Almost tight lower bounds for 1-out-of-2 quantum oblivious transfer

Ryan Amiri,[1] Petros Wallden,[2] and Erika Andersson[1]

[1]SUPA, Institute of Photonics and Quantum Sciences,
Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[2]LFCS, School of Informatics, University of Edinburgh,
10 Crichton Street, Edinburgh EH8 9AB, United Kingdom

Extended Abstract

A. Introduction and related work

Oblivious transfer (OT) is one of the most important and fundamental primitives in modern classical cryptography, with a variety of applications including secure multiparty computation, oblivious sampling, e-voting, signatures and many more. Its prominence stems from the fact that it can be used as the foundation for all secure two-party computations; with OT, all secure two-party computations are possible [1, 2]. Perfectly secure OT is impossible to achieve in the information-theoretic setting, but imperfect variants, in which the participants' ability to cheat is limited, are possible using quantum means despite remaining classically impossible. Precisely what security parameters are attainable in these imperfect variants remains unknown. For OT, as well as for many other cryptographic primitives, it has been an interesting and productive open question to determine the optimal achievable security parameters.

For strong coin flipping, Kitaev [5] introduced the semi-definite programming formalism to show that the product of Alice's and Bob's cheating probabilities must be greater than $1/2$, implying that the minimum cheating probability is at least $1/\sqrt{2}$. For weak coin flipping, it was shown by Mochon [6] that it is possible to achieve a cheating probability of $1/2+\epsilon$ for any $\epsilon > 0$, and that this is optimal. Chailloux and Kerenidis [7] used the results on weak coin flipping to generate a protocol for strong coin flipping achieving the bound set by Kitaev. Lastly, for quantum bit commitment, Chailloux and Kerenidis [8] proved that the minimum cheating probability is 0.739, and presented a protocol achieving this bias. Thus, for both bit commitment, strong coin flipping and weak coin flipping, the known bounds are tight with the known protocols.

For OT on the other hand, the situation is not so clear-cut. Even in terms of definitions, there is a wide spectrum of distinct protocols all referred to using the same umbrella term "oblivious transfer". OT was first introduced informally by Wiesner as "a means for transmitting two messages, either but not both of which may be received" [9], and subsequently formalised as 1-out-of-2 OT (1-2 OT) in [11]. In related work, Rabin [12] introduced a protocol (now called Rabin OT), which was later shown by Crépeau [13] to be equivalent to 1-2 OT. Various "weaker" variants of OT have also been proposed, most notably Generalised OT, XOR OT and Universal OT, but all have been shown to be equivalent to 1-2 OT in the sense that if it is possible to do one, then it is possible to use this to implement the others [14, 15]. There is also work by Damgård, Fehr, Salvail and Schaffner [16] who define OT in a slightly different way, and who use binary linear functions to characterise security. With these definitions (and their quantum counterparts), and by using the *additional* assumption of bounded quantum storage, the authors describe a perfectly secure protocol for 1-2 OT [17].

B. Our contributions

In this paper [18] we consider stand-alone quantum protocols for 1-2 OT, and are concerned only with information-theoretic security. Intuitively, 1-2 OT is a two-party protocol in which Alice inputs two bits, x_0 and x_1, and Bob inputs a single bit, b. The protocol outputs x_b to Bob with the guarantees that Alice does not know b, and that Bob does not know $x_{\overline{b}}$. A cheating Alice aims to find the value of b, and her probability of doing so is denoted by A_{OT}. A cheating Bob aims to correctly guess both x_0 and x_1, and his probability of doing so is denoted by B_{OT}. The cheating probability of the protocol is defined as $p_C = \max\{A_{OT}, B_{OT}\}$.

As stated above, perfect 1-2 OT is impossible to achieve with information-theoretic security, meaning that all protocols attempting 1-2 OT in the information-theoretic setting must have $p_C > 1/2$. It is not known exactly how much larger than $1/2$ the cheating probability must be. In fact, the best known protocol is described in Ref. [19] and has $p_C = A_{OT} = B_{OT} = 0.75$. Prior to our work, the best lower bound on p_C for 1-2 OT was found by Chailloux, Gutoski and Sikora [20] to be

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

Clearly, there is still a gap between the known lower bound on p_C and the cheating probabilities attained by known protocols; our paper aims to close this gap. In other words, we address the theoretical question: how close to ideal can unconditionally secure 1-2 OT protocols be? Our paper contains three main contributions:

1. We introduce the concept of Semi-random OT and prove an equivalence between cheating in 1-2 OT and Semi-random OT. We further describe a general framework for Semi-random OT.

2. We use this framework to study Semi-random OT and, by extension, 1-2 OT protocols in the information-theoretic setting. We are able to increase the lower bound on p_C for 1-2 OT protocols by constructing specific cheating strategies that are always available to Alice and Bob and which are always undetectable. Our construction parametrises Alice's and Bob's ability to cheat in terms of a single quantity and suggests how to construct schemes when guarding against one of either sender or receiver dishonesty is prioritised, as well as allowing us to derive bounds these settings. Unbalanced scenarios can arise, for example, in the context of quantum signature schemes [21, 22], and the derived bounds prove useful for understanding the potential application of imperfect OT to signatures.

3. We illustrate our construction by describing a new OT protocol relying on unambiguous state elimination (USE) measurements. The protocol improves on all previous protocols in the sense that it decreases the average cheating probabilities of the participants. The security parameters achieved are almost tight with the bounds proved in this paper.

C. Semi-random OT

Semi-random OT is a protocol almost identical to 1-2 OT, except that Bob has no input; instead, Bob obtains two outputs, b and x_b, such that the value of b is random. We show that it is equivalent to 1-2 OT in the sense that, if there exists a protocol implementing Semi-random OT with cheating probabilities A_{OT} and B_{OT}, then this can be used to implement 1-2 OT with the same cheating probabilities, and vice versa. This allows us to study 1-2 OT indirectly, going via Semi-random OT. The reason for introducing yet another new type of OT is that it is easier to analyse than 1-2 OT, since all Semi-random OT protocols fall within the framework set out in this paper, or can at least be rewritten into this standard form without altering the cheating probabilities.

The framework allows us to construct specific cheating strategies that are always available to Alice and Bob and which are always undetectable. We express the cheating probabilities of both Alice and Bob in terms of a single parameter, F, related to the maximum fidelity between the different possible output states held by Bob in the final round of the protocol [18]. We find that for any Semi-random OT protocol

$$p_C = \max\{A_{OT}, B_{OT}\} \geq 2/3, \tag{2}$$

which agrees with the bound found by Chailloux, Gutoski and Sikora [20] using a different technique. Further, if the possible outputs of the honest protocol are pure symmetric states then

$$p_C = \max\{A_{OT}, B_{OT}\} \geq 0.749. \tag{3}$$

In this context a pure symmetric set of states $\{|\psi_0\rangle, \dots, |\psi_N\rangle\}$ is one for which there exists a permuting unitary U such that $|\psi_j\rangle = U^j|\psi_0\rangle$ for all $j = 1, \dots, N$. Symmetric sets of states are ubiquitous in quantum information, with the BB84 states being a well known example. Due to the inherent symmetry of 1-2 OT, we conjecture that protocols using pure symmetric states will be optimal in general and the tighter bound will always apply. This would effectively close the gap between the known bounds and the known protocols.

D. Unambiguous state elimination

Lastly, the protocol we propose explores a novel new application of USE measurements by using them to implement Semi-random OT with $A_{OT} = 0.75$ and $B_{OT} = 0.729$. Combined with the previous results, this directly implies the existence of a 1-2 OT protocol with the same cheating probabilities, thereby improving upon all known protocols. We believe that USE measurements are well suited to cryptography, and will likely find many applications. Unambiguous measurements give "perfect" information in the sense that, given a successful measurement outcome, it is certain that the information obtained is correct. However, successful measurement outcomes either do not give complete information, or do not occur with probability 1. To date, unambiguous measurements have been proposed in two forms, unambiguous state discrimination (USD), and unambiguous state elimination. A successful USD measurement gives complete information on the identity of the quantum state being measured; a successful USE measurement allows the observer to rule out one or more of the possible quantum states with certainty. 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 in cryptographic applications. More concretely, USD can be seen as similar to Rabin OT, while USE measurements seem closely related to the more common 1-2 OT. Since OT plays a central role in secure two-party computations, it seems likely that unambiguous measurements could also play a major role in the developing field. By presenting a new application of USE measurements, we hope to encourage its use in future work.

[1] Goldrcich, Oded, and Ronen Vainish. "How to solve any protocol problem-an efficiency improvement." Advances in Cryptology - CRYPTO'87. Springer Berlin Heidelberg, 1987.

[2] Kilian, Joe. "Founding crytpography on oblivious transfer." Proceedings of the twentieth annual ACM symposium on Theory of computing. ACM, 1988.

[3] Mayers, Dominic. "Unconditionally secure quantum bit commitment is impossible." Physical review letters 78.17 (1997): 3414.

[4] Lo, Hoi-Kwong. "Insecurity of quantum secure computations." Physical Review A 56.2 (1997): 1154.

[5] Kitaev, Alexei. "Quantum coin-flipping." Talk at QIP (2003).

[6] Mochon, Carlos. "Quantum weak coin flipping with arbitrarily small bias." arXiv preprint arXiv:0711.4114 (2007).

[7] Chailloux, André., and Iordanis Kerenidis. "Optimal quantum strong coin flipping." Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on. IEEE, 2009.

[8] Chailloux, André, and Iordanis Kerenidis. "Optimal bounds for quantum bit commitment." Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. IEEE, 2011.

[9] S. Wiesner. "Conjugate coding." SIGACT News, 15(1):78-88, 1983

[10] Wullschleger, Jürg. "Oblivious-transfer amplification." Springer Berlin Heidelberg, 2007.

[11] Even, Shimon, Oded Goldreich, and Abraham Lempel. "A randomized protocol for signing contracts." Communications of the ACM 28.6 (1985): 637-647.

[12] Rabin, Michael O. "How To Exchange Secrets with Oblivious Transfer." IACR Cryptology ePrint Archive 2005 (2005): 187.

[13] Crépeau, Claude. "Equivalence between two flavours of oblivious transfers." Advances in Cryptology - CRYPTO'87. Springer Berlin Heidelberg, 1987.

[14] Brassard, Gilles, and Claude Crépeau. "Oblivious transfers and privacy amplification." Advances in Cryptology - EUROCRYPT'97. Springer Berlin Heidelberg, 1997.

[15] Brassard, Gilles, Claude Crépeau, and Stefan Wolf. "Oblivious transfers and privacy amplification." Journal of Cryptology 16.4 (2003): 219-237.

[16] Schaffner, Christian. "Cryptography in the bounded-quantum-storage model." arXiv preprint arXiv:0709.0289 (2007).

[17] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. "Cryptography in the bounded quantum-storage model." In 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 449–458, 2005.

[18] Amiri, Ryan, Petros Wallden, and Erika Andersson. "Almost tight lower bounds for 1-out-of-2 quantum oblivious transfer." Manuscript in preparation.

[19] Chailloux, André, Iordanis Kerenidis, and Jamie Sikora. "Lower bounds for quantum oblivious transfer." arXiv preprint arXiv:1007.1875v2 (2010).

[20] Chailloux, André, Gus Gutoski, and Jamie Sikora. "Optimal bounds for semi-honest quantum oblivious transfer." arXiv preprint arXiv:1310.3262 (2013).

[21] Wallden, Petros, Vedran Dunjko, Adrian Kent, and Erika Andersson. "Quantum digital signatures with quantum-key-distribution components." Physical Review A 91, no. 4 (2015): 042304.

[22] Amiri, Ryan, Petros Wallden, Adrian Kent, and Erika Andersson. "Secure quantum signatures using insecure quantum channels." Physical Review A 93, no. 3 (2016): 032325.

Almost tight lower bounds for 1-out-of-2 quantum oblivious transfer

Ryan Amiri,[1] Petros Wallden,[2] and Erika Andersson[1]

[1] *SUPA, Institute of Photonics and Quantum Sciences,*
Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[2] *LFCS, School of Informatics, University of Edinburgh,*
10 Crichton Street, Edinburgh EH8 9AB, United Kingdom

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 characterised 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, the result does not exclude imperfect variants of these protocols from being 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 semi-definite programming formalism to show that the product of Alice's and Bob's cheating probabilities must be greater than $1/2$, implying that the minimum cheating probability is at least $1/\sqrt{2}$. For weak coin flipping, Mochon [5] showed that the minimum cheating probability is at least $1/2+\epsilon$ 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] utilised 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 so clear-cut. 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 cheat but their abilities are limited. OT is one of the most widely used and fundamental primitives 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 flavours, 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 formalised as 1-out-of-2 oblivious transfer (1-2 OT) in [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 Generalised 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, Fehr, Salvail and Schaffner [16] who define OT in a slightly different way, and who characterise security in terms of information leakage. With these definitions (and their quantum counterparts), the authors describe a 1-2 OT protocol which is secure in the bounded quantum storage model.

In this paper we consider stand-alone quantum protocols for 1-2 OT, 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, Gutoski and Sikora [17], who show that the minimum cheating probability is at least $2/3$. However, the best known 1-2 OT protocol has a cheating probability of 0.75, showing there is a gap between what is known to be achievable, and what is known to be impossible. Our paper contains three main contributions:

1. We introduce a new framework for studying general Semi-random OT protocols and, by extension, 1-2 OT protocols in the information-theoretic setting.

2. Using this framework we increase the lower bound on the minimum achievable cheating probability for 1-2 quantum OT protocols in the information-theoretic security model to 0.749 if the states in the final round of the (honest) protocol are pure and symmetric. In the completely general setting, our results reproduce the known $2/3$ bound. Due to the inherent symmetry of 1-2 OT, we conjecture that protocols using pure symmetric states will be optimal in general and the tighter bound will always apply. Our construction parametrises Alice's and Bob's ability to cheat in terms of a single quantity, F, the maximum fidelity of the possible protocol output states. This parametrisation suggests how

to construct schemes when one of either sender or receiver dishonesty is prioritised, and also allows us to derive bounds these settings. Such a scenario arises in the context of quantum signature schemes [18, 19], and the derived bounds prove useful for understanding the potential application of imperfect OT to signatures.

3. We illustrate our construction by describing a new OT protocol relying on unambiguous state elimination (USE) measurements. The protocol improves on all previous protocols in the sense that it decreases the cheating probability of the receiver. It also serves to highlight the interesting connection between USE measurements and 1-2 OT, and represents a novel new application for this relatively underused type of measurement. The security parameters achieved are almost tight with the bounds proved in this paper.

The paper is organised as follows. We begin in Section II by defining Semi-random OT, a useful variant of OT employed throughout this paper. In Section III we describe a general framework for studying Semi-random OT protocols and consider specific cheating strategies available to Alice and Bob within this model that are always undetectable. We use these to lower bound the achievable cheating probabilities for unbounded adversaries. In Section IV we introduce unambiguous measurements; in particular we focus on USE measurements and motivate their use in cryptography. As an example we describe an N-round Semi-random OT protocol which utilises USE measurements and we analyse its security in the asymptotic limit.

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 $x_{\overline{b}}$. A cheating Alice aims to find the value of b, while a cheating Bob aims to correctly guess both x_0, x_1.

Definition 1. [20] *A 1-2 quantum OT protocol is a protocol between two parties, Alice and Bob, such that*

- *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).*
- *At the end of the protocol, Bob outputs y or Abort and Alice can either Abort or not.*
- *If Alice and Bob are honest, they never Abort, $y = x_b$, Alice has no information about b and Bob has no information about $x_{\overline{b}}$.*
- $A_{OT} := \sup\{\Pr[\textit{Alice guesses } b \wedge \textit{Bob does not Abort}]\}$ $= \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob guesses } (x_0, x_1) \wedge \textit{Alice does not Abort}]\}$ $= \frac{1}{2} + \epsilon_B$

The suprema are taken over all cheating strategies available to Alice and Bob. We define $p_C := \max\{A_{OT}, B_{OT}\}$ to be the *cheating probability* of the protocol. This definition of security differs from some other work, for example [21], in which security is characterised 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 useful variant of OT, called Semi-random OT, which differs from the above 1-2 OT in that Bob does not have any inputs and is randomly assigned an output. More concretely, Semi-random OT is defined as

Definition 2. *1-2 quantum Semi-random OT, or simply Semi-random OT, is a protocol between two parties, Alice and Bob, such that*

- *Alice chooses two input bits $(x_0, x_1) \in \{0,1\}$ or Abort.*
- *Bob outputs two bits (c, y) or Abort.*
- *If Alice and Bob are honest, they never Abort, $y = x_c$, Alice has no information about c and Bob has no information on $x_{\overline{c}}$. Further, c is a uniformly random bit.*
- $A_{OT} := \sup\{\Pr[\textit{Alice guesses } c \wedge \textit{Bob does not Abort}]\}$ $= \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob guesses } (x_0, x_1) \wedge \textit{Alice does not Abort}]\}$ $= \frac{1}{2} + \epsilon_B$

The reason for introducing Semi-random OT is that it is simpler to work with than 1-2 OT, and the ability to perform Semi-random OT with cheating probabilities A_{OT} and B_{OT} is equivalent to being able to perform 1-2 quantum OT with the same cheating probabilities (see Appendix).

Lastly, we note that there are also less common variants of the definition of B_{OT}, all with subtly different cheating implications. Ref. [23] defines cheating in terms of Bob being able to guess the XOR of Alice's bits, while Ref. [17] defines 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.

III. GENERIC PROTOCOL

In this section we introduce a general framework for Semi-random OT and conjecture that it includes all possible Semi-random OT protocols. We present undetectable cheating strategies available to Alice and Bob and analyse them to lower bound their cheating probabilities arising from an optimal strategy. We show that for protocols within this framework, it is always the case that

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

Further, if the states output by the protocol are pure and symmetric, then

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

We will prove this by expressing Alice's and Bob's cheating probabilities in terms of a single parameter, F, related to the fidelity of the overall output states of the protocol. 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. 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, the inherent symmetry of the protocol seems to lead to this property.

A. Protocol Framework

Here we describe the stages of a general Semi-random OT protocol with N rounds of communication between Alice and Bob. This framework is based on the general strong coin flipping protocol introduced in Ref. [4], and includes all possible Semi-random OT protocols.

1. Bob starts with the state ρ_{BM} and Alice starts with an auxiliary system A initialised to $|0\rangle\langle 0|_A$. The overall state is $\rho_{BMA} := \rho_{BM} \otimes |0\rangle\langle 0|_A$. We further suppose Alice and Bob share the counter variable i, initialised 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 $U_{MA}^{x_0x_1,i} \in \{U_{AM}^{00,i}, U_{AM}^{01,i}, U_{AM}^{11,i}, U_{AM}^{10,i}\}$. She sends system M back to Bob.

5. Bob performs the unitary operation $V_{BM}^{(i)}$.

6. The index i is incremented by 1. If $i = N+1$, the protocol proceeds to Step 7, otherwise it returns to Step 3.

7. The final output held by Bob is
$$\sigma_{BM}^{x_0x_1} := \mathrm{Tr}_A(\eta_{BMA}^{x_0x_1}), \tag{3}$$
where
$$\eta_{BMA}^{x_0x_1} := V_{BM}^{(N)} U_{MA}^{x_0x_1,N} \ldots V_{BM}^{(1)} U_{MA}^{x_0x_1,1} \rho_{BMA}. \tag{4}$$

8. Bob performs a POVM with elements $\{\Pi_{BM}^{0*}, \Pi_{BM}^{1*}, \Pi_{BM}^{*0}, \Pi_{BM}^{*1}\}$ to obtain the value of c and x_c. For example, the outcome Π_{BM}^{1*} denotes that $c = 0$ and $x_0 = 1$.

B. Honest Case

For the protocol to be correct in the honest case, we require the following conditions to hold:

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

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

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

Bob 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, i.e. he wants to know exactly which of the four σ states he holds. To do this, his optimal strategy would be to perform a minimum-error measurement. However, since the states are not fixed by the general framework, the optimum minimum-error measurement is not known. Instead, to provide a lower bound on Bob's optimal cheating probability, we assume that Bob performs the Square Root Measurement (SRM) [24]. Again, this may not be his optimal strategy, but it is a valid cheating strategy that he can employ without being caught. Using the success probability of the SRM, we can bound Bob's optimal cheating probability as [25]

$$B_{OT} \geq 1 - \frac{1}{8}\sum_{jk \neq lm} F(\sigma_{BM}^{jk}, \sigma_{BM}^{lm}), \tag{7}$$

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

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

Eqs. (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, we suppose σ^{00}_{BM} and σ^{01}_{BM} are the pair with the highest fidelity. Define

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

Then

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

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 $\{\sigma^{00}_{BM}, \sigma^{01}_{BM}, \sigma^{11}_{BM}, \sigma^{10}_{BM}\}$ forms a symmetric set[22] of pure states, then Bob's SRM measurement is successful with probability [27]

$$B^{\text{pure}}_{OT} \geq \frac{1}{4}\left(1 + \frac{1}{2}\sqrt{1-2F} + \frac{1}{2}\sqrt{1+2F}\right)^2, \tag{11}$$

for $F \in [0, 1/2]$. Since there is no reason to bias Bob's ability to cheat based on Alice's random choice of input, it seems likely that most protocols would output symmetric states and this tighter bound would apply.

D. Security against Alice

Suppose Alice is dishonest and aims to guess the value of 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 strategy, and use this to obtain a lower bound for Alice's achievable cheating probability given that she performs some optimal strategy.

Let $|\Psi\rangle_{BMAE}$ be a purification of ρ_{BMA}, where E denotes the environment. Alice also prepares an additional state $|+\rangle_D$ for use as a control qubit to perform her strategy. Since we consider information-theoretic security, Alice can do anything allowed within quantum mechanics and the overall state is

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

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^{00}_{BM} and σ^{01}_{BM}. A valid cheating strategy available to Alice is as follows. In each Step 4 of the protocol, rather than performing a unitary $U^{x_0x_1,i}_{MA}$, Alice instead performs

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

Defining $\mathcal{U} = V^{(N)}_{BM} U^{00,N}_{MA} \dots V^{(1)}_{BM} U^{00,1}_{MA}$ and $\mathcal{V} = V^{(N)}_{BM} U^{01,N}_{MA} \dots V^{(1)}_{BM} U^{01,1}_{MA}$, Alice's strategy leads to an output state

$$\begin{aligned}|\chi\rangle &:= \frac{1}{\sqrt{2}}\left(\mathcal{U}\,|\Psi\rangle_{BMAE}\,|0\rangle_D + \mathcal{V}\,|\Psi\rangle_{BMAE}\,|1\rangle_D\right)\\ &:= \frac{1}{\sqrt{2}}\left(\left|\psi^{00}\right\rangle_{BMAE}|0\rangle_D + \left|\psi^{01}\right\rangle_{BMAE}|1\rangle_D\right).\end{aligned} \tag{14}$$

This strategy is not detectable by Bob, since without access to system D it is as if Alice has performed either the $x = 00$ or $x = 01$ honest operations, each with probability 1/2. The states $\left|\psi^{jk}\right\rangle$ 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

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

where $W^{(1)}_{AE}$ and $W^{(2)}_{AE}$ are chosen to transform $\left|\psi^{00}\right\rangle$ and $\left|\psi^{01}\right\rangle$ into $\left|\phi^{00}\right\rangle$ and $\left|\phi^{01}\right\rangle$, 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

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

In Step 7 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

$$\mu_D = \frac{1}{2}\sum_{i,j,z}\left\langle\phi^i\right|\Pi^z_{MB}\left|\phi^j\right\rangle|j\rangle\langle i|_D\,, \tag{17}$$

where $i, j \in \{0, 1\}$, $z \in \{0*, 1*, *0, *1\}$ and for ease of notation we have identified $\phi^0 := \phi^{00}$ and $\phi^1 := \phi^{01}$.

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

$$\begin{aligned}\langle\phi^{jk}|\Pi^z_{BM}|\phi^{jk}\rangle &= \mathrm{Tr}_{BMAE}\Big(\Pi^z_{BM}\left|\phi^{jk}\right\rangle\left\langle\phi^{jk}\right|\Big)\\ &= \mathrm{Tr}_{BM}(\Pi^z_{BM}\sigma^{jk}_{BM}).\end{aligned} \tag{18}$$

This 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* $\mathrm{Tr}_{BM}(\Pi^z_{BM}\sigma^{jk}_{BM}) = 0$, *it holds that*

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

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

$$\Pi^z_{BM} \otimes \mathbb{1}_{AE} = \sum_n c_n\,|c_n\rangle\langle c_n|\,, \tag{20}$$

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

$$\begin{aligned}\mathrm{Tr}_{BM}(\Pi^z_{BM}\sigma^{jk}_{BM}) = 0 &\Rightarrow \langle\phi^{jk}|\Pi^z_{BM} \otimes \mathbb{1}_{AE}|\phi^{jk}\rangle = 0\\ &\Rightarrow \langle c_i|\phi^{jk}\rangle = 0\ \forall i,\end{aligned} \tag{21}$$

and the result follows. □

Using this lemma, μ_D simplifies to

$$\begin{aligned}\mu_D &= \frac{1}{2}\Bigg[\frac{1}{2}|0\rangle\langle 0|_D + \langle\phi^{01}|\Pi^{0*}_{MB}|\phi^{00}\rangle|0\rangle\langle 1|_D + \\ &\qquad \langle\phi^{00}|\Pi^{0*}_{MB}|\phi^{01}\rangle|1\rangle\langle 0|_D + \frac{1}{2}|1\rangle\langle 1|_D\Bigg] \\ &\quad + \frac{1}{2}\Bigg[\frac{1}{2}|0\rangle\langle 0|_D + \frac{1}{2}|1\rangle\langle 1|_D\Bigg] \\ &= \frac{1}{2}\mu_D^{c=0} + \frac{1}{2}\mu_D^{c=1},\end{aligned} \tag{22}$$

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 getting an outcome of $c = 1$ (i.e. Π^{*0} or Π^{*1}). Lastly, we must evaluate $\langle\phi^{01}|\Pi^{0*}_{MB}|\phi^{00}\rangle$.

To satisfy no-signalling, the density matrix in system D must be the same regardless of whether or not Bob actually performs his measurement. If Bob performs no measurement, Eq. (16) gives system D as

$$\begin{aligned}&\frac{1}{2}[|0\rangle\langle 0|_D + \langle\phi^{01}|\phi^{00}\rangle|0\rangle\langle 1|_D \\ &\quad + \langle\phi^{00}|\phi^{01}\rangle|1\rangle\langle 0|_D + |1\rangle\langle 1|_D].\end{aligned} \tag{23}$$

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

$$\begin{aligned}A_{OT} &= \frac{1}{2}\left(1 + |\langle\phi^{01}|\phi^{00}\rangle|\right) \\ &= \frac{1}{2}\left(1 + F(\sigma^{00}_{BM}, \sigma^{01}_{BM})\right) \\ &:= \frac{1}{2}\left(1 + F\right),\end{aligned} \tag{24}$$

where the second equality follows from Uhlmann's theorem [28] since $|\phi^{00}\rangle$ and $|\phi^{01}\rangle$ are the purifications of σ^{00}_{BM} and σ^{01}_{BM} with maximum overlap.

E. Result

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

$$\max\{A_{OT}, B_{OT}\} \geq 2/3. \tag{25}$$

Our results in the previous section reproduce this bound since

$$\begin{aligned}&A_{OT} = \frac{1}{2}(1 + F),\ \ B_{OT} = 1 - F \\ &\quad\Rightarrow\ \min_F\Big(\max\{A_{OT}, B_{OT}\}\Big) = \frac{2}{3}.\end{aligned} \tag{26}$$

Further, if the output states of the protocol are pure and symmetric, then we use Eq. (11) to obtain the tighter bound

$$\min_F\Big(\max\{A_{OT}, B_{OT}\}\Big) \approx 0.749. \tag{27}$$

If instead we are particularly interested in one of either A_{OT} or B_{OT}, our construction quantifies the trade-offs possible between these parameters. This situation arises in the context of quantum signatures [19], where, in the distribution stage, signing keys are partially distributed in a manner very similar to 1-2 OT. In these protocols A_{OT} is prioritised, and it is important that $A_{OT} \approx 0.5$ 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 parametrisation 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 which, in the honest case, outputs states that are almost orthogonal. Unfortunately, given $A_{OT} \approx 0.5$, our results show that it is necessary to have $B_{OT} \approx 1$. Therefore imperfect OT protocols will not prove useful for quantum signatures in the information-theoretic security setting. Nevertheless, while imperfect OT has not proved useful for quantum signatures, there may be other useful direct applications.

IV. UNAMBIGUOUS MEASUREMENTS

Classical-quantum states of the form $\rho_{XA} = \sum_{x\in\mathcal{X}} p(x)\,|x\rangle\,\langle x|_X \otimes \rho_A^x$ have been widely studied in quantum information in a variety of contexts such as channel coding, secure multiparty computations, quantum key distribution and quantum signatures to name a few. They occur when quantum states (in this case ρ_A^x) are used to transmit classical information (in this case x). Retrieving the information stored in ρ_A^x using an "optimal" measurement is a subjective concept, and the identity of the optimal measurement depends heavily on the application. For communication protocols, it is common for the optimal measurement to be a minimum-error measurement – one which decodes the classical message with the smallest probability of error. For cryptographic protocols, the optimal measurement is often one which 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 flavours: unambiguous state discrimination (USD), and unambiguous state elimination (USE). A successful USD measurement on ρ_A^x would identify x with certainty, but successful measurement outcomes do not occur with probability 1. USE measurements on the other hand can 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 1/2, and otherwise receives nothing with probability 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 computations, it seems likely that unambiguous measurements could also play a major role in the developing field.

A. Semi-random OT using Unambiguous State Elimination

In this section, we present an interesting novel application of USE measurements. We describe a protocol for implementing many runs of Semi-random OT and analyse it in the asymptotic limit. We again work in the information–theoretic security model but this time prove *upper* bounds on the cheating probabilities achievable for Alice and Bob. We show that our protocol performs better than all previous protocols, and is almost optimal with respect to the bounds derived in the previous section. The protocol proceeds as follows:

1. Alice uniformly, randomly and independently selects N elements from the set $X = \{00, 01, 11, 10\}$. 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 N two-qubit states to Bob.

3. Bob randomly selects $\sqrt{N}$ out of the N states he receives and asks Alice to reveal their identity. 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. All states used in the previous step are discarded.

5. For each of the $N-\sqrt{N}$ remaining states, Bob measures the first qubit in the Z basis and the second qubit in the X basis. These measurements consitute 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 $Y_0 = \{00, 11\}$, and one from the set $Y_1 = \{01, 10\}$. 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 $N - \sqrt{N}$ runs of Semi-random OT. Below we analyse the average cheating probabilities achieved by each of the protocols. Recall that a Semi-random OT protocol can be transformed into a standard 1-2 OT protocol with the same cheating probabilities, and vice versa (see Appendix).

The scheme described can be set in the general framework considered in the previous section by defining $U = R \otimes R$, where

$$R = |+\rangle\langle 0| - |-\rangle\langle 1|. \tag{28}$$

Alice begins with the state $|00\rangle$ and applies either $\mathbb{1}$, U, U^2 or U^3 to get 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 average cheating probabilities of $A_{OT} = 0.75$ and $B_{OT} \approx 0.729$.

B. Security against Bob

If Bob wants to cheat, then his aim is to correctly guess both x_0 and x_1. In the asymptotic limit, the fraction of states discarded for testing in Step 3 tends to zero. Since the states are prepared independently, any strategy Bob performs (including general measurements correlated across all N states) cannot have an *average* success probability (probability of correctly identifying both x_0 and x_1) which is greater than the minimum error measurement on a single state [26]. Correlated measurements performed across multiple states may give higher success probabilities if one allows postselection, but here Bob is trying to optimally cheat on *all* non-test states. Therefore, in the asymptotic limit we can bound Bob's average cheating probability across all $N - \sqrt{N} \approx N$ 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 [27]. Using this measurement Bob can guess both of Alice's input bits with probability

$$B_{OT} = \frac{1}{4}\left(1 + \frac{1}{\sqrt{2}}\right)^2 \approx 0.729. \tag{29}$$

In this case, Bob's optimal strategy is the exact strategy considered in the general scenario in Section III C.

C. 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 the ones in S. In general, Alice will generate $\rho_{AB_{11}B_{12}B_{21}B_{22}\ldots B_{N1}B_{N2}}$ 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 $\sqrt{N}$ of the 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

$$\begin{aligned}|\Psi\rangle_{B_{k1}B_{k2}A} = b_0|00\rangle_{B_{k1}B_{k2}}|0\rangle_A + b_1|++\rangle_{B_{k1}B_{k2}}|1\rangle_A \\ + b_2|11\rangle_{B_{k1}B_{k2}}|2\rangle_A + b_3|--\rangle_{B_{k1}B_{k2}}|3\rangle_A,\end{aligned} \tag{30}$$

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

Essentially, this means that Alice is restricted to the attacks considered in the general protocol analysis in Section III D – attacks that are superpositions of honest operations, and as such are always undetectable by Bob. In fact, it is numerically verifiable that an optimal strategy for Alice is to prepare

$$\frac{1}{\sqrt{2}}\left(|00\rangle_B|0\rangle_A + |++\rangle_B|1\rangle_A\right), \tag{31}$$

which corresponds exactly to the operation given in Eq. (13). Since the overlap between all adjacent states in S is 1/2, Eq. (24) implies that Alice can correctly guess the value of c with probability 0.75.

V. CONCLUSION

In this paper we introduced a general framework for studying Semi-random OT protocols. We explicitly constructed undetectable cheating strategies available to Alice and Bob and used them to lower bound the cheating probability of any Semi-random OT protocol. The derived bounds are directly transferable to standard 1-2 quantum OT allowing us to reproduce the known lower bound $p_C \geq 2/3$, or, if the states output by the protocol are pure and symmetric, improve the bound to $p_C \geq 0.749$. We conjecture that this higher bound also holds in general. As in [17], our construction has the added advantage of providing a simple quantitative relationship between Alice's and Bob's ability to cheat. In applications more sensitive to sender dishonesty than receiver dishonesty (or vice versa), our parametrisation 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. This relationship proves useful in the context of quantum signatures, where it is desirable to have $A_{OT} \approx 0.5$.

Lastly, to illustrate our construction we presented an OT protocol using unambiguous state elimination measurements to achieve cheating probabilities $A_{OT} = 0.75$, $B_{OT} \approx 0.729$ and therefore $p_C = 0.75$. This compares favourably with the previously best known protocol given in Ref. [20] in which $A_{OT} = B_{OT} = 0.75$. Since the protocol outputs symmetric states, the cheating probabilities achieved are almost tight with the bounds proved in this paper.

ACKNOWLEDGMENTS

The authors would like to thank J. Sikora and I. Kerenidis for helpful discussions. This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under EP/K022717/1 and EP/M013472/1. R.A. gratefully acknowledges EPSRC studentship funding under grant number EP/I007002/1.

VI. APPENDIX

Here we prove the following claim (stated below) contained in the main paper.

Proposition 1. *The existence of a Semi-random 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 introducing a related OT variant called Random OT (ROT), defined as follows.

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

- *Alice outputs two bits $(x_0, x_1) \in \{0, 1\}$ or Abort.*
- *Bob outputs two bits (c, y) or Abort.*
- *If Alice and Bob are honest, they never Abort, $y = x_c$, Alice has no information about c and Bob has no information on $x_{\overline{c}}$. Further, x_0, x_1 and c are uniformly random bits.*
- $A_{OT} := \sup\{\Pr[$*Alice guesses c $\wedge$ Bob does not Abort*$]\}$ $= \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[$*Bob guesses (x_0, x_1) $\wedge$ Alice does not Abort*$]\}$ $= \frac{1}{2} + \epsilon_B$

Ref. [20] 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 quantum OT with the same cheating probabilities. Following similar arguments, in the following subsections we will show that the existence of a Semi-random 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. [20], proves the proposition.

1. Semi-random OT from ROT

Let P be a ROT protocol with cheating probabilities $A_{OT}(P)$ and $B_{OT}(P)$. We construct a Semi-random OT protocol 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 Q is a Semi-random OT protocol with cheating probabilities $A_{OT}(P)$ and $B_{OT}(P)$.

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

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

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 $B_{OT}(P)$. Therefore $B_{OT}(Q) = B_{OT}(P)$.

2. ROT from Semi-random OT

Let P be a Semi-random OT protocol with cheating probabilities $A_{OT}(P)$ and $B_{OT}(P)$. We construct a ROT protocol Q with the same cheating probabilities as follows:

1. Alice picks $x_0, x_1 \in_R \{0, 1\}$ uniformly at random.

2. Alice and Bob perform the Semi-random 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 (in the honest case) since Alice chooses her input at random. Therefore Q does indeed implement ROT. From the construction of Q it is also clear that $A_{OT}(Q) = A_{OT}(P)$ and $B_{OT}(Q) = B_{OT}(P)$.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (1984) pp. 175–179.

[2] D. Mayers, Physical review letters **78**, 3414 (1997).

[3] H.-K. Lo, Physical Review A **56**, 1154 (1997).

[4] A. Kitaev, Talk at QIP (2003).

[5] C. Mochon, arXiv preprint arXiv:0711.4114 (2007).

[6] A. Chailloux and I. Kerenidis, in *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on* (IEEE, 2009) pp. 527–533.

[7] A. Chailloux and I. Kerenidis, in *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on* (IEEE, 2011) pp. 354–362.

[8] O. Goldrcich and R. Vainish, in *Conference on the Theory and Application of Cryptographic Techniques* (Springer, 1987) pp. 73–86.

[9] J. Kilian, in *Proceedings of the twentieth annual ACM symposium on Theory of computing* (ACM, 1988) pp. 20–31.

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

[11] S. Even, O. Goldreich, and A. Lempel, Communications of the ACM **28**, 637 (1985).

[12] M. O. Rabin, IACR Cryptology ePrint Archive **2005**, 187 (2005).

[13] C. Crépeau, in *Conference on the Theory and Application of Cryptographic Techniques* (Springer, 1987) pp. 350–354.

[14] G. Brassard and C. Crépeau, in *International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, 1997) pp. 334–347.

[15] G. Brassard, C. Crépeau, and S. Wolf, Journal of Cryptology **16**, 219 (2003).

[16] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, SIAM Journal on Computing **37**, 1865 (2008).

[17] A. Chailloux, G. Gutoski, and J. Sikora, arXiv preprint arXiv:1310.3262 (2013).

[18] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Physical Review A **91**, 042304 (2015).

[19] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Physical Review A **93**, 032325 (2016).

[20] A. Chailloux, I. Kerenidis, and J. Sikora, arXiv preprint arXiv:1007.1875 (2010).

[21] L. Salvail, C. Schaffner, and M. Sotáková, in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, 2009) pp. 70–87.

[22] In fact, the cited paper proves this for Random OT only, but the proof for Semi-random OT is essentially identical.

[23] J. Sikora, A. Chailloux, and I. Kerenidis, Physical Review A **89**, 022334 (2014).

[24] P. Hausladen and W. K. Wootters, Journal of Modern Optics **41**, 2385 (1994).

[25] K. M. Audenaert and M. Mosonyi, Journal of Mathematical Physics **55**, 102201 (2014).

[26] Symmetric sets of states are ubiquitous in quantum in-

formation. In this context "symmetric.

[27] P. Wallden, V. Dunjko, and E. Andersson, Journal of Physics A: Mathematical and Theoretical **47**, 125303 (2014).

[28] A. Uhlmann, Reports on Mathematical Physics **9**, 273 (1976).

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