. This involves bounding the trace distance of the resulting states as a function of the (small) failure of tests, and is postponed for a future publication.

Note that, from a security perspective, the protocol given above can be set in the general framework considered of the previous section by defining $U = R \otimes R$, where

$$R = |+\rangle\langle 0| - |-\rangle\langle 1|. \tag{29}$$

Alice begins with the state $|00\rangle$ and applies either $\mathbb{1}$, U, U^2, or U^3 to obtain either $|00\rangle$, $|++\rangle$, $|11\rangle$, or $|--\rangle$, respectively. The subsequent rounds simply consist of classical communication and measurements, the latter of which can be described as a unitary operation acting on a larger Hilbert space, with state collapse delayed until a protocol output is required. We show that this protocol can be made secure with $A_{\mathrm{OT}} = 0.75$ and $B_{\mathrm{OT}} \approx 0.729$.

C. Security against Bob

If Bob wants to cheat then his aim is to correctly guess both x_0 and x_1 for each individual pair. In the asymptotic limit, the fraction of states discarded for testing in step 3 tends to 0. Since the states are prepared independently, any strategy Bob performs (including general measurements correlated across all $\mathcal{N}$ states) cannot have an *average* success probability (probability of correctly identifying both x_0 and x_1) that is greater than the minimum-error measurement on a single state [51]. Therefore, in the asymptotic limit we can bound Bob's average cheating probability for each of the $\mathcal{N} - \sqrt{\mathcal{N}} \approx \mathcal{N}$ runs by considering the minimum-error measurement on a single state. Since the set $S := \{|00\rangle, |++\rangle, |11\rangle, |--\rangle\}$ forms a set of symmetric pure states, the minimum-error measurement is the SRM [33]. Using this measurement, Bob can guess both of Alice's input bits with probability

$$B_{\mathrm{OT}} = \frac{1}{4}\left(1 + \frac{1}{\sqrt{2}}\right)^2 \approx 0.729. \tag{30}$$

In this case, Bob's optimal strategy is the exact strategy considered in the general scenario in Sec. III C. (If the tested fraction of states does not tend to 0 as $\mathcal{N} \to \infty$ then Bob's optimal measurement would be a maximum confidence measurement [38,52], with a success probability increasing with the fraction of tested states, reaching a maximum of $\frac{3}{4}$ if at least $\frac{1}{4}$ of the states are tested. Bob would then perform the relevant measurement with higher confidence in the result, and if the measurement fails, ask to "test" the state in that position.)

D. Security against Alice

If Alice wants to cheat, her aim is to correctly guess the value of c such that Bob received x_c. To do this, she may send states other than those in S. In general, Alice will generate $\rho_{AB_{11}B_{12}B_{21}B_{22}\cdots B_{N1}B_{N2}}$ and send the B systems to Bob, keeping the A system for herself. In step 3 of the protocol Bob then randomly selects a pair of the qubits he received, say $\rho_{B_{k1}B_{k2}}$, and asks Alice to declare the identity of the state. He does this for $\sqrt{\mathcal{N}}$ of the $\mathcal{N}$ pairs. Since we are looking for an upper bound on Alice's capabilities, we assume that she holds a purification $|\Psi\rangle_{B_{k1}B_{k2}A}$ of $\rho_{B_{k1}B_{k2}}$.

Alice must declare a state to Bob that will agree with his measurement outcomes in step 3. If she can do this with

certainty then the state $|\Psi\rangle_{B_{k1}B_{k2}A}$ must be of the form

$$|\Psi\rangle_{B_{k1}B_{k2}A} = b_0|00\rangle_{B_{k1}B_{k2}}|0\rangle_A + b_1|++\rangle_{B_{k1}B_{k2}}|1\rangle_A + b_2|11\rangle_{B_{k1}B_{k2}}|2\rangle_A + b_3|--\rangle_{B_{k1}B_{k2}}|3\rangle_A, \tag{31}$$

where $\{|0\rangle_A, |1\rangle_A, |2\rangle_A, |3\rangle_A\}$ is an orthonormal basis. If Alice does not send states in the above form then she cannot guess Bob's measurement outcomes with certainty, and for asymptotically large $\mathcal{N}$, it becomes virtually certain that the protocol will abort.

We note that Alice also cannot improve her average cheating probability by using strategies where she uses entanglement not just between the system she keeps and Bob's individual qubit pairs, but where she also introduces entanglement between the different qubit pairs she sends to Bob. Any state for which Alice will deterministically pass a test on the qubits in position $B_{k1}B_{k2}$, can be written as

$$|\Psi\rangle_{B_{k1}B_{k2}A'} = b_0|00\rangle_{B_{k1}B_{k2}}|0\rangle_{A'} + b_1|++\rangle_{B_{k1}B_{k2}}|1\rangle_{A'} + b_2|11\rangle_{B_{k1}B_{k2}}|2\rangle_{A'} + b_3|--\rangle_{B_{k1}B_{k2}}|3\rangle_{A'}, \tag{32}$$

where $\{|0\rangle_{A'}, |1\rangle_{A'}, |2\rangle_{A'}, |3\rangle_{A'}\}$ is an orthonormal basis that may include not just a system Alice holds, but Bob's qubits in other positions than $B_{k1}B_{k2}$. This state is evidently of the form in Eq. (31). That is, if Alice is able to deterministically pass a test done on a qubit pair then this directly limits her average cheating probability for that qubit pair, and this is true for all qubit pairs also when Alice can entangle the qubits she sends to Bob in arbitrary ways.

Essentially, this means that Alice is restricted to the attacks considered in the general protocol analysis in Sec. III D—attacks that are superpositions of honest operations, and as such, are always undetectable by Bob. In fact, it can be proven (see Appendix C) that an optimal strategy for Alice is to prepare

$$\frac{1}{\sqrt{2}}(|00\rangle_B|0\rangle_A + |++\rangle_B|1\rangle_A), \tag{33}$$

which corresponds exactly to the operation given in Eq. (13). Since the overlap between all adjacent states in S is $\frac{1}{2}$, Eq. (25) implies that Alice can correctly guess the value of c with probability $\frac{3}{4}$. The analysis in Appendix C confirms that this is her cheating probability.

E. A combined protocol with lower average cheating probability

One can combine our example scheme, where $A_{\mathrm{OT}} = \frac{3}{4}$ and $B_{\mathrm{OT}} = 0.729$, with a "trivial" scheme where $A_{\mathrm{OT}} = \frac{1}{2}$ and $B_{\mathrm{OT}} = 1$, to achieve a scheme where both Alice's and Bob's average cheating probabilities are below $\frac{3}{4}$. Note that this is possible because our protocol had different cheating probabilities for sender and receiver. This illustrates that the maximum of the two cheating probabilities does not fully characterize the performance of a protocol, since the smaller cheating probability can become relevant in such combined protocols. As in Ref. [22], Alice and Bob execute a weak coin flipping protocol to probabilistically choose between a protocol that is more favorable to Alice, and one that is more favorable to Bob. In Ref. [22], it is considered in some detail how to securely compose weak coin flipping and a subsequent OT protocol. In the trivial OT scheme we use, Alice simply sends Bob both bits, and Bob reads the bit he wants and discards the other, giving $A_{\mathrm{OT}} = \frac{1}{2}$ and $B_{\mathrm{OT}} = 1$. If our example scheme is chosen with probability p and the trivial scheme chosen with probability $1-p$, the average cheating probabilities become

$$\tilde{A}_{\mathrm{OT}} = 3p/4 + (1-p)/2, \qquad \tilde{B}_{\mathrm{OT}} = 0.729p + (1-p). \tag{34}$$

Choosing p to set these equal results in a combined scheme where both Alice and Bob can cheat on average at most with probability $\tilde{A}_{\mathrm{OT}} = \tilde{B}_{\mathrm{OT}} = p_C \approx 0.74$. This is the smallest cheating probability that a concrete protocol can achieve to our knowledge. Interestingly, this is lower than 0.749 both for Alice and Bob, thus proving that protocols using symmetric pure states are not optimal for semirandom oblivious transfer in terms of the average cheating probability.

V. EXPERIMENT

A major advantage of the above protocol is that it can be realized using a standard BB84 quantum key distribution setup [53]. However, we implement the semirandom OT protocol slightly differently to also enable the realization of optimal cheating strategies. Namely, we created Alice's entangled state with the help of optical multiqubit quantum logic gates. But still one photon carrying a single qubit stays at Alice's side and the other photon carrying two qubits travels to Bob's side.

A. Experimental setup

Pairs of 810-nm time-correlated photons are generated using type-II spontaneous parametric down-conversion in a β-barium-borate crystal. The photons are guided to the experimental setup depicted in Fig. 1(a). Primarily, the state of the first of the qubits B chosen by Alice is encoded by quarter- and half-wave plates (QWP, HWP) into the polarization of the signal photon. Then a calcite beam displacer (BD) spatially separated horizontally and vertically polarized components into two parallel beams with a lateral distance of 4 mm. This turns the encoding of the first qubit from polarization to spatial encoding. Wave plates

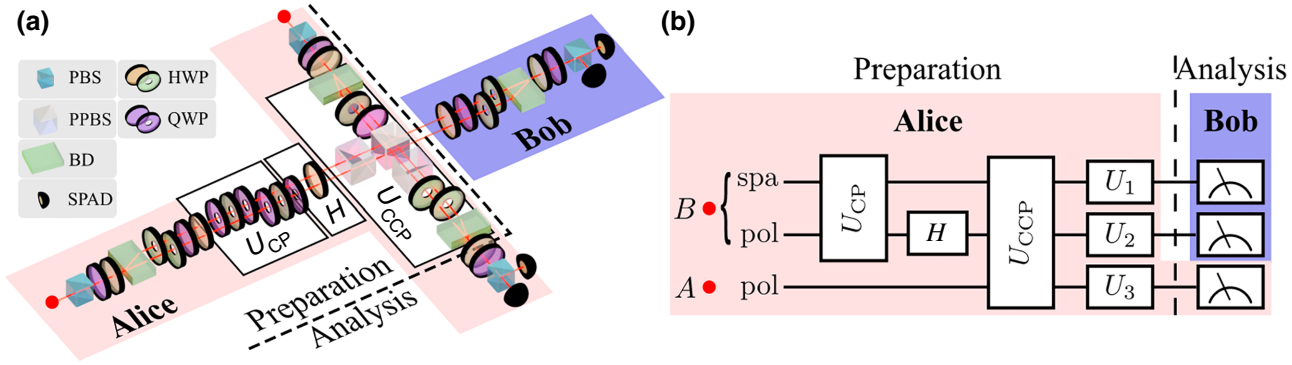

FIG. 1. (a) Experimental setup. (b) Quantum circuit diagram of the experiment. With appropriate tuning of the controlled-phase gates U_{CP}, U_{CCP} and the single-qubit gates $U_{1,2,3}$, Alice prepares the required state (spa and pol denote qubits encoded into spatial and polarization modes respectively).

acting on both parallel beams are then used to encode the state of the second qubit B into polarization. In this way, a single photon carried both qubits.

When the basic operation of the semirandom OT is tested, as well as when Bob's cheating strategy is implemented, we utilize the idler photon (the other photon in the pair) only to herald successful generation of the signal photon. When Alice's cheating strategy is studied, the state of Alice's qubit A is encoded into the polarization state of the idler photon. Linear-optical quantum logic gates, shown in Fig. 1(b), then entangle the input qubits to produce the required state (33).

The two-qubit controlled-phase gate (U_{CP}) operates on qubits B and introduces an arbitrary phase shift on state $|11\rangle$. The wave plates in the lower optical path perform the phase shift, the wave plates in the upper path only compensate for the path length difference. Another half-wave plate implements the Hadamard gate acting on the second one of qubits B (encoded in the polarization degree of freedom). The three-qubit controlled-controlled-phase gate (U_{CCP}) provides a way to entangle qubit A with qubits B. The beam displacer separates the path of the idler photon according to its polarization into two parallel beams with 6-mm spacing. This extends the Hilbert space, providing room for manipulation. Suitable polarization operations, two-photon interference, and consecutive coincident detection then constitute the U_{CCP} operation. The two-photon interference takes place in the central block of three partially polarizing beam splitters (PPBSs), the central one with reflectances $R_H = 0, R_V = \frac{2}{3}$, the other two with $R_H = \frac{2}{3}, R_V = 0$. This is the core of the gate operation [54–57], which is explained in detail in the Methods section of our previous work [58]. The gate is probabilistic and succeeds with theoretical probability $\frac{1}{9}$ for phase shifts 0 and π, which are used in the experiment.

Final projective measurements are realized by wave plates, polarizing beam splitters, and single-photon avalanche diodes (SPADs). This enables projection onto an arbitrary product state [59]. Electric signals are processed by coincidence logic. The overall coincidence count rate is roughly 330 counts per second. The experimental integration time is 5 s for each projective-measurement setting.

B. Both parties are honest

To test the case when both parties are honest, we set the U_{CP} and U_{CCP} gates to zero phase shift and turn off the Hadamard operation H.

We sequentially prepare states $|00\rangle, |++\rangle, |--\rangle, |11\rangle$ and measure each of them in the ZX basis on Bob's side. The probability of Bob correctly receiving one of Alice's bits is estimated to be 0.9943(9), where the number in the brackets represents one standard deviation at the final decimal place. It means that, due to experimental imperfections, there is a small probability (about 0.6%) that Bob obtains an erroneous bit value. Complete experimental data are provided in Table IV of Appendix E.

The protocol also includes test measurements. If the parties are honest, this means that the states $|00\rangle$, $|11\rangle$ are measured in the ZZ basis and states $|++\rangle, |--\rangle$ in the XX basis. Such measurements should unambiguously discriminate between the incoming states and Bob should never abort the protocol when Alice is honest. But in an experimental implementation imperfections may cause errors. In our experiment, the average error probability is 0.013(1). All measured data are provided in Table V of Appendix E.

C. Bob is cheating

Bob's optimal cheating strategy is to perform a minimum-error measurement [60]. In our case, this means measuring the first qubit in the basis

$$\{|\zeta_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, |\zeta_1\rangle = \beta\,|0\rangle - \alpha\,|1\rangle\}$$

and the other in the basis

$$\{|\xi_0\rangle = \alpha\,|0\rangle - \beta\,|1\rangle\,, |\xi_1\rangle = \beta\,|0\rangle + \alpha\,|1\rangle\}$$

with $\alpha = \cos(\pi/8)$ and $\beta = \sin(\pi/8)$. Each combination of detector clicks gives Bob a guess of both Alice's bits. The average experimental value of the cheating probability, i.e., the probability of a correct guess of both bits, is 0.718(5), which is close to the theoretical value of 0.729. Recorded counts are provided in Table VI of Appendix E.

D. Alice is cheating

To test Alice's optimal cheating strategy, we set the phase shifts of the gates U_{CP} and U_{CCP} to -138.2° and 180°, respectively. We prepare the input qubits in a suitable product state and adjust the output single-qubit operations $U_{1,2,3}$ to achieve the desired entangled state (33). The specific choice of input states, gate parameters, and unitary operations is a result of numerical optimization, which is discussed in Appendix D.

In order to verify the prepared entangled state, we perform quantum state tomography [61]. The purity of the state is $P = 0.884$ and its fidelity with respect to the ideal state (33) is $F = 0.921$. The cause of imperfect purity and fidelity is the sensitivity of the U_{CCP} gate to interferometric phase instability and spatiotemporal misalignment of the photons. Imperfect wave-plate retardances reduce the quality of the state even further.

To determine which bit is obtained by Bob, Alice measures her qubit A in state (33) in the X basis. Honest Bob makes his measurements according to the protocol. As described above, Bob's outcomes $|0+\rangle_B\,, |1-\rangle_B$ correspond to $c = 0$ and $|1+\rangle_B\,, |0-\rangle_B$ correspond to $c = 1$. If Alice obtains $|+\rangle_A$ ($|-\rangle_A$) then she guesses that $c = 0$ ($c = 1$). Alice's measurements in the X basis and Bob's measurements in the ZX basis are already contained in the data from the three-qubit state tomography. We estimate the cheating probability as the number of detection events in which Bob and Alice obtain the same value of c, divided by the number of all detection events. Alice correctly estimated Bob's bit c with probability 0.77(1). The measured count rates are given in Table VII in Appendix E.

In the case of test measurements, Bob measures in the ZZ or the XX basis and Alice in the Z basis. These data are also obtainable from the tomographic measurement. In theory, Bob should not be able to detect this type of cheating strategy by Alice. But in the experiment, there is a small fraction of outcomes telling Bob to abort the protocol, on average 0.059(6). This fraction is calculated as the number of counts in which Bob's measurement outcome does not match Alice's declaration divided by the total number of counts. The relevant data are presented in Table VIII of Appendix E.

In our experiment, Alice's probability of making a correct guess, 0.77, is higher than the theoretical limit 0.75. But there is also a relatively high probability of Bob discovering her cheating (0.059, which is higher than the probability of "false alarm," 0.013, if Alice is honest). These effects are likely caused by imperfect preparation of the state (33).

VI. DISCUSSION

In this paper we introduce semirandom OT and a general framework useful for its study. We explicitly construct undetectable cheating strategies available to Alice and Bob and use them to lower bound the cheating probability for any semirandom OT protocol within our framework. The derived bounds are directly transferable to standard 1-2 quantum OT, allowing us to obtain the lower bound $p_C \geq \frac{2}{3}$, but using different assumptions on cheating strategies than assuming semihonest adversaries as done by Chailloux *et al.* [22]. Our technique, other than rederiving the previous bound, allows us to (i) quantify the trade-off between cheating probabilities for different parties, which can be useful for applications where limiting cheating by one party is prioritized, and (ii) obtain tighter bounds if we impose further restrictions. In particular, if the states used by honest parties are pure and symmetric, we obtain the bound $p_C \geq 0.749$, which was not obtained previously.

Our construction provides a simple quantitative relationship between Alice's and Bob's ability to cheat, and gives new bounds in biased settings. In applications more sensitive to sender dishonesty than receiver dishonesty (or vice versa), our parametrization of A_{OT} and B_{OT} in terms of the fidelity shows explicitly how reductions in one party's ability to cheat will impact the other's cheating probability. To illustrate our construction, we present an OT protocol using unambiguous state elimination measurements to achieve cheating probabilities $A_{\mathrm{OT}} = \frac{3}{4}$, $B_{\mathrm{OT}} \approx 0.729$ and, therefore, $p_C = \frac{3}{4}$, together with its experimental realization. The cheating probabilities compare favorably with the previously best-known protocol given in Ref. [23] in which $A_{\mathrm{OT}} = B_{\mathrm{OT}} = \frac{3}{4}$. Unlike for the qutrit protocol proposed in Ref. [23], in our example protocol, the bound on Alice's cheating probability concerns her average cheating probability. On the other hand, Bob's cheating probability is lower (0.729 against 0.75 in Ref. [23]), and above all, our protocol does not require entanglement and can be realized using the same experimental components as BB84 quantum key distribution. A minor modification could render our protocol even more practical. Bob could, before asking Alice to reveal any states, randomly select some qubit pairs and measure them in the same basis, either the X or the Z basis. He then asks Alice to receive these states, but only after he has measured these qubit pairs. If Alice's declaration does not match his measurement results, he again aborts. Bob's test is then only useful if his selected basis matches the basis states used by Alice. Another variation would be for Bob to randomly select

which qubit he measured in the X basis and which in the Z basis. This makes no difference if Alice is limited to using undetectable cheating strategies, but would lead to somewhat improved performance when loss and imperfections are present and in finite-size scenarios, where Alice may choose to employ a cheating strategy that could be detected by Bob with some probability.

Since our example protocol outputs symmetric pure states, the cheating probabilities achieved are almost tight with the bounds proven in this paper for this class of protocols. Combining the example protocol with a trivial protocol, however, an average cheating probability $p_C \approx 0.74$ for both Alice and Bob is possible. It follows that protocols with pure and symmetric output states are not optimal. There thus remains a gap between the known lower bounds on cheating probabilities for quantum oblivious transfer, and what the lowest achievable cheating probabilities are.

We further note that if two protocols are combined using weak coin flipping then the parties know which protocol actually got implemented. The bound on cheating probabilities in such combined protocols are therefore also only bounds on average cheating probabilities. For an individual round, the parties are aware that they have higher or lower cheating probabilities. Related to this, cheating probabilities do not fully capture how certain a cheating party can be that the extra information they have dishonestly obtained is correct. In our example protocol, Bob can never be certain that his dishonestly obtained information is correct. He only ever knows that his guess is correct with probability 0.729. Alice, however, can be certain of Bob's bit choice with probability $\frac{1}{4}$, and she knows when this occurs. The rest of the time her guess is right with probability $\frac{2}{3}$. This is a further advantage of our protocol, compared with the one in Ref. [23]. To elaborate, if one probabilistically chooses between a trivial protocol where Alice can cheat perfectly and Bob cannot cheat at all ($A_{\mathrm{OT}} = 1$ and $B_{\mathrm{OT}} = \frac{1}{2}$) and a trivial protocol where Alice cannot cheat at all and Bob can cheat perfectly ($A_{\mathrm{OT}} = \frac{1}{2}$ and $B_{\mathrm{OT}} = 1$), then the average cheating probabilities for either party are $\frac{3}{4}$, but with probability $\frac{1}{2}$, either party knows for sure that they can cheat perfectly. When executing the protocol in Ref. [23], Alice similarly knows for sure what Bob's bit choice was half the time, and the rest of the time she randomly guesses. In our protocol, Alice is only sure with probability $\frac{1}{4}$. Bob, however, cheats with a minimum-error measurement both in our protocol and the one in Ref. [23], and is never sure that his guess is correct. Since the states Bob receives in both protocols are linearly dependent, he can never unambiguously determine both of Alice's bit values. We also present an optical realization of our protocol. The achieved experimental performance parameters agree well with the theoretical values, showing that the protocol is feasible.

As a final point, we note that in quantum cryptography, it is often easier to analyze so-called individual, identically distributed (i.i.d.) cheating strategies, where dishonest parties are restricted to act individually on each quantum system transmitted (or to act individually on other relevant "units" in the protocol), and where they act in the same way for each transmitted quantum system. If the parties can use cheating strategies that operate jointly on several transmitted quantum systems, sometimes called "coherent" cheating strategies, then cheating probabilities might increase. It is therefore worth emphasizing that the results we obtain are in fact valid for general cheating strategies, not just i.i.d. cheating strategies. First, note that the bounds we derive are lower bounds for cheating probabilities, and are therefore immediately valid for all cheating strategies, including joint or coherent cheating strategies by either party. Second, in the example protocol, we do not need to restrict either Alice or Bob to i.i.d. cheating strategies. As for Alice, in connection with Eq. (32), we explain why she does not benefit from entanglement with other positions. That is, we are allowing her joint cheating strategies, and show that this does not increase her ability to predict Bob's output for each instance of OT. However, it should be pointed out that this results from the fact that we make the simplifying assumption that Alice needs to pass Bob's tests with unit probability. If this assumption is not made then the analysis of whether joint or coherent strategies can help Alice cheat is less straightforward. If Alice is allowed to fail Bob's tests with some probability then she can use a state that slightly deviates from the state in Eqs. (31) and (32), and a more careful analysis of i.i.d. versus joint or coherent cheating strategies for Alice would be required. Bob, on the other hand, needs to maximize his average probability to correctly guess both of Alice's bits. His optimal cheating probability is obtained by individual minimum-error measurements on each qubit pair. Joint measurements on more than one qubit pair do not help him, and there is no need to restrict Bob to i.i.d. cheating strategies in the finite-size scenario either.

ACKNOWLEDGMENTS

The authors would like to thank J. Sikora and I. Kerenidis for helpful discussions. This work is supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grants No. EP/T001011/1, No. EP/T001062/1, and No. EP/M013472/1. R.A. gratefully acknowledges EPSRC studentship funding under Grant No. EP/I007002/1. R.S., M.M., L.M., and M.D. acknowledge support by Palacký University under Grant No. IGA-PrF-2020-009.

APPENDIX A: EQUIVALENCE BETWEEN SEMI-RANDOM OT, OT, AND RANDOM OT

Here we prove the following claim contained in the main text.

Proposition 1. *The existence of a semirandom OT protocol with cheating probabilities A_{OT} and B_{OT} is equivalent to the existence of a* 1-2 *quantum OT protocol with the same cheating probabilities.*

To prove this, we begin by giving the definition of a related OT variant called random OT (ROT), as follows.

Definition 3. *Random OT is a protocol between two parties, Alice and Bob, such that the following statements hold.*

(a) Alice outputs two bits $(x_0, x_1) \in \{0,1\}$ or abort.
(b) Bob outputs two bits (c, y) or abort.
(c) If Alice and Bob are honest, they never abort, $y = x_c$, Alice has no information about c, and Bob has no information about $x_{c\oplus 1}$. Furthermore, x_0, x_1, and c are uniformly random bits.
(d) $A_{OT} := \sup\{Pr[\text{Alice correctly guesses } c \wedge \text{Bob does not abort}]\} = \frac{1}{2} + \epsilon_A$.
(e) $B_{OT} := \sup\{Pr[\text{Bob correctly guesses } (x_0, x_1) \wedge \text{Alice does not abort}]\} = \frac{1}{2} + \epsilon_B$.

Chailloux *et al.* [23] proved that the existence of a ROT protocol with cheating probabilities A_{OT} and B_{OT} is equivalent to the existence of a 1-2 OT with the same cheating probabilities. Following very similar arguments, in the following subsections we show that the existence of a semirandom OT protocol with cheating probabilities A_{OT} and B_{OT} is equivalent to the existence of a ROT with the same cheating probabilities. This, combined with the results in Ref. [23], proves the proposition.

1. Semirandom OT from ROT

Let P be a ROT protocol with cheating probabilities $A_{\mathrm{OT}}(P)$ and $B_{\mathrm{OT}}(P)$. We construct a semirandom OT protocol Q with the same cheating probabilities as follows.

1. Alice has inputs (z_0, z_1).
2. Alice and Bob run protocol P to output (x_0, x_1) for Alice and (c, y) for Bob.
3. Alice and Bob abort in Q if and only if they abort in P. Otherwise, Alice sends $(z_0 \oplus x_0, z_1 \oplus x_1)$ to Bob.
4. Bob outputs (c, y'), where $y' = (z_c \oplus x_c \oplus y)$.

We now show that Q is a semirandom OT protocol with cheating probabilities $A_{\mathrm{OT}}(P)$ and $B_{\mathrm{OT}}(P)$.

If Alice and Bob are honest then by definition we have $y = x_c$ and so $y' = z_c$. Alice has no information about c and Bob has no information about $z_{c\oplus 1}$, as required.

If Alice is dishonest, she cannot guess c except with probability $A_{\mathrm{OT}}(P)$ since she only receives communications from Bob via protocol P. Therefore, $A_{\mathrm{OT}}(Q) = A_{\mathrm{OT}}(P)$.

If Bob is dishonest, he holds $(z_0 \oplus x_0, z_1 \oplus x_1)$ and aims to guess (z_0, z_1). This is equivalent to Bob guessing (x_0, x_1), which he can do with probability $B_{\mathrm{OT}}(P)$ Therefore, $B_{\mathrm{OT}}(Q) = B_{\mathrm{OT}}(P)$.

2. ROT from semirandom OT

Let P be a semirandom OT protocol with cheating probabilities $A_{\mathrm{OT}}(P)$ and $B_{\mathrm{OT}}(P)$. We construct a ROT protocol Q with the same cheating probabilities as follows.

1. Alice picks $x_0, x_1 \in \{0,1\}$ uniformly at random.
2. Alice and Bob perform the semirandom OT protocol P where Alice inputs x_0, x_1. Let (c, y) be Bob's outputs.
3. Alice and Bob abort in Q if and only if they abort in P. Otherwise, the outputs of protocol Q are (x_0, x_1) for Alice and (c, y) for Bob.

The outputs of Q are uniformly random bits (if both parties are honest) since Alice chooses her input at random. Note that, in the definition of ROT, the outputs are only required to be random in the honest case, and no assertions are made when one party acts dishonestly. Therefore, Q does indeed implement ROT. From the construction of Q, it is also clear that $A_{\mathrm{OT}}(P) = A_{\mathrm{OT}}(Q)$ and $B_{\mathrm{OT}}(Q) = B_{\mathrm{OT}}(P)$.

3. Semirandom OT from ROT in the general protocol framework

In order to fully motivate why the protocol framework in Sec. III A is general for semirandom OT, we here sketch how to recast semirandom OT, realized by performing ROT together with the classical processing as detailed above in Sec. A 1, in the form of our general framework. ROT with classical processing is not immediately in the form of the general protocol framework for semirandom OT, since in a quantum protocol for ROT, Alice has outputs that she would obtain through a measurement. In the general protocol framework in Sec. III A, however, Alice makes no measurements. We also show that the cheating probabilities do not change when the protocol is recast.

Suppose therefore that Alice obtains her two output bits in ROT by measuring a part of a quantum system held by her at some point during the protocol. (If desired, this measurement may be deferred to the end of the protocol, using the standard technique for this, closely related to the procedure we describe below.) Any POVM may be realized as a projective measurement in a suitably enlarged Hilbert space [62], with as many dimensions as outcomes. We label this Hilbert space C. Suppose therefore that in this possibly enlarged Hilbert space, Alice's four-outcome measurement has measurement operators $\Pi_C^{x_0,x_1} = |x_0, x_1\rangle_{CC}\langle x_0, x_1|$, which are orthonormal projectors on four orthogonal basis states $|x_0, x_1\rangle_C$ for $x_0, x_1 \in \{0,1\}$. (The construction below can easily be extended to

the case where Alice's four measurement operators are orthogonal projectors onto more than one basis state, that is, have rank > 1.)

Now, instead of measuring system C to obtain (x_0, x_1) and sending $(z_0 \oplus x_0, z_1 \oplus x_1)$ to Bob, where (z_0, z_1) are Alice's inputs, Alice performs one of the four unitary transforms

$$U_{CD}^{z_0,z_1} = \sum_{x_0,x_1 \in \{0,1\}} |x_0, x_1\rangle_{CC}\langle x_0, x_1| \otimes |z_0 \oplus x_0, z_1 \oplus x_1\rangle_{DD}\langle \text{aux}| \quad \text{(A1)}$$

on system C and an auxiliary system D, where $|\text{aux}\rangle_D$ is a "blank" state that could, e.g., be chosen as $|0,0\rangle$. The states $|0,0\rangle_D, |0,1\rangle_D, |1,0\rangle_D, |1,1\rangle_D$ form an orthonormal basis for the four-dimensional D system. She then sends system D to Bob, who (if he is honest) can measure this system to obtain $(z_0 \oplus x_0, z_1 \oplus x_1)$.

This modified protocol for semirandom OT is now in the form of the general framework. [If desired, Bob's measurements to obtain $(z_0 \oplus x_0, z_1 \oplus x_1)$ and (c, y) can be combined into a single measurement by Bob that directly gives (c, y').] By no signaling [34–38], Bob cannot tell whether or not Alice has measured system C. Therefore, Bob's cheating probability remains the same as if an honest Alice simply had measured system C and sent him the state $|z_0 \oplus x_0, z_1 \oplus x_1\rangle$. Equivalently, Bob's cheating probability is the same as if Alice had measured system C and sent him the classical bits $(z_0 \oplus x_0, z_1 \oplus x_1)$. Since the recast semirandom OT protocol is otherwise the same as the ROT protocol we started with, in particular, how Bob obtains (c, y) remains the same, Alice's cheating probabilities are also equal in both versions of the semirandom protocol. That is, cheating probabilities remain the same in the version that is in the form of the general framework, and in the version where Alice and Bob perform ROT with classical processing.

APPENDIX B: BOB'S CHEATING PROBABILITY FOR SYMMETRIC SETS OF STATES

We need to obtain Bob's cheating probability for a symmetric set of four equiprobable pure states $\sigma_{BM}^{ij} = |\psi^{ij}\rangle\langle\psi^{ij}|$, where "symmetric" means that there exists a unitary transform U such that $U^4 = \mathbb{1}$, and successive applications of U to a "starting state" will result in the other states in the set. It could either hold that $|\psi^{01}\rangle = U|\psi^{00}\rangle, |\psi\rangle^{11} = U^2|\psi^{00}\rangle, |\psi^{10}\rangle = U^3|\psi^{00}\rangle$, which we refer to as "case 1," or that $|\psi^{11}\rangle = U|\psi^{00}\rangle, |\psi\rangle^{01} = U^2|\psi^{00}\rangle, |\psi^{10}\rangle = U^3|\psi^{00}\rangle$, which we refer to as "case 2." All other orderings will be equivalent to these two cases. Case 1 will result in a lower cheating probability for Bob for a given largest pairwise fidelity F between two of the four states. That is, case 1 will give 1-out-of-2 OT protocols with better performance.

In either case, Bob's optimal measurement is the minimum-error measurement for distinguishing between these four states. For a set of symmetric equiprobable states, the optimal minimum-error measurement is the so-called square-root measurement. Its success probability for pure symmetric states can be obtained in terms of the sum of the square roots of the Gram matrix for the states [33]. The elements of the Gram matrix for a set of states $\{|\psi_j\rangle\}$ are given by $G_{ij} = \langle\psi_i|\psi_j\rangle$. For four symmetric pure states, the Gram matrix is given by

$$G = \begin{pmatrix} 1 & f & G & f^* \\ f^* & 1 & f & G \\ G & f^* & 1 & f \\ f & G & f^* & 1 \end{pmatrix}, \quad \text{(B1)}$$

where f is generally complex but G is always real. In case 1, it holds that $f = \langle\psi^{00}|\psi^{01}\rangle = \langle\psi^{01}|\psi^{11}\rangle = \langle\psi^{11}|\psi^{10}\rangle = \langle\psi^{10}|\psi^{00}\rangle$ and $G = \langle\psi^{00}|\psi^{11}\rangle = \langle\psi^{01}|\psi^{10}\rangle$. For sets of states that allow us to implement 1-out-of-2 oblivious transfer, in case 1 it will also hold that $G = 0$. As already mentioned, this follows from conditions (5) and (6). In case 1 it also then holds that the largest pairwise fidelity between two of the states $F = |f|$. In case 2, it will instead hold that $f = 0$ and G is nonzero, with $|G|$ equal to the largest pairwise fidelity F.

The eigenvalues of the Gram matrix are equal to

$$\lambda_0 = 1 + f + G + f^*, \qquad \lambda_1 = 1 + if - G - if^*,$$
$$\lambda_2 = 1 - f + G - f^*, \qquad \lambda_3 = 1 - if - G + if^*. \quad \text{(B2)}$$

These eigenvalues are all real, and can also be shown to always be nonnegative. The success probability for the square-root measurement, and hence Bob's cheating probability, is given by [33]

$$B_{\text{OT}} = \tfrac{1}{16}\left(\sqrt{\lambda_0} + \sqrt{\lambda_1} + \sqrt{\lambda_2} + \sqrt{\lambda_3}\right)^2 = \tfrac{1}{16}\left(\sqrt{1 + G + 2\text{Re}f} + \sqrt{1 + G - 2\text{Re}f} + \sqrt{1 - G + 2\text{Im}f} + \sqrt{1 - G - 2\text{Im}f}\right)^2. \quad \text{(B3)}$$

(Since the eigenvalues of the Gram matrix are nonnegative, the arguments of each of the square roots are non-negative.)

In case 1, where $G = 0$, Bob's optimal cheating probability becomes

$$B_{\text{OT}} = \tfrac{1}{16}\left(\sqrt{1 + 2\text{Re}f} + \sqrt{1 - 2\text{Re}f} + \sqrt{1 + 2\text{Im}f} + \sqrt{1 - 2\text{Im}f}\right)^2.$$

Since Alice can always cheat at least with probability $A_{\text{OT}} \geq (1 + F)/2$, the interesting range is $F = |f| \leq \frac{1}{2}$.

It is relatively easy to show that the expression on the right-hand side is then minimized when f is pure real or pure imaginary. To show this, one can, e.g., set $f = F\cos\theta + iF\sin\theta$, and differentiate with respect to θ. For fixed $F \leq \frac{1}{2}$, B_{OT} reaches its maximum value when $\theta = k\pi/2$ and its minima when $\theta = \pi/4 + k\pi/2$, where k is an integer. (In the general case, where $|f|$ can be larger than $\frac{1}{2}$, we should make either Ref or Imf as large as possible, without the arguments of any of the square roots being negative, in order to minimize B_{OT}.) That is, in case 1 the smallest possible cheating probability for Bob when $F \leq \frac{1}{2}$ is equal to

$$B_{\mathrm{OT}} = \tfrac{1}{4}\left(1 + \tfrac{1}{2}\sqrt{1+2F} + \tfrac{1}{2}\sqrt{1-2F}\right)^2, \tag{B4}$$

as a function of the largest pairwise fidelity F between the states.

In case 2, Bob's optimal cheating probability is instead given by

$$B_{\mathrm{OT}} = \tfrac{1}{4}\left(\sqrt{1+G} + \sqrt{1-G}\right)^2, \tag{B5}$$

where now the largest pairwise fidelity $F = |G|$. For a given F, this cheating probability for Bob is always larger than that in Eq. (B4). To summarize, for a given largest pairwise fidelity $F \leq \frac{1}{2}$, Bob's cheating probability B_{OT} for a set of equiprobable pure symmetric states is at least as large as the cheating probability given in Eq. (B4).

APPENDIX C: ALICE'S OPTIMAL CHEATING STRATEGY IN THE EXAMPLE PROTOCOL

Alice, to pass a test by Bob with certainty, has to send a state of the form

$$\begin{aligned}|\psi_{\mathrm{ch}}\rangle = {} & a\,|0\rangle_A \otimes |00\rangle_B + b\,|1\rangle_A \otimes |{+}{+}\rangle_B \\ & + c\,|2\rangle_A \otimes |11\rangle_B + d\,|3\rangle_A \otimes |{-}{-}\rangle_B\,,\end{aligned} \tag{C1}$$

where $\{|1\rangle_A, |2\rangle_A, |3\rangle_A, |4\rangle_A\}$ is an orthonormal basis for a system A she retains while sending Bob system B, and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

Bob measures the first B qubit in the Z basis and the second B qubit in the X basis. It holds that

$$\langle 0 + |\psi_{\mathrm{ch}}\rangle = \frac{1}{\sqrt{2}}(a\,|0\rangle_A + b\,|1\rangle_A), \tag{C2a}$$

$$\langle 1 + |\psi_{\mathrm{ch}}\rangle = \frac{1}{\sqrt{2}}(b\,|1\rangle_A + c\,|2\rangle_A), \tag{C2b}$$

$$\langle 0 - |\psi_{\mathrm{ch}}\rangle = \frac{1}{\sqrt{2}}(a\,|0\rangle_A + d\,|3\rangle_A), \tag{C2c}$$

$$\langle 1 - |\psi_{\mathrm{ch}}\rangle = \frac{-1}{\sqrt{2}}(c\,|2\rangle_A + d\,|3\rangle_A). \tag{C2d}$$

These states are the unnormalized states conditionally prepared on Alice's side, given Bob's measurement outcome. The norm of each of the above states gives the probability for that outcome on Bob's side. That is, it is the probability with which the corresponding state is prepared.

To successfully cheat, Alice needs to determine whether Bob received the first or second bit. Bob obtains the first bit if he obtains $(0,+)$ or $(1,-)$, and the second bit if he obtains $(0,-)$ or $(1,+)$. It so happens that each of these outcome combinations occur with probability $\frac{1}{2}$, irrespective of a, b, c, d. The two density matrices Alice needs to distinguish between are ρ_0 and ρ_1, with

$$\begin{aligned}\tfrac{1}{2}\rho_0 &= \langle 0+|\psi_{\mathrm{ch}}\rangle\,\langle\psi_{\mathrm{ch}}|0+\rangle + \langle 1-|\psi_{\mathrm{ch}}\rangle\,\langle\psi_{\mathrm{ch}}|1-\rangle\,, \\ \tfrac{1}{2}\rho_1 &= \langle 0-|\psi_{\mathrm{ch}}\rangle\,\langle\psi_{\mathrm{ch}}|0-\rangle + \langle 1+|\psi_{\mathrm{ch}}\rangle\,\langle\psi_{\mathrm{ch}}|1+\rangle\,,\end{aligned} \tag{C3}$$

which in matrix form, with the basis states ordered $\{|0\rangle_A, |1\rangle_A, |2\rangle_A, |3\rangle_A\}$, are given by

$$\rho_0 = \begin{pmatrix} |a|^2 & ab^* & 0 & 0 \\ a^*b & |b|^2 & 0 & 0 \\ 0 & 0 & |c|^2 & cd^* \\ 0 & 0 & c^*d & |d|^2 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} |a|^2 & 0 & 0 & ad^* \\ 0 & |b|^2 & bc^* & 0 \\ 0 & b^*c & |c|^2 & 0 \\ a^*d & 0 & 0 & |d|^2 \end{pmatrix}.$$

Alice's optimal measurement is the Helstrom measurement, given by a projection in the eigenbasis of $\rho_0 - \rho_1$. If Alice obtains an outcome corresponding to a positive eigenvalue, she guesses that Bob obtained the first bit, and if she obtains an outcome corresponding to a negative eigenvalue, then she guesses that Bob obtained the second bit. If Alice obtains an outcome corresponding to a zero eigenvalue, she can guess either the first or second bit, without altering her success probability (conditioned on such an outcome, Bob is equally likely to have obtained the first or second bit). Because the state space on Bob's side is three dimensional, the situation is effectively three dimensional on Alice's side too, but it is convenient to keep $\{|0\rangle_A, |1\rangle_A, |2\rangle_A, |3\rangle_A\}$ as a basis.

We therefore need to find the eigenvalues of

$$\rho_0 - \rho_1 = \begin{pmatrix} 0 & ab^* & 0 & -ad^* \\ a^*b & 0 & -bc^* & 0 \\ 0 & -b^*c & 0 & cd^* \\ -a^*d & 0 & c^*d & 0 \end{pmatrix}. \tag{C4}$$

The eigenvalues are

$$\lambda_1 = \lambda_2 = 0, \tag{C5a}$$

$$\begin{aligned}\lambda_{3,4} &= \pm\sqrt{|ab|^2 + |bc|^2 + |cd|^2 + |ad|^2} \\ &= \pm\sqrt{(|a|^2 + |c|^2)(|b|^2 + |d|^2)},\end{aligned} \tag{C5b}$$

where we choose the + sign for λ_3. The success probability is therefore given by

$$\begin{aligned}p_{\text{cheat}} &= \tfrac{1}{2} + \tfrac{1}{4}\text{Tr}|\rho_0 - \rho_1| \\ &= \tfrac{1}{2} + \tfrac{1}{4}\sum_i |\lambda_i| \\ &= \tfrac{1}{2}\left[1 + \sqrt{(|a|^2 + |c|^2)(|b|^2 + |d|^2)}\right].\end{aligned} \tag{C6}$$

Clearly, Alice's cheating probability is maximized when $|a|^2 + |c|^2 = |b|^2 + |d|^2 = \frac{1}{2}$, giving a maximum cheating probability of $\frac{3}{4}$ whenever this condition is met. One optimal choice for Alice is, for example, $|a| = |b| = 1/\sqrt{2}$ and $c = d = 0$. In this case, $\rho_0 = |+\rangle\langle+|$ and $\rho_1 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Alice should measure in the $|+\rangle, |-\rangle$ basis, where $|\pm\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. With probability $\frac{1}{4}$, she will obtain the outcome "−" and is then sure that Bob obtained the second bit [outcomes $(0,-)$ or $(1,+)$ for Bob]. With probability $\frac{3}{4}$, she will obtain the outcome "+" and then she guesses that Bob obtained the first bit. Her guess is in this case however only correct with probability $\frac{2}{3}$, giving an overall cheating probability of $\frac{3}{4}$.

Choosing either $|a|$ or $|c|$ equal to $1/\sqrt{2}$ and the other one equal to zero, and either $|b|$ or $|d|$ equal to $1/\sqrt{2}$ and the other one equal to zero gives the same cheating probability. These optimal cheating strategies all require only a two-dimensional system on Alice's side. Choosing $|a| = |b| = |c| = |d| = \frac{1}{2}$ also gives $p_{\text{cheat}} = \frac{3}{4}$; these are examples of cheating states with high symmetry. As an example of a suboptimal cheating strategy, choosing three of the parameters equal to $1\sqrt{3}$ and the remaining one equal to zero gives $p_{\text{cheat}} = \frac{1}{2}(1 + \sqrt{2}/3)$, which is less than $\frac{3}{4}$.

APPENDIX D: PREPARATION OF ALICE'S ENTANGLED STATE

In this appendix we describe in detail the preparation of state (33):

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}(|00\rangle_B|0\rangle_A + |++\rangle_B|1\rangle_A).$$

This state can be prepared by means of a controlled-phase gate U_{CP}, a Hadamard gate H, a controlled-controlled-phase gate U_{CCP}, and local unitary operations. Controlled-phase gates introduce tunable and conditional phase shifts. Specifically,

$$\begin{aligned}U_{\text{CP}} &= \mathbb{I} + [\exp(i\alpha) - 1]|11\rangle\langle 11|, \\ U_{\text{CCP}} &= U_{\text{CCP}} = \mathbb{I} + [\exp(i\beta) - 1]|111\rangle\langle 111|.\end{aligned}$$

We use the quantum circuit in Fig. 1(a) to turn an initially separable state $|\psi_{\text{in}}\rangle$ into a state that is equivalent to $|\Sigma\rangle$ up to local unitary operations. The parameters α, β describe the net operation $U(\alpha,\beta) = U_{\text{CCP}}(\beta)(\mathbb{I}\otimes H\otimes\mathbb{I})[U_{\text{CP}}(\alpha)\otimes\mathbb{I}]$.

The input state can be parameterized by two tuples of angles, $\boldsymbol{\theta} = \{\theta_{i=1,2,3}\}$ and $\boldsymbol{\phi} = \{\phi_{i=1,2,3}\}$, as

$$|\psi_{\text{in}}\rangle = \bigotimes_{i=1,2,3}\prod [\cos(\theta_i/2)|0\rangle + \sin(\theta_i/2)e^{i\phi_i}|1\rangle].$$

The degree of local-unitary equivalence $E(|a\rangle, |b\rangle)$ between states $|a\rangle$ and $|b\rangle$ can be quantified by an overlap maximized over all local unitary operations

$$E(|a\rangle, |b\rangle) = \max_{\mathbf{v}} |\langle a|V_{\text{LO}}(\mathbf{v})|b\rangle|^2,$$

where $\mathbf{v}$ is a tuple containing nine parameters $\{A_j, B_j, C_j\}_{j=1,2,3}$ that parameterize the operation $V_{\text{LO}} = V_1 \otimes V_2 \otimes V_3$. Specifically, the parameters A_j, B_j, and C_j describe a j th local operation

$$V_j = \begin{pmatrix} \cos(A_j)\exp(iB_j) & -\sin(A_j)\exp(-iC_j) \\ \sin(A_j)\exp(iC_j) & \cos(A_j)\exp(-iB_j)\end{pmatrix}. \tag{D1}$$

We maximize $E[|\Sigma\rangle, U(\alpha,\beta)|\psi_{\text{in}}(\boldsymbol{\theta},\boldsymbol{\phi})\rangle]$ numerically using the Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm [63].

First we perform the optimization with all parameters being free and with multiple random initial guesses. From the set of optima we arbitrarily pick the parameter tuples with $\theta_1 \approx 120°$, fixed $\theta_1 = 120°$ and perform the optimization again. We repeat this procedure to gradually also fix ϕ_1, θ_2, ϕ_2, β, and φ_3, in this order. The parameters α and θ_3 remain free in the last round of the optimization. The optimal parameters are listed in Table I. With these parameters, the complement of E to one is sufficiently small, $1 - E \approx 8 \times 10^{-11}$.

Next, we initialize the circuit and the input state with the optimal parameters and perform tomography of the output quantum state. Employing the maximum-likelihood

TABLE I. Optimal parameters for the preparation of state $|\Sigma\rangle$.

θ_1	120.000°	ϕ_1	22.500°
θ_2	90.000°	ϕ_2	90.000°
θ_3	116.565°	ϕ_3	180.000°
α	−138.190°	β	180.000°

TABLE II. Parameters of the corrective unitary operations.

i	A_i (deg)	B_i (deg)	C_i (deg)
1	41.315	49.770	136.535
2	48.385	−37.718	42.637
3	29.367	−1.225	−177.329

method [61] we reconstruct the density matrix $\rho_{\text{exp},0}$ of actually prepared quantum state. Then we numerically maximize the expectation value

$$\langle\Sigma|U_{\text{LO}}(\mathbf{u})\rho_{\text{exp},0}U_{\text{LO}}^{\dagger}(\mathbf{u})|\Sigma\rangle$$

to find the corrective local operations U_{LO}. The optimal U_{LO} not only implements the required local operation to finish the preparation of $|\Sigma\rangle$, but also compensates for some systematic errors. The parameters of the optimal unitaries are listed in Table II. We parameterize $U_{\text{LO}} = U_1 \otimes U_2 \otimes U_3$ the same way as in case of V; see Eq. (D1). Note that these parameters are not unique, multiple solutions exist (due to insensitivity to global phase and phase periodicity).

An arbitrary unitary operation acting on a single polarization qubit can be easily implemented by a sequence of a quarter-wave plate, half-wave plate, and another quarter-wave plate. However, we merge the unitary U_{LO} into final projective measurements. It can be done because the output state is projected at the end onto a state $|\pi\rangle$ and the projection $\langle\pi|U_i|\eta\rangle$ is equivalent to $\langle\tilde{\pi}|\eta\rangle$ with $|\tilde{\pi}\rangle = U_i^{\dagger}|\pi\rangle$. We find the corresponding wave-plate angles for six-state tomography by means of numerical minimization; see Table III. This optimization reduces the number of components in the experimental setup, reducing experimental imperfections and losses that accumulate with each added component.

APPENDIX E: EXPERIMENTAL DATA

In this appendix we present the full sets of experimental data. The tables contain measured counts C, relative frequencies (or estimated probabilities) f, and theoretically predicted probabilities p_t. Relative frequencies are calculated as a ratio of the number of respective counts to the total number of counts. Digits in parentheses represent one standard deviation at the final decimal place. The statistical errors are computed using error propagation and the fact that the count rates obey Poisson distribution.

TABLE III. Wave-plate angles for transformed projectors. All numbers are in degrees.

$\|\pi\rangle$	HWP1	QWP1	HWP2	QWP2	HWP3	QWP3
$\|0\rangle$	−15.35	49.83	9.80	53.28	80.78	8.54
$\|1\rangle$	29.65	−40.17	91.52	−53.28	27.24	−8.54
$\|+\rangle$	3.16	94.65	47.90	92.29	9.80	92.26
$\|-\rangle$	43.50	85.35	2.90	2.29	−35.20	2.26
$\|R\rangle$	22.80	−1.28	64.96	82.06	9.51	53.85
$\|L\rangle$	−20.93	1.28	19.96	−7.94	54.51	−36.15

TABLE IV. Measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when both the parties were honest. Here $|\psi_B\rangle$ is a state that Alice sends to Bob. Bob measures projection onto $|\pi_B\rangle$; p_s is the probability of correct receipt, i.e., Bob gets an erroneous bit with probability $1 - p_s$.

		$\|\pi_B\rangle$				
	$\|\psi_B\rangle$	$\|0+\rangle$	$\|0-\rangle$	$\|1+\rangle$	$\|1-\rangle$	p_s
C	$\|00\rangle$	892	829	3	3	
f		0.52(1)	0.48(1)	0.002(1)	0.002(1)	1.00(2)
p_t		0.5	0.5	0	0	1
C	$\|++\rangle$	823	2	782	7	
f		0.51(1)	0.0012(9)	0.48(1)	0.004(2)	0.99(2)
p_t		0.5	0	0.5	0	1
C	$\|--\rangle$	7	824	15	867	
f		0.004(2)	0.48(1)	0.009(2)	0.51(1)	0.99(2)
p_t		0	0.5	0	0.5	1
C	$\|11\rangle$	0	1	800	841	
f		0.000(0)	0.0006(5)	0.49(1)	0.51(1)	1.00(2)
p_t		0	0	0.5	0.5	1

In Table IV we show data for the case when both parties were honest. Alice sent states $|00\rangle$, $|++\rangle$, $|--\rangle$, $|11\rangle$ and Bob measured in the ZX basis. In Table V we show data for Bob's test measurements when he measured the incoming states in the XX or ZZ basis.

In Table VI we summarize results for the situation when Alice was honest but Bob was cheating. This means that Bob has been performing square-root measurements.

TABLE V. Data for Bob's test measurements in the case when Alice was honest. Here, p_{FA} is the probability of "false alarm," i.e., the probability that Bob aborts the protocol even if Alice is not cheating.

		$\|\pi_B\rangle$				
	$\|\psi_B\rangle$	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$	p_{FA}
C	$\|00\rangle$	1701	3	1	0	
f		0.998(1)	0.002(1)	0.0006(5)	0.000(0)	0.002(1)
p_t		1	0	0	0	0
C	$\|11\rangle$	0	0	15	1592	
f		0.000(0)	0.000(0)	0.009(2)	0.991(2)	0.009(2)
p_t		0	0	0	1	0
		$\|++\rangle$	$\|+-\rangle$	$\|-+\rangle$	$\|--\rangle$	
C	$\|++\rangle$	1615	1	43	1	
f		0.973(4)	0.0006(5)	0.026(4)	0.0006(5)	0.027(4)
p_t		1	0	0	0	0
C	$\|--\rangle$	5	9	9	1660	
f		0.003(1)	0.005(2)	0.005(2)	0.986(3)	0.014(3)
p_t		0	0	0	1	0

TABLE VI. Bob was cheating, Alice was honest. Here, p_{CE} is the probability of Bob correctly estimating the incoming state.

		$\|\pi_B\rangle$				
	$\|\psi_B\rangle$	$\|\zeta_0\rangle\|\xi_0\rangle$	$\|\zeta_0\rangle\|\xi_1\rangle$	$\|\zeta_1\rangle\|\xi_0\rangle$	$\|\zeta_1\rangle\|\xi_1\rangle$	p_{CE}
C	$\|00\rangle$	85	1215	4	114	
f		0.060(6)	0.857(9)	0.003(1)	0.080(7)	0.857(9)
p_t		0.125	0.729	0.021	0.125	0.729
C	$\|++\rangle$	1013	184	301	53	
f		0.65(1)	0.119(8)	0.19(1)	0.034(5)	0.65(1)
p_t		0.729	0.125	0.125	0.021	0.729
C	$\|--\rangle$	64	253	384	1441	
f		0.030(4)	0.118(7)	0.179(8)	0.67(1)	0.67(1)
p_t		0.021	0.125	0.125	0.729	0.729
C	$\|11\rangle$	228	48	1360	253	
f		0.121(7)	0.025(4)	0.72(1)	0.134(8)	0.72(1)
p_t		0.125	0.021	0.729	0.125	0.729

TABLE VII. Alice was cheating, Bob was honest. The table shows the probabilities of Alice correctly or incorrectly guessing Bob's bit c.

Alice's estimate	Bob's bit c	C	f	p_t
0	0	856	0.53(1)	0.5
0	1	356	0.22(1)	0.25
1	0	17	0.010(3)	0
1	1	400	0.25(1)	0.25

TABLE VIII. Test measurements for an honest Bob when Alice was cheating. Alice measured her qubit in the Z basis and Bob measured his qubit in the ZZ or XX basis.

$\|\pi_A\rangle$	$\|\pi_B\rangle$	C	f	p_t
$\|0\rangle$	$\|00\rangle$	851	0.52(1)	0.5
$\|0\rangle$	$\|01\rangle$	15	0.009(2)	0
$\|0\rangle$	$\|10\rangle$	28	0.017(3)	0
$\|0\rangle$	$\|11\rangle$	31	0.019(3)	0
$\|1\rangle$	$\|++\rangle$	688	0.42(1)	0.5
$\|1\rangle$	$\|+-\rangle$	7	0.004(2)	0
$\|1\rangle$	$\|-+\rangle$	11	0.007(2)	0
$\|1\rangle$	$\|--\rangle$	4	0.002(1)	0

The situation when Bob was honest but Alice was cheating is recorded in the last two tables. In Table VII we show the relative frequencies of Alice's correct and incorrect estimates of the values of Bob's bit c. In Table VIII we show relative frequencies of different results of Alice's and Bob's measurements in the test phase of the protocol. Theoretically, Bob should only detect $|++\rangle$ or $|00\rangle$.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), p. 175.

[2] D. Mayers, Unconditionally Secure Quantum Bit Commitment is Impossible, Phys. Rev. Lett. **78**, 3414 (1997).

[3] H.-K. Lo, Insecurity of Quantum Secure Computations, Phys. Rev. A **56**, 1154 (1997).

[4] A. Kitaev, in *Talk at the Quantum Information Processing Conference* (MSRI, Berkeley, CA, 2002).

[5] C. Mochon, Quantum weak coin flipping with arbitrarily small bias, arXiv:0711.4114 (2007).

[6] A. Chailloux and I. Kerenidis, in *50th Annual IEEE Symposium on Foundations of Computer Science Foundations of Computer Science (FOCS'09)* (2009), p. 527.

[7] A. Chailloux and I. Kerenidis, in *52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2011), p. 354.

[8] O. Goldreich and R. Vainish, in *Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology* (1987), p. 73.

[9] J. Kilian, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing* (1988), p. 20.

[10] S. Wiesner, Conjugate coding, ACM Sigact News **15**, 78 (1983).

[11] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, Commun. ACM **28**, 637 (1985).

[12] M. O. Rabin, How to exchange secrets with oblivious transfer, IACR Cryptol. ePrint Arch. **2005**, 187 (2005).

[13] C. Crépeau, in *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology* (1987), p. 350.

[14] G. Brassard and C. Crépeau, in *International Conference on the Theory and Applications of Cryptographic Techniques* (1997), p. 334.

[15] G. Brassard, C. Crépeau, and S. Wolf, Oblivious transfers and privacy amplification, J. Cryptol. **16**, 219 (2003).

[16] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded-quantum-storage model, SIAM J. Comput. **37**, 1865 (2008).

[17] D. Pitalua-Garcia, Spacetime-constrained oblivious transfer, Phys. Rev. A **93**, 062346 (2016).

[18] D. Pitalua-Garcia and I. Kerenidis, Practical and unconditionally secure spacetime-constrained oblivious transfer, Phys. Rev. A **98**, 032327 (2018).

[19] D. Pitalua-Garci, One-out-of-m spacetime-constrained oblivious transfer, Phys. Rev. A **100**, 012302 (2019).

[20] S. Kundu, J. Sikora, and E. Y.-Z. Tan, A device-independent protocol for XOR oblivious transfer, arXiv:2006.06671 (2020).

[21] M. Roehsner, J. A. Kettlewell, T. B. Batalhao, J. F. Fitzsimons, and P. Walther, Quantum advantage for probabilistic one-time programs, Nat. Commun. **9**, 5225 (2018).

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

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

[24] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Quantum digital signatures with quantum-key-distribution components, Phys. Rev. A **91**, 042304 (2015).

[25] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Phys. Rev. A **93**, 032325 (2016).

[26] J. Sikora, A. Chailloux, and I. Kerenidis, Strong connections between quantum encodings, nonlocality, and quantum cryptography, Phys. Rev A **89**, 022334 (2014).

[27] L. Salvail, C. Schaffner, and M. Sotáková, in International Conference on the Theory and Application of Cryptology and Information Security (Springer, 2009), p. 70.

[28] As also stated in Ref. [22], it is standard to assume, in this setting, that an honest party's input bits are uniformly random, so that the corresponding cheating probabilities are computed on average.

[29] A mechanism producing true randomness is a destructive quantum measurement.

[30] P. Hausladen and W. K. Wootters, A "pretty good" measurement for distinguishing quantum states, J. Mod. Opt. **41**, 2385 (1994).

[31] K. M. Audenaert and M. Mosonyi, Upper bounds on the error probabilities and asymptotic error exponents in quantum multiple state discrimination, J. Math. Phys. **55**, 102201 (2014).

[32] Symmetric sets of states are ubiquitous in quantum information. In this context "symmetric" means that there exists a unitary U such that $U^4 = \mathbb{1}$ and $\sigma^{00}_{BM} = U \circ \sigma^{01}_{BM} = U^2 \circ \sigma^{11}_{BM} = U^3 \circ \sigma^{10}_{BM}$.

[33] P. Wallden, V. Dunjko, and E. Andersson, Minimum-cost quantum measurements for quantum information, J. Phys. A: Math. Theor. **47**, 125303 (2014).

[34] G. C. Ghirardi, A. Rimini, and T. Weber, A general argument against superluminal transmission through the quantum mechanical measurement process, Lett. Nuovo Cimento Soc. Ital. Fis. **27**, 293 (1980).

[35] P. J. Bussey, "Super-luminal communication" in einstein-podolsky-Rosen experiments, Phys. Lett. A **90**, 9 (1982).

[36] T. F. Jordan, Quantum correlations do not transmit signals, Phys. Lett. A **94**, 264 (1983).

[37] Stephen M. Barnett and Erika Andersson, Bound on measurement based on the no-signaling condition, Phys. Rev. A **65**, 044307 (2002).

[38] S. Croke, E. Andersson, and S. M. Barnett, No-signaling bound on quantum state discrimination, Phys. Rev. A **77**, 012113 (2008).

[39] A. Uhlmann, The "transition probability" in the state space of a *-algebra, Rep. Math. Phys. **9**, 273 (1976).

[40] H. Buhrman, M. Christandl, and C. Schaffner, Complete Insecurity of Quantum Protocols for Classical Two-Party Computation, Phys. Rev. Lett. **109**, 160501 (2012).

[41] M. Pusey, J. Barrett, and T. Rudolph, On the reality of the quantum state, Nat. Phys. **8**, 475 (2012).

[42] C. Caves, C. Fuchs, and R. Schack, Conditions for compatibility of quantum-state assignments, Phys. Rev. A **66**, 062111 (2002).

[43] S. Bandyopadhyay, R. Jain, J.Oppenheim, and C. Perry, Conclusive exclusion of quantum states, Phys. Rev. A **89**, 022336 (2014).

[44] P. Wallden, V. Dunjko, and E. Andersson, Minimum-cost measurements for quantum information, J. Phys. A: Math. Theor. **47**, 125303 (2014).

[45] T. Heinosaari and O. Kerppo, Antidistinguishability of pure quantum states, J. Phys. A: Math. Theor. **51**, 365303 (2018).

[46] C. Perry, R. Jain, and J. Oppenheim, Communication Tasks with Infinite Quantum-Classical Separation, Phys. Rev. Lett. **115**, 030504 (2015).

[47] T. Heinosaari and O. Kerppo, Communication of partial ignorance with qubits, J. Phys. A: Math. Theor. **52**, 395301 (2019).

[48] V. Havlíček and J. Barrett, Simple Communication Complexity Separation from Quantum State Antidistinguishability, arXiv:1911.01927 (2019).

[49] J. Crickmore, I. V. Puthoor, B. Ricketti, S. Croke, M. Hillery, and E. Andersson, Unambiguous quantum state elimination for qubit sequences, Phys. Rev. Res. **2**, 013256 (2020).

[50] The choice of $\sqrt{N}$ test bits is somewhat arbitrary. For security in the asymptotic case, we only need Bob to choose a number of test states such that the number of test states tends to ∞ as N increases; the fraction of states chosen for testing tends to 0 as N increases.

[51] If there were such a measurement, Bob could simulate this strategy when he has only a single state and beat the minimum-error measurement.

[52] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, Maximum Confidence Quantum Measurements, Phys. Rev. Lett. **96**, 070401 (2006).

[53] Actually, Bob does not need a quantum memory for his test measurements. He can randomly decide to make a test measurement in the ZZ or the XX basis, and only afterwards ask Alice to reveal the corresponding states. Half of the test measurements will not contribute, but this will not affect the function of the protocol.

[54] R. Stárek, M. Mičuda, M. Miková, I. Straka, M. Dušek, M. Ježek, and J. Fiurášek, Experimental investigation of a four-qubit linear-optical quantum logic circuit, Sci. Rep. **6**, 33475 (2016).

[55] R. Okamoto, H. F. Hofmann, S. Takeuchi, and K. Sasaki, Demonstration of an Optical Quantum Controlled-Not Gate Without Path Interference, Phys. Rev. Lett. **95**, 210506 (2005).

[56] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White, Demonstration of a Simple Entangling Optical Gate and its use in Bell-State Analysis, Phys. Rev. Lett. **95**, 210504 (2005).

[57] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, Linear Optics Controlled-Phase Gate Made Simple, Phys. Rev. Lett. **95**, 210505 (2005).

[58] R. Stárek, M. Mičuda, I. Straka, M. Nováková, M. Dušek, M. Ježek, J. Fiurášek, and R. Filip, Experimental quantum decoherence control by dark states of the environment, arXiv:2005.07169 (2020).

[59] We use a simplified configuration at Bob's side, but it is possible to build a four-output measurement spanning the full two-qubit space solely by linear optics.

[60] In this situation it is a square-root measurement that is actually quite intuitive: the states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ form a "cross" on the Bloch sphere. The measurement on the first qubit is represented by two orthogonal states that lie on the diagonal. The measurement on the second qubit is different and corresponds to the other diagonal.

[61] M. Ježek, J. Fiurášek, and Z. Hradil, Quantum inference of states and processes, Phys. Rev. A **68**, 012305 (2003).

[62] M. A. Neumark, Spectral functions of a symmetric operator, Izv. Akad. Nauk. SSSR, Ser. Mat. **4**, 277 (1940).

[63] "Quasi-Newton methods" in *Numerical Optimization* (Springer, New York, NY, 2006), p. 135.