Quantum cryptography beyond quantum key distribution: variants of quantum oblivious transfer

Quantum cryptography beyond quantum key distribution: variants of quantum oblivious transfer

Erika Andersson[a], Lara Stroh[a], Ittoop V. Puthoor[a], David Reichmuth[a], Nikola Horová[b], Robert Stárek[b], Michal Mičuda[b], Miloslav Dušek[b], and Petros Wallden[c]

[a]SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[b]Department of Optics, Faculty of Science, Palacký University, 17. listopadu 1192/12, 779 00 Olomouc, Czech Republic
[c]School of Informatics, University of Edinburgh, Edinburgh, UK

ABSTRACT

Modern cryptography is more than sending secret messages, and quantum cryptography is more than quantum key distribution. One example is oblivious transfer, which is interesting partly because it can be used to implement secure multiparty computation.[1,2] We discuss a protocol for quantum XOR oblivious transfer, and how non-interactive quantum oblivious transfer protocols can be "reversed", so that oblivious transfer is still implemented from a sender to a receiver, but so that it is the receiver who sends a quantum state to the sender, who measures it, instead of the other way round. This is useful when one party can only prepare and send quantum states, and the other party can only measure them, which is often the case in practical quantum communication systems. Both the "original" XOR oblivious transfer protocol and its reversed version have been implemented optically. We also discuss how quantum random access codes can be connected with quantum oblivious transfer.

Keywords: Quantum cryptography, quantum communication, quantum oblivious transfer

1. INTRODUCTION

Perhaps the most common variant of oblivious transfer is 1-out-of-2 oblivious transfer,[3] where a sender has two bits, and a receiver obtains one of these. The sender should have no information about which bit the receiver received, and the receiver should have no information about the bit they did not receive. Another variant of oblivious transfer is XOR oblivious transfer (XOT),[4] which is similar, except that Bob obtains either the first bit, the second bit, or their XOR. Unfortunately, perfect quantum oblivious transfer is impossible with information-theoretic security, unless we restrict the quantum memory that adversaries have access to (the so-called "bounded quantum storage model"[5]). Cheating probabilities can however be limited even when there are no restrictions on adversaries, and quantum protocols for oblivious transfer can achieve an advantage over corresponding classical protocols.

2. QUANTUM XOR OBLIVIOUS TRANSFER

We first describe a non-interactive quantum XOT protocol, where the cheating probabilities are $A_{OT} = 1/2$ for Alice and $B_{OT} = 3/4$ for Bob.[6] Let us note that even in an ideal protocol, a dishonest sender Alice can cheat with probability 1/3 using a random guess, and a dishonest receiver Bob can cheat with probability 1/2, again using a random guess. These are therefore the lowest possible cheating probabilities one can hope to achieve. The cheating probabilities $A_{OT} = 1/2$ and $B_{OT} = 3/4$ are lower than what can be achieved in classical XOT protocols. The protocol can also be said to be optimal among non-interactive protocols using pure symmetric states, since it achieves the smallest possible cheating probability 3/4 for Bob, and the smallest possible cheating probability 1/2 for Alice, given that Bob's cheating probability is 3/4 (for details see Reference 6).

Further author information: (Send correspondence to A.A.A.)
A.A.A.: E-mail: aaa@tbk2.edu, Telephone: 1 505 123 1234
B.B.A.: E-mail: bba@cmp.com, Telephone: +33 (0)1 98 76 54 32

In this protocol, Alice encodes two bit values x_0, x_1 in one of the four non-orthogonal states

$$|\phi_{x_0x_1}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + (-1)^{x_1}|1\rangle + (-1)^{x_0}|2\rangle). \tag{1}$$

The states $|\phi_{x_0x_1}\rangle$ are selected so that it is possible to unambiguously exclude two of them, meaning that it is possible to learn either x_0, x_1, or $x_0 \oplus x_1$. Because the states are non-orthogonal, it is not possible to unambiguously determine which single state was received, meaning that it is impossible for Bob to perfectly learn both bits x_0, x_1. Alice chooses her bits $(x_0, x_1) \in \{0, 1\}$ uniformly at random and sends the respective state to Bob, who makes an unambiguous quantum state elimination measurement to exclude two of the four possible states. There are six different pairs of states he can exclude. Each excluded pair corresponds to learning either x_0, x_1, or $x_0 \oplus x_1$, with either the value 0 or 1. To construct Bob's measurement operators, we need six states, each one orthogonal to a pair of states in Eq. (1). The measurement operators are then proportional to projectors onto these six states, normalised so that their sum is equal to the identity matrix. For instance, the measurement operator $\Pi_A = (1/4)(|0\rangle + |2\rangle)(\langle 0| + \langle 2|)$ will exclude the states $|\phi_{11}\rangle$ and $|\phi_{10}\rangle$, so that Bob's outcome bit will be $x_0 = 0$; similarly for the other operators. Table 1 gives the excluded pairs, the corresponding measurement operators, and the deduced output bits for Bob.

Table 1. Bob's measurement operators and outcomes

Outcome bit	Eliminated states	Measurement operator
$x_0 = 0$	$\|\phi_{11}\rangle$ and $\|\phi_{10}\rangle$	$\Pi_A = \frac{1}{4}(\|0\rangle + \|2\rangle)(\langle 0\| + \langle 2\|)$
$x_0 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{01}\rangle$	$\Pi_B = \frac{1}{4}(\|0\rangle - \|2\rangle)(\langle 0\| - \langle 2\|)$
$x_1 = 0$	$\|\phi_{11}\rangle$ and $\|\phi_{01}\rangle$	$\Pi_C = \frac{1}{4}(\|0\rangle + \|1\rangle)(\langle 0\| + \langle 1\|)$
$x_1 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{10}\rangle$	$\Pi_D = \frac{1}{4}(\|0\rangle - \|1\rangle)(\langle 0\| - \langle 1\|)$
$x_2 = 0$	$\|\phi_{01}\rangle$ and $\|\phi_{10}\rangle$	$\Pi_E = \frac{1}{4}(\|1\rangle + \|2\rangle)(\langle 1\| + \langle 2\|)$
$x_2 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{11}\rangle$	$\Pi_F = \frac{1}{4}(\|1\rangle - \|2\rangle)(\langle 1\| - \langle 2\|)$

Bob will receive either x_0, x_1 or $x_2 = x_0 \oplus x_1$ at random, but it is possible to let him choose which bit he receives using classical post-proccessing, without affecting cheating probabilities. This non-interactive XOT protocol has the same cheating probabilities as protocol (3) given by Kundu *et al.*[7] That protocol, however, uses entanglement and is interactive, that is, quantum states are sent back and forth between sender and receiver. The above protocol achieves the same cheating probabilities but is easier to implement, since it is non-interactive and does not require entanglement.

3. REVERSING QUANTUM OBLIVIOUS TRANSFER

Instead of preparing and sending one of the states $|\phi_{x_0x_1}\rangle$ as in the original protocol, Alice could prepare the state

$$|\Psi_{\text{ent}}\rangle_{AB} = \frac{1}{2}\left(|a\rangle_A |\phi_{00}\rangle_B + |b\rangle_A |\phi_{01}\rangle_B + |c\rangle_A |\phi_{10}\rangle_B + |d\rangle_A |\phi_{11}\rangle_B\right), \tag{2}$$

where $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ is an orthonormal basis for a system she keeps on her side. She sends the B system to Bob. If Alice measures the A system in the $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ basis, then this prepares one of the states $|\phi_{x_0x_1}\rangle_B$ on Bob's side. From both Bob's and Alice's viewpoints, this is equivalent to the original protocol, and their cheating probabilities remain the same. Using the definitions of $|\phi_{x_0,x_1}\rangle$, the entangled state in (2) can also

be written

$$|\Psi_{\rm ent}\rangle_{AB} = \frac{1}{\sqrt{3}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B),$$

where

$$\begin{aligned} |0\rangle_A &= \frac{1}{2}(|a\rangle_A + |b\rangle_A + |c\rangle_A + |d\rangle_A), \quad |1\rangle_A = \frac{1}{2}(|a\rangle_A + |b\rangle_A - |c\rangle_A - |d\rangle_A) \\ |2\rangle_A &= \frac{1}{2}(|a\rangle_A - |b\rangle_A + |c\rangle_A - |d\rangle_A), \quad |3\rangle_A = \frac{1}{2}(|a\rangle_A - |b\rangle_A - |c\rangle_A + |d\rangle_A), \end{aligned} \tag{3}$$

are orthonormal states, and we have defined a fourth basis ket $|3\rangle_A$. Both Alice's and Bob's state spaces for the state $|\Psi_{\rm ent}\rangle_{AB}$ are three-dimensional; its Schmidt number is 3. Alice's measurement in the $|a\rangle_A, |b\rangle_A, |c\rangle_A, |d\rangle_A$ basis can be understood as a realisation, with a Neumark extension using the auxiliary basis state $|3\rangle_A$, of a generalised quantum measurement with measurement operators given by

$$\begin{aligned} \Pi_{00} &= \frac{1}{4}(|0\rangle + |1\rangle + |2\rangle)(\langle 0| + \langle 1| + \langle 2|), \quad \Pi_{01} = \frac{1}{4}(|0\rangle - |1\rangle + |2\rangle)(\langle 0| - \langle 1| + \langle 2|), \\ \Pi_{11} &= \frac{1}{4}(|0\rangle - |1\rangle - |2\rangle)(\langle 0| - \langle 1| - \langle 2|), \quad \Pi_{10} = \frac{1}{4}(|0\rangle + |1\rangle - |2\rangle)(\langle 0| + \langle 1| - \langle 2|). \end{aligned} \tag{4}$$

If instead Bob prepares the state $|\Psi_{\rm ent}\rangle_{AB}$, sends the A system to Alice, and measures his B system using the measurement he makes in the original protocol, then this prepares one of six states $|\phi_{x_i=b}\rangle$ on Alice's side. This gives a "reversed" protocol. That is, starting from the entangled state $|\Psi_{\rm ent}\rangle_{AB}$, either the original or a reversed protocol can be implemented. In both cases, Alice makes the measurement she would make in the reversed protocol, and Bob makes the measurement he would make in the original protocol. What determines whether the procedure is equivalent to the original or reversed protocol is who prepares the state $|\Psi_{\rm ent}\rangle_{AB}$. This can matter, because Alice and Bob are not guaranteed to follow the protocol, and could prepare some other state if they are dishonest.

In the reversed case, Bob is the sender of the quantum state, so he has the freedom of choosing whatever state he wants to send, potentially increasing his cheating probability. Alice's cheating probability might on the other hand decrease, since she no longer can choose to send different states (only to alter her measurement, made on the state Bob prepared). However, it can be shown that both Alice's and Bob's cheating probabilities in the reversed protocol are equal to their cheating probabilities in the original unreversed version of the protocol. As in the unreversed case, a dishonest Alice wants to know which of the three bits Bob has obtained. Therefore, she needs to distinguish between the three mixtures of the states corresponding to the same b. Her optimal cheating strategy, applying a minimum-error measurement on the resulting mixed states, yields her cheating probability $A^r_{OT} = 1/2$. Also dishonest Bob's aim in the reversed case stays the same. He wants to know all three bits, instead of just one of x_0, x_1, and $x_2 = x_0 \oplus x_1$. It is enough if he learns any two of these bits. His best cheating strategy is to send one of the eigenstates corresponding to the highest eigenvalue of Alice's measurement operators. That is, he will send $(|0\rangle+|1\rangle+|2\rangle)/\sqrt{3}$ for $x_0x_1 = 00$, $(|0\rangle-|1\rangle+|2\rangle)/\sqrt{3}$ for $x_0x_1 = 01$, $(-|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}$ for $x_0x_1 = 11$, or $(-|0\rangle - |1\rangle + |2\rangle)/\sqrt{3}$ for $x_0x_1 = 10$, all of which have 3/4 as their corresponding eigenvalue. Thus, with a cheating probability of $B^r_{OT} = 3/4$, Bob will then be able to learn both x_0 and x_1.

In order to illustrate the generality of this procedure, let us "reverse" the protocol for 1-out-of-2 quantum oblivious transfer in Reference 8. Here, Alice sends one of the two-qubit states $|0\rangle|0\rangle, |+\rangle|+\rangle, |1\rangle|1\rangle, |-\rangle|-\rangle$ to Bob, encoding her bit values $00, 01, 11$ and 10, respectively, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Since each of Alice's four states are symmetric under exchange of the two qubits, the state space is actually three-dimensional. Bob measures one qubit in the $|0\rangle, |1\rangle$ basis and the other one in the $|+\rangle, |-\rangle$ basis, which allows him to rule out two of the four possible states, so that he can infer the value of either Alice's first bit or her second bit (never their XOR). We will here use an equivalent set of four states with the same pairwise overlaps,

$$|\phi'_{x_0x_1}\rangle = \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_0}\frac{1}{2}|1\rangle + (-1)^{x_1}\frac{1}{2}|2\rangle, \tag{5}$$

making it immediately clear that the state space is three-dimensional. Alice could now instead prepare the state

$$\begin{aligned} |\Phi'_{\text{ent}}\rangle &= \frac{1}{2}(|a\rangle_A |\phi'_{00}\rangle_B + |b\rangle_A |\phi'_{01}\rangle_B + |c\rangle_A |\phi'_{01}\rangle_B + |d\rangle_A |\phi'_{11}\rangle_B) \\ &= \frac{1}{\sqrt{2}} |0\rangle_A |0\rangle_B + \frac{1}{2} |1\rangle_A |1\rangle_B + \frac{1}{2} |2\rangle_A |2\rangle_B , \end{aligned} \tag{6}$$

with the same definition of the states $|0\rangle_A , |1\rangle_A , |2\rangle_A$ as in equation (3), and send the B system to Bob. If Alice measures the A system in the $|a\rangle_A , |b\rangle_A , |c\rangle_A , |d\rangle_A$ basis – or makes the equivalent four-outcome generalised measurement in the three-dimensional space spanned by the states $|0\rangle_A , |1\rangle_A , |2\rangle_A$ – then this prepares one of the states $|\phi'_{x_0 x_1}\rangle$ on Bob's side. This is then equivalent to Alice's actions in the protocol in Reference 8. Preparing the above entangled state is also how a dishonest Alice would cheat in the protocol in Reference 8. She can then always revert to effectively sending Bob one of the states she should have sent him, if Bob decides to test the state she has sent, which he does with a small but nonzero probability. If Alice does go ahead with cheating, she measures the A system in a way that optimally lets her deduce which bit value (x_0 or x_1) Bob has obtained, in which case she can learn this with probability 3/4. If Bob does not test any of the states Alice sends, one can show that she in fact can cheat with probability 1 (and that it does not help if Bob randomly chooses which qubit he measures in what basis). If Bob is dishonest, he can determine which one of the four states $|\phi_{x_0 x_1}\rangle$ Alice has sent him with probability ≈ 0.729.

If instead Bob would prepare the entangled state and send the A system to Alice, we obtain a reversed version of the protocol in Reference 8. One can show that the measurement an honest Bob makes prepares one of the four states

$$\begin{aligned} |\phi_{x_0=0}\rangle &= \frac{1}{\sqrt{2}}(|a\rangle_A + |b\rangle_A), \quad |\phi_{x_1=0}\rangle = \frac{1}{\sqrt{2}}(|a\rangle_A + |c\rangle_A), \\ |\phi_{x_1=1}\rangle &= \frac{1}{\sqrt{2}}(|b\rangle_A + |d\rangle_A), \quad |\phi_{x_1=0}\rangle = \frac{-1}{\sqrt{2}}(|c\rangle_A + |d\rangle_A) \end{aligned} \tag{7}$$

on Alice's side. If Bob is dishonest, he can send Alice some other state(s) in the three-dimensional state space spanned by these states; the state $(|a\rangle_A - |b\rangle_A - |c\rangle_A + |d\rangle_A)/2$ is orthonormal to all of the above four states. It is necessary to re-analyze what the cheating probabilities are in the reversed protocol, since they may change when a protocol is reversed. Bob's cheating probability could increase, since more cheating strategies are available to him, while Alice's cheating probability could decrease. In this case, it can be shown that Bob's cheating probability increases to 3/4 if Alice does not test the states he prepares, and remains equal to ≈ 0.729 if she does test a small fraction of his states. Alice's cheating probability is equal to 3/4 (and is not affected by whether or not she tests Bob's states – in the reversed protocol, Alice's tests only serve to decrease Bob's cheating probability).

4. QUANTUM OBLIVIOUS TRANSFER AND RANDOM ACCESS CODES

Cheating probabilities which are higher than what can be achieved using a random guess (but still limited) is one in which way an oblivious transfer protocol can be imperfect. Another type of "imperfection" is to allow for errors in the bit values received, even when both sender and receiver are acting according to the protocol. This is sometimes called an "incomplete" protocol, and can allow for lower cheating probabilities than in corresponding "complete" protocols.

For example, let us consider incomplete 1-out-of-2 oblivious transfer where the sender can only cheat with probability $p_s = 1/2$, and the receiver can cheat with a probability as low as possible, for a fixed probability p_f that the receiver will obtain an incorrect bit value even if both sender and receiver are following the protocol.[9] (If $p_f = 0$, corresponding to a complete protocol, then the receiver can necessarily cheat with probability 1 whenever the sender's cheating probability is equal to 1/2.) One optimal class of protocol is where Alice encodes her two bits using one of the four qubit states

$$|\psi_{00}\rangle = a |0\rangle + b |1\rangle , \quad |\psi_{01}\rangle = a |0\rangle + ib |1\rangle , |\psi_{11}\rangle = a |0\rangle - b |1\rangle , \quad |\psi_{10}\rangle = a |0\rangle - ib |1\rangle , \tag{8}$$

where $0 \leq |a|, |b| \leq 1$, with $|a|^2 + |b|^2 = 1$. This set of states is symmetric with the symmetry operation $U = |0\rangle\langle 0| + i|1\rangle\langle 1|$, meaning that $|\psi_{01}\rangle = U|\psi_{00}\rangle, |\psi_{11}\rangle = U|\psi_{01}\rangle, |\psi_{10}\rangle = U|\psi_{11}\rangle$, where $U^4 = \hat{1}$. For $a = b = 1\sqrt{2}$ we obtain the eigenstates of σ_x and σ_y, that is, four states isomorphic to the "Wiesner" or BB84 states, which are eigenstates of σ_x and σ_z. By varying a and b, we will generally obtain lower cheating probability p_r for the receiver, and higher failure probability p_f, than for the "Wiesner" states. The sender's cheating probability is always equal to $1/2$, since the receiver is choosing one of two different measurements for obtaining x_0 or x_1. For $|a| = 1, b = 0$ or $a = 0, |b| = 1$, all four states are equal to the same state, giving $p_f = 1/2$ and $p_r = 1/4$. It can be shown that more generally[9]

$$\begin{aligned} p_f &= \frac{1}{2}(1 - \sqrt{2}|ab|), \\ p_r &= \frac{1}{4}(|a| + |b|)^2 = \frac{1}{4}(1 + 2|ab|), \end{aligned} \tag{9}$$

and it therefore also holds that

$$p_r = \frac{1}{\sqrt{2}}(1 - p_f) + \frac{1}{4}(1 - \sqrt{2}), \tag{10}$$

that is, Bob's cheating probability p_r is a straight line as a function of the protocol success probability $1 - p_f$. It can also be shown that this is the lowest possible p_r for a given p_f with p_f in the range $p_f^W \leq p_f \leq 1/2$. Moreover, it can be shown that in the range $p_f \lesssim 0.31$, this class of protocols outperform corresponding classical protocols.

This can be seen as a generalisation of complete oblivious transfer, but also as a generalization of random access codes (RACs).[10,11] For a RAC, in the simplest case (which will correspond most closely to 1-out-of-2 oblivious transfer), one restricts the sender to use one bit to encode two bit values. The sender does not know which bit the receiver wants, but aims for the receiver to correctly retrieve the bit of their choice with a probability that is as high as possible. For a corresponding quantum random access code (QRAC),[10,11] the sender is restricted to using one qubit for encoding two classical bit values.

Unlike in oblivious transfer, in a RAC or QRAC one is not concerned with the probability that the sender guesses which bit value the receiver wants to access. But since the receiver is choosing between two measurements, depending on which bit value they choose, the sender is not able to tell better than with a random guess. In oblivious transfer protocols where Bob is choosing between two measurements, depending on whether he is trying to retrieve x_0 or x_1, the sender Alice can correctly guess which bit the receiver Bob wants only with probability $1/2$, which is analogous to a RAC or QRAC.

Another difference between RACS and QRACs on one hand, and oblivious transfer on the other hand, is that for oblivious transfer, there is no restriction on the dimensionality of the state space that can be used. Instead of fixing the dimensionality of the state space, one wants to restrict the probability for the receiver to retrieve all of the sent information. In this sense, incomplete oblivious transfer is a generalisation of a QRAC (as well as being a generalization of complete or "perfect" oblivious transfer). That is, for incomplete oblivious transfer, one is concerned with (i) maximising the probability that the receiver correctly obtains their chosen bit value, as in a RAC, but also (ii) minimising the probability that they correctly obtain both bit values, which generalises the restriction of sending a single bit or qubit. A remaining point is that in complete protocols for oblivious transfer, the receiver should always correctly retrieve their chosen bit value, whereas in a RAC or QRAC, and in an incomplete protocol for oblivious transfer, the probability for the bit value to be correct is generally lower than 1. That is, incomplete protocols for oblivious transfer can be said to interpolate between or "connect" random access codes and oblivious transfer, generalizing both functionalities.

5. CONCLUSIONS

The protocols for quantum oblivious transfer we have considered are all non-interactive, which means that there is a single state transmission of a quantum state from one party to another, followed by a quantum measurement, and do not require entanglement. They are easier to realise than protocols which are interactive and use entanglement. Non-interactive protocols can be "reversed" by reimagining them in terms of a shared entangled state. This allows us to implement oblivious transfer from a sender to a receiver, or vice versa,

even if only one of the parties can prepare and send quantum states, and the other party can only receive and measure quantum states. Both the original and reversed versions of the XOR oblivious transfer protocol, including optimal cheating strategies, have been realised optically, with results that well agree with theoretical performance parameters, demonstrating their feasibility.[6] We also discussed oblivious transfer protocols where the received bit values can sometimes be incorrect. This allows us to lower cheating probabilities, as compared with protocols where the bit values always have to be correct. It can also be seen as a generalisation of quantum random access codes, connecting these two functionalities.

ACKNOWLEDGMENTS

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grants No. EP/T001011/1 and EP/R513386/1. R.S., N.H., and M.D. acknowledge support by Palacký University under Grants No. IGA-PrF-2021-006 and IGA-PrF-2022-005.

REFERENCES

[1] Kilian, J., "Founding cryptography on oblivious transfer," in Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC '88 (Association for Computing Machinery, New York, NY, USA, 1988) p. 20–31.

[2] Ishai, Y., Prabhakaran, M., and Sahai, A., "Founding cryptography on oblivious transfer – efficiently," in Advances in Cryptology – CRYPTO 2008, edited by David Wagner (Springer Berlin Heidelberg, Berlin, Heidelberg, 2008) pp. 572–591.

[3] Even, S., Goldreich, O., and Lempel, A., "A randomized protocol for signing contracts," Commun. ACM **28**, 637–647 (1985).

[4] Brassard, G., Crépeau, C., and Wolf, S., "Oblivious transfers and privacy amplification," J. Cryptol. **16**, 219–237 (2003).

[5] Damgård, I., Fehr, S., Salvail, L., and Schaffner, C. "Cryptography in the bounded quantum-storage model," SIAM Journal on computing **37**, 1865–1890 (2008).

[6] Stroh, L., Horová, N., Stárek, R., Puthoor, I. V., Mičuda, M., Dušek, M., and Andersson, E., "Non-interactive XOR quantum oblivious transfer: optimal protocols and their experimental implementations", *ArXiv:2209:11300* (2022).

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

[8] Amiri, R. *et al.*, "Imperfect 1-Out-of-2 Quantum Oblivious Transfer: Bounds, a Protocol, and its Experimental Implementation", PRX Quantum **2**, 010335 (2021).

[9] Reichmuth, D., Puthoor, I. V., Wallden, P., and Andersson, E., to be submitted.

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

[11] Ambainis, A., Nayak, A., Ta-Shma, A., and Vazirani, U., Journal of the ACM, **49**, 496 (2002).