

Incomplete quantum oblivious transfer with perfect one-sided security

David Reichmuth,¹ Ittoop V. Puthoor^{2,*}, Petros Wallden³, and Erika Andersson^{1,†}

¹*IPaQS, Heriot-Watt University, Edinburgh, United Kingdom*

²*School of Computing, Newcastle University, Newcastle upon Tyne, United Kingdom*

³*School of Informatics, University of Edinburgh, Edinburgh, United Kingdom*



(Received 8 October 2024; accepted 23 July 2025; published 10 November 2025)

Oblivious transfer is a fundamental cryptographic primitive that is useful for secure multiparty computation. There are several variants of oblivious transfer. We consider 1-out-of-2 oblivious transfer, where a sender sends two bits of information to a receiver. The receiver receives only one of the two bits, while the sender does not know which bit the receiver has received. Perfect quantum oblivious transfer with information-theoretic security is known to be impossible. We aim to find the lowest possible cheating probabilities. Bounds on cheating probabilities have been investigated for “complete” protocols, where if both parties follow the protocol, the bit value obtained by the receiver matches the sender’s bit value. We instead investigate incomplete protocols, where the receiver obtains an incorrect bit value with probability p_f . We present optimal noninteractive protocols where Alice’s bit values are encoded in four symmetric pure quantum states, and where she cannot cheat better than with a random guess. We find the protocols such that for a given p_f , Bob’s cheating probability p_r is as low as possible, and vice versa. Furthermore, we show that noninteractive quantum protocols can outperform noninteractive classical protocols and give a lower bound on Bob’s cheating probability in interactive quantum protocols. Importantly for optical implementations, our protocols do not require entanglement nor quantum memory.

DOI: [10.1103/d5yk-nn96](https://doi.org/10.1103/d5yk-nn96)

I. INTRODUCTION

1-out-of-2 oblivious transfer (OT) is a cryptographic primitive where a sender Alice holds two bits and a receiver Bob receives one of them. The receiver should not know the other bit, and the sender should not know which bit the receiver obtained. A dishonest sender Alice will attempt to find out which bit Bob obtained, and a dishonest receiver Bob will attempt to learn both bit values. Apart from 1-out-of-2 oblivious transfer [1,2], there are other variants. In Rabin oblivious transfer [3], for example, a single bit is either received or not. Oblivious transfer is important not the least because it is universal for multiparty computation [4].

Oblivious transfer is a fundamental cryptographic primitive that enables many secure protocols, including secure multiparty computation and private information retrieval, tasks that offer great value in cyber security applications. Unlike quantum key distribution (QKD), where the two parties that intend to communicate trust each other, in OT the involved parties can both be adversarial. In other words, the functionality achieved, the trust setting, and the applications where OT can be used are radically different from QKD, which has also been much more investigated. On the other hand, the technological requirements of the parties and the

quantum communication required are, in general, very similar for OT and QKD, although a full comparison can only be made given the details of an OT and a QKD protocol. Also, unlike for QKD, information-theoretically secure perfect quantum oblivious transfer is impossible [5,6]. It does become possible with restrictions on quantum memory for cheating parties [7]. Variants of oblivious transfer where the parties are constrained by special relativity are also possible [8]. While perfect quantum oblivious transfer is impossible without restrictions on cheating parties, quantum protocols with bounded cheating probabilities for the (otherwise unrestricted) parties are still possible. Currently known protocols, however, do not achieve cheating probabilities that are tight with existing lower bounds. The known bounds also hold specifically for “complete” protocols [9–12], where completeness means that the protocol always works correctly if the parties are honest. For such protocols, a lower bound on the greater of Alice’s and Bob’s cheating probabilities is $2/3$ in general [11,12] and ≈ 0.749 if symmetric pure states are used [12]. One variant of oblivious transfer is XOR oblivious transfer (XOT), where the sender has two bits and a receiver obtains the first bit, the second bit, or their XOR. Using pure symmetric states, the XOT protocol has been demonstrated to be an optimal protocol having lower cheating probabilities than the classical XOT protocols [13]. Another variant of OT is Rabin oblivious transfer, where the sender holds a bit and the receiver either obtains the bit or not with some probability. It has been demonstrated that quantum Rabin OT is possible using two pure states and is shown that the quantum protocol outperforms the classical protocols [14].

We will here instead examine noninteractive incomplete protocols for 1-out-of-2 quantum oblivious transfer.

*Contact author: ittoop.puthoor@newcastle.ac.uk

†Contact author: erika.andersson@hw.ac.uk

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.

Noninteractive means that there is no back-and-forward communication, either classical or quantum; the protocols have a single step, where one party sends classical and/or quantum information to the other party, who measures what is received. Some of our results also provide bounds valid for interactive protocols. “Incomplete” means that a protocol might fail even when both parties follow the protocol. Here, protocol failure will mean that Bob obtains an incorrect bit value. There are several reasons to investigate protocols that can fail. It turns out that a nonzero failure probability means that cheating probabilities can be lowered. There is also a connection to quantum random access codes (QRACs) [1,15], as will be discussed at the end; incomplete oblivious transfer can be seen as a generalization that “interpolates” between random access codes (RACs) and complete oblivious transfer. Noise and imperfections will also often lead to a nonzero failure probability in implementations. Vulnerability that arises as a result of imperfect implementation such as side-channel attacks or quantum hacking [16] is something that needs to be considered separately for each new quantum cryptographic primitive. This goes beyond the scope of this work. Specifically, the fact that all “legitimate” parties (sender and receiver) can be adversarial, and not only external third parties, makes such analysis harder and requires careful thought.

Specifically, we investigate incomplete protocols for quantum oblivious transfer, where the sender Alice can never cheat any better than with a random guess. That is, the security against a cheating Alice is “perfect.” For a given protocol failure probability p_f , the goal is then to minimize Bob’s cheating probability p_r , and vice versa. Bob’s cheating probability is the probability that he correctly guesses both of Alice’s bit values.

We discuss the definition of protocol failure in Sec. II, noninteractive classical protocols in Sec. III, and some general properties of incomplete quantum oblivious transfer in Sec. IV. In Sec. V, we find the lowest possible cheating probability for receiver Bob for a given protocol failure probability for protocols using symmetric pure states, and in Sec. VI, we give examples of optimal quantum protocols of this type. The example protocols are feasible to realize with current technology, for example, using photons. We finish with a discussion.

II. DEFINITION OF PROTOCOL FAILURE

“Failure” could in principle mean either that Bob obtains an incorrect bit value or that he fails to obtain any bit value at all. An incorrect bit value could be due to noise or randomness that is in principle avoidable (but might be intentional), or, in a quantum protocol, due to the fact that nonorthogonal quantum states cannot be perfectly distinguished from each other. Bob could fail to obtain any bit value at all again because of randomness or noise, e.g., if no detector on Bob’s side registers anything. Or, in a quantum protocol, if Bob is for example using an unambiguous quantum measurement to determine one of Alice’s bit values, then such a measurement might give an inconclusive result, meaning that Bob fails to obtain a bit value even if the implementation is perfect.

We will concentrate on incomplete protocols where Bob always obtains a bit value, which is incorrect with probability p_f , and where Bob generally does not know if his bit value is

correct or not. The other type of incomplete protocol would be if Bob sometimes fails to obtain any bit value at all (in addition, when he does obtain a bit value, it might be guaranteed to be correct or might be correct with a probability less than 1). If Bob fails to obtain a bit value at all, then this will be obvious to Bob. If both parties are honest, they could agree to simply repeat the protocol until a bit value is obtained by Bob (with Alice using new bit values each time). Taken together, if the bit value that Bob in the end obtains is guaranteed to be correct, this would then simply be another instance of a complete protocol for quantum oblivious transfer. If the bit value obtained by Bob in the end is sometimes incorrect, then the protocol is of the type we consider. Apart from repeating the protocol until success, the parties could also agree that if Bob fails to obtain a bit value, he makes a random guess to produce a bit value. In this case, Bob again obtains an incorrect bit value with some probability. This is therefore again a protocol of the type we will be considering. Generally, Bob’s lowest failure probability p_f will be achieved when he is never certain that the bit value he received is correct (because Bob’s optimal measurement will be a minimum-error measurement).

To summarize, we will consider the case where Bob always obtains a bit value, which is incorrect with probability p_f , and where Bob does not know when the protocol has failed (or at least does not always know). In the quantum protocols we will examine, Alice does not know whether the protocol has succeeded or failed.

Cheating probabilities could be calculated either as overall cheating probabilities, whether the protocol has failed or not, or as conditional cheating probabilities, conditioned on the protocol failing or succeeding. In the quantum protocols we consider, the honest parties do not know whether a particular run of the protocol has failed or not. It therefore seems most natural to consider overall cheating probabilities. In the classical noninteractive protocols below, on the other hand, Alice may know whether or not a bit value is correct (but not whether Bob has received it). This can be seen as an advantage for Alice. We will nevertheless compare overall cheating probabilities for classical and quantum protocols.

III. CLASSICAL NONINTERACTIVE PROTOCOLS

As always in quantum cryptography, we will need to compare our quantum protocols to classical protocols, and hence we will need to know how low cheating probabilities can be in classical protocols. First, recall that in any complete protocol for 1-out-of-2 oblivious transfer (quantum or classical), either party can always successfully cheat with a probability of $1/2$ using a random guess. Furthermore, in protocols with information-theoretic (as opposed to computational) security, if one party can successfully cheat only with probability $1/2$, then the other party can necessarily cheat with probability 1 [11]. This holds both for “classical” and for quantum protocols that are complete. A classical protocol achieving this is where Alice sends both bits to Bob, who (if he is honest) reads out only one of them. Alice’s cheating probability is then $1/2$ (her probability to correctly guess which bit Bob obtains), and Bob’s cheating probability is 1 (his probability to obtain both of Alice’s bits). Conversely, if Alice sends one of the bits to Bob and “forgets” which one she sent if she is honest, then

Alice can cheat with probability 1 and Bob can cheat with probability $1/2$.

Let us now consider incomplete classical protocols that fail with some probability p_f , where the sender can only cheat with probability $1/2$, to see how much the receiver's cheating probability can be lowered. Let us start with an example. Suppose that Alice sends two bits to Bob, but that she (or a "noisy environment" that Bob cannot control or access) flips one of her bit values with some probability and leaves the other one unchanged. Each bit is equally likely to be the flipped one. Suppose that the first bit is flipped and the second bit left correct with probability $p \leq 1/3$ and the first bit left correct and the second one flipped also with probability p . Both bit values are left correct with probability $1 - 2p \geq 1/3$ (and it never happens that both bit values are flipped). The failure probability is then $p_f = p$, which is the probability that an honest Bob is unlucky and reads out a flipped bit value. Bob's cheating probability if he reads out both bits is $1 - 2p = 1 - 2p_f$.

For a noninteractive classical protocol, this turns out to be optimal, in the sense that for a given $p_f \leq 1/3$, Bob's cheating probability p_r is as small as it can be, keeping Alice's cheating probability equal to $p_s = 1/2$. Let us consider a general classical noninteractive protocol where Alice sends some information to Bob, who then reads out one bit if he is honest and both bits if he is dishonest. "Reading out" may involve some information processing; we are placing no computational restrictions on either Alice or Bob. Classical information can be copied, and therefore, for example, the probability that if Bob chooses to read out the first bit value, it is correct, is independent of whether or not he also chooses to read out the second bit value. (This would not be the case in a quantum protocol, where Bob generally, if he learns about a particular property of a quantum state, will be able to obtain less information about something else.)

Let us denote the probability that both bit values can be correctly read out by Bob by c , the probability that the first bit value is correct and the second is wrong by p , the probability that the first bit value is correct and the second is wrong by q , and the probability that both bit values are wrong by w . It holds that $c + p + q + w = 1$. We can without loss of generality assume that c is larger than p , q , and w (if this is not the case to start with, then Bob can flip bit values to make it so). Bob's cheating probability will then be $p_r = c$. An honest Bob's success probability to obtain one bit value correctly, if he randomly reads out either the first or the second bit, is $1 - p_f = c + (p + q)/2$. The probability that his bit value is wrong is $p_f = w + (p + q)/2$. It therefore holds that

$$p_r = c = 1 - w - q - p = 1 - 2p_f + w. \quad (1)$$

In order to minimize Bob's probability to cheat, for a given p_f for an honest Bob, Alice should clearly choose w as small as possible. This means that in addition to $c = \text{Max}(c, p, q, w)$, Alice will ensure that $w = \text{Min}(c, p, q, w)$. Other choices are possible, but will lead to a higher cheating probability for Bob, for a given protocol success probability, and we (and Alice) are interested in the *lowest* possible cheating probability for Bob. If $c \geq 1/3$, then Alice can choose p, q , and w so that $w = 0$, and it then holds that $p_r = 1 - 2p_f$. Generally, when $0 \leq p_f \leq 1/3$, for classical

noninteractive protocols it therefore holds that

$$p_r \geq 1 - 2p_f. \quad (2)$$

If $c \leq 1/3$, then the smallest w Alice can choose is $w = 1 - 3c$, by picking $p = q = c$. In this case, the protocol failure probability $p_f = 1 - 2c = 1 - 2p_r$. When $p_f \geq 1/3$, it therefore holds that Bob's cheating probability is bounded as

$$p_r \geq \frac{1}{2}(1 - p_f). \quad (3)$$

A receiver who performs the protocol as if they are honest, but then randomly guesses the bit value they do not obtain, will correctly guess both bit values with probability $p_r = \frac{1}{2}(1 - p_f)$. Equation (3) therefore means that for $p_f \geq 1/3$, this is Bob's best cheating strategy.

This combined bound in Eqs. (2) and (3), for noninteractive classical protocols where the sender can only cheat with probability $p_s = 1/2$, will serve as a benchmark for our quantum protocols. It turns out that for corresponding noninteractive quantum protocols, the cheating probability for the receiver Bob can be *less* than in classical protocols.

IV. INCOMPLETE QUANTUM PROTOCOLS

We will now consider quantum oblivious transfer with a failure probability p_f , where the sender can only cheat with probability $p_s = 1/2$, that is, no better than using a random guess. As mentioned above, we define the sender's and receiver's cheating probabilities as their overall probability to cheat successfully, independently of whether the protocol fails or not. This makes sense since the parties will not know whether or not the protocol has failed. (In complete quantum protocols, dishonest parties will also not always know whether the information they have obtained is correct, if they maximize their cheating probabilities.)

We will consider noninteractive protocols where a quantum state is sent only once from sender to receiver, who makes a final measurement. In general, protocols for quantum oblivious transfer can have several steps where quantum states are sent back and forth, such as in the protocol by Chailloux *et al.* [10] and as in the general framework in Ref. [12]. Some of our results generalize to such protocols. In particular, a dishonest party can always cheat by honestly performing the protocol until the last step, and then cheating by altering their final measurement. The cheating probability for this particular strategy then gives a lower bound for their general cheating probability. That is, lower bounds for cheating in noninteractive protocols also give lower bounds for cheating in interactive protocols.

In 1-out-of-2 oblivious transfer, Alice has two classical input bits x_0 and x_1 , and Bob has one input bit c . Usually one considers the case where Alice and Bob select their bit values randomly. Suppose that an honest sender Alice encodes her two classical bit values in one of the quantum states $\sigma_{00}, \sigma_{01}, \sigma_{10}$, and σ_{11} , where the subscripts indicate Alice's bit values. She sends this quantum state to Bob, who (if he is honest) selects between making a measurement to learn the value of the first bit ($c = 0$) or a measurement to learn the value of the second bit ($c = 1$), with equal probability. Bob choosing between two measurements, and the fact that there is no further communication with Alice, will guarantee

that Alice's overall cheating probability is $1/2$. By no signaling, she cannot tell which measurement Bob is choosing or indeed whether Bob has made a measurement at all [17]. She therefore cannot cheat better than with a random guess. Bob's cheating probability, on the other hand, can be higher than $\frac{1}{2}(1 - p_f)$, which he would achieve with a random guess. Conversely, if Alice should be able to cheat no better than with a random guess, then she should not be able to distinguish between Bob obtaining the first or the second bit value. It follows that whatever Bob does can, from Alice's point of view, be described as him choosing between two different generalized measurements, depending on which bit value he wishes to obtain.

We will now examine how well the protocol works if both parties are honest. If Bob is honest and wishes to learn the value of the first bit, then he performs a measurement to distinguish between the sets of states $S_{00} = \{\sigma_{00}, \sigma_{01}\}$ and $S_{01} = \{\sigma_{10}, \sigma_{11}\}$, where all states are equiprobable. This is the same as making a measurement to distinguish between the equiprobable states $\frac{1}{2}\sigma_{00} + \frac{1}{2}\sigma_{01}$ and $\frac{1}{2}\sigma_{10} + \frac{1}{2}\sigma_{11}$. The minimum-error measurement that distinguishes between two states ρ_0 and ρ_1 , occurring with probabilities p_0 and p_1 , has the error probability

$$p_{\text{err}} = \frac{1}{2}(1 - \text{Tr}|p_0\rho_0 - p_1\rho_1|). \quad (4)$$

The measurement is a projection in the eigenbasis of $p_0\rho_0 - p_1\rho_1$. The probability that Bob obtains an incorrect value for the first bit, if he uses a minimum-error measurement, is therefore

$$p_{f,0} = \frac{1}{2}\left(1 - \frac{1}{4}\text{Tr}|\sigma_{00} + \sigma_{01} - \sigma_{10} - \sigma_{11}|\right). \quad (5)$$

If Bob wishes to learn the second bit, then he performs a measurement to distinguish between the sets of states $S_{10} = \{\sigma_{00}, \sigma_{10}\}$ and $S_{11} = \{\sigma_{01}, \sigma_{11}\}$, where again all states are equiprobable. This is equivalent to distinguishing between the equiprobable states $\frac{1}{2}\sigma_{00} + \frac{1}{2}\sigma_{10}$ and $\frac{1}{2}\sigma_{01} + \frac{1}{2}\sigma_{11}$. Bob's minimum-error measurement gives an incorrect value for the second bit with the probability

$$p_{f,1} = \frac{1}{2}\left(1 - \frac{1}{4}\text{Tr}|\sigma_{00} + \sigma_{10} - \sigma_{01} - \sigma_{11}|\right). \quad (6)$$

On average, Bob's probability to obtain an incorrect bit value is

$$p_f = \frac{1}{2}(p_{f,0} + p_{f,1}). \quad (7)$$

If Bob's failure probability is independent of whether he tries to obtain the first or the second bit, then $p_{f,0} = p_{f,1} = p_f$.

We already remarked that Alice's best cheating strategy is a random guess. If Bob wishes to cheat, then he needs to distinguish between all four of Alice's states. His optimal measurement for this necessarily gives the wrong result at least as often as either of the above two measurements where he learns only one bit value. This means that Bob's cheating probability p_r , defined as the probability that he can correctly guess both of Alice's bit values, is generally strictly smaller than either of $p_{f,0}$, $p_{f,1}$, or p_f above. That is, it holds that

$$p_r \leq 1 - p_{f,0}, \quad p_r \leq 1 - p_{f,1}, \quad \text{and} \quad p_r \leq 1 - p_f, \quad (8)$$

and the inequalities are strict except in special cases (which would correspond to poorly designed protocols). However,

for a quantum OT protocol to have a lower cheating probability for Bob than the best noninteractive classical protocol, we would want p_r to be lower than the bounds in Eqs. (2) and (3).

We can also make further statements about p_f and p_r . From Eqs. (5) and (6), if Bob is selecting between learning either the first or the second bit value, then his failure probability p_f will be nonzero unless the states $\sigma_{00}, \sigma_{01}, \sigma_{10}$, and σ_{11} all have distinct supports, and can therefore be perfectly distinguished from each other. That is, as was already known, $p_f = 0$ necessarily implies that Bob's cheating probability $p_r = 1$, if we also demand that Alice should not be able to cheat any better than with a random guess.

Moreover, that $p_f = 0 \wedge p_s = 1/2$ implies $p_r = 1$ holds true whether or not c is actively chosen by Bob. In so-called semirandom protocols, Bob does not select between two courses of action during the protocol depending on his input c , but instead obtains his value of c randomly as an output from the protocol [12]. Without loss of generality, whether or not Bob actively chooses c , we can assume that Bob obtains both c and the bit value x_c using a measurement that he defers to the end of the protocol. Bob's final measurement then has four outcomes. We denote Bob's generalized measurement operators by π^{i*} for $c = 0$ and π^{*i} for $c = 1$, where $i = 0, 1$ gives the value of x_c . For example, the measurement operator π^{1*} corresponds to $c = 0$ and $x_0 = 1$. Alice can cheat by using entanglement, so that she and Bob in the last step of the protocol share an entangled state. The requirement that Alice is unable to learn anything about c means that the state she holds after Bob's measurement cannot depend on Bob's output c . From no signaling [17], this implies that $\pi^{0*} + \pi^{1*} = q\hat{1}$ and $\pi^{*0} + \pi^{*1} = (1 - q)\hat{1}$, where $0 \leq q \leq 1$. Bob's measurement is therefore equivalent to him making a random choice between learning the first bit with probability q and the second bit with probability $1 - q$. Equations (5) and (6) then again mean that if $p_f = 0 \wedge p_s = 1/2$, then $p_r = 1$ holds, also when Bob does not choose c as an input, but obtains it as an output from the protocol.

When $p_f > 0$, we can reason as follows: Let us assume that the same measurements Bob would use to learn either the first or the second bit are used instead when it is in addition known that Alice is sending either σ_{00} or σ_{11} , with equal probability. In this case, learning either of the bit values determines the state. If $p_{f,0}$ does not depend on whether σ_{00} or σ_{01} was prepared, or whether σ_{10} or σ_{11} was prepared, it follows that

$$p_{f,0} \geq \frac{1}{2}\left(1 - \frac{1}{2}\text{Tr}|\sigma_{00} - \sigma_{11}|\right), \quad (9)$$

where the right-hand side (RHS) is the minimum-error probability for the measurement that optimally distinguishes between the equiprobable states σ_{00} and σ_{11} . Similarly, if $p_{f,1}$ does not depend on whether σ_{00} or σ_{10} was prepared, or whether σ_{01} or σ_{11} was prepared, we have

$$p_{f,1} \geq \frac{1}{2}\left(1 - \frac{1}{2}\text{Tr}|\sigma_{00} - \sigma_{11}|\right). \quad (10)$$

If both of these equations hold, then we obtain

$$p_f \geq \frac{1}{2}\left(1 - \frac{1}{2}\text{Tr}|\sigma_{00} - \sigma_{11}|\right). \quad (11)$$

If $\sigma_{00} = |\psi_{00}\rangle\langle\psi_{00}|$ and $\sigma_{11} = |\psi_{11}\rangle\langle\psi_{11}|$ are pure, then we obtain

$$p_f \geq \frac{1}{2}(1 - \sqrt{1 - |\langle\psi_{00}|\psi_{11}\rangle|^2}). \quad (12)$$

A similar argument can be used to derive

$$p_f \geq \frac{1}{2}(1 - \frac{1}{2}\text{Tr}|\sigma_{01} - \sigma_{10}|). \quad (13)$$

Bob's optimal cheating strategy will be a minimum-error measurement for distinguishing between all four states $\sigma_{00}, \sigma_{10}, \sigma_{01}$, and σ_{11} . In a general interactive protocol with more steps, the success probability of this measurement gives a lower bound for Bob's cheating probability. We will use a bound by Audenaert and Mosonyi [18] for the minimum-error probability for distinguishing between a set of states $\{\rho_i\}$ with prior probabilities p_i ,

$$p_{\text{err}} \leq \frac{1}{2} \sum_{i \neq j} \sqrt{p_i p_j} F(\rho_i, \rho_j), \quad (14)$$

where the fidelity of two quantum states (sometimes called square-root fidelity) is defined as

$$F = \text{Tr}[(\sqrt{\rho_0} \rho_1 \sqrt{\rho_0})]^{1/2}. \quad (15)$$

For two pure states, this reduces to the absolute value of their overlap. We denote the largest of the "nearest-neighbor" fidelities between σ_{00} and σ_{01} , between σ_{00} and σ_{10} , between σ_{11} and σ_{01} , and between σ_{11} and σ_{10} by F , and the larger of the fidelities between σ_{00} and σ_{11} , and between σ_{01} and σ_{10} by G . Bob's cheating probability then obeys

$$p_r \geq 1 - F - \frac{1}{2}G. \quad (16)$$

If $p_f = 0$, then $G = 0$ is necessary, and the equation above reduces to the corresponding bound for complete protocols [12].

Equation (12) (or the corresponding equation for $|\psi_{01}\rangle$ and $|\psi_{10}\rangle$, depending on which fidelity is larger) can be rewritten as

$$\sqrt{p_f(1 - p_f)} \geq \frac{1}{2}G, \quad (17)$$

which holds if σ_{ij} are pure states. It then holds that

$$p_r \geq 1 - F - \sqrt{p_f(1 - p_f)}. \quad (18)$$

From the above equations, it seems that a nonzero failure probability p_f may allow for a lower cheating probability p_r for Bob (lower than if $p_f = 0$). The minimum of the RHS in Eq. (18) is obtained when $p_f = 1/2$, giving $p_r \geq 1/2 - F$, but $p_f = 1/2$ corresponds to a random (and thus useless) result for an honest Bob. The expression is of course only a lower bound on Bob's cheating probability, but the lower bound is lower for nonzero p_f and G .

Alice's cheating probability remains equal to $1/2$ independent of F and G , since an honest Bob is randomly selecting between two measurements to learn either the first or the second bit value. For complete protocols, it generally holds that $p_s \geq (1 + F)/2$ [12], which together with $p_r \geq 1 - F$ means that for complete protocols, Alice's and Bob's cheating probabilities obey the trade-off relation $2p_s + p_r \geq 2$. For the incomplete (imperfect) protocols we are examining, with $p_s = 1/2$, it instead holds that

$$2p_s + p_r \geq 2 - F - \frac{1}{2}G, \quad (19)$$

which shows that in incomplete protocols for quantum oblivious transfer, $2p_s + p_r$ can be lower than complete protocols. For pure states, we can also obtain a trade-off relation in terms of the failure probability p_f as

$$2p_s + p_r \geq 2 - F - \sqrt{p_f(1 - p_f)}. \quad (20)$$

V. PROTOCOLS USING SYMMETRIC PURE STATES

We will now derive the failure and success probabilities for an honest Bob, and Bob's cheating probability, for protocols using symmetric pure states. For N symmetric states $|\psi_j\rangle$, $j = 0, 1, \dots, N - 1$, it holds that $|\psi_j\rangle = U^j |\psi_0\rangle$, where U is a unitary transform that satisfies $U^N = \mathbf{1}$.

Assume that Alice encodes her two bits in the states $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{11}\rangle$, and $|\psi_{10}\rangle$, where $|\psi_{01}\rangle = U|\psi_{00}\rangle$, $|\psi_{11}\rangle = U^2|\psi_{00}\rangle$, and $|\psi_{10}\rangle = U^3|\psi_{00}\rangle$, where $U^4 = \mathbf{1}$. Two of the pairwise overlaps between the states are $\langle\psi_{01}|\psi_{00}\rangle = f$ and $\langle\psi_{11}|\psi_{00}\rangle = g$. The overlap f is in general complex, while due to the symmetry g has to be real, but can be negative. Since the states are symmetric, this also determines $\langle\psi_{10}|\psi_{00}\rangle = f^*$ and all other pairwise overlaps. An honest Bob chooses between a minimum-error measurement to learn the value of the first bit and a minimum-error measurement for learning the value of the second bit. The optimal cheating strategy for a dishonest Bob is to make the minimum-error measurement to distinguish between all four equiprobable states.

We will first calculate Bob's cheating probability p_r in this noninteractive quantum protocol. Also, if Bob should distinguish between the four states $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{11}\rangle$, and $|\psi_{10}\rangle$ in the last step of a protocol with many steps, then the p_r calculated below will be a lower bound on his cheating probability. If the states are equiprobable and symmetric, then the optimal measurement a cheating Bob can make is the so-called square-root measurement. Its success probability can be obtained in terms of the sum of the square roots of the eigenvalues of the Gram matrix $\mathcal{G}$ for the states [19]. The Gram matrix has elements $\mathcal{G}_{ij} = \langle\psi_i|\psi_j\rangle$. For the four states we are considering, it is given by

$$\mathcal{G} = \begin{pmatrix} 1 & f & g & f^* \\ f^* & 1 & f & g \\ g & f^* & 1 & f \\ f & g & f^* & 1 \end{pmatrix}. \quad (21)$$

Its eigenvalues are equal to

$$\begin{aligned} \lambda_0 &= 1 + f + g + f^*, & \lambda_1 &= 1 + if - g - if^*, \\ \lambda_2 &= 1 - f + g - f^*, & \lambda_3 &= 1 - if - g + if^*. \end{aligned} \quad (22)$$

The number of nonzero eigenvalues of the Gram matrix is equal to the dimension D of the space spanned by the states $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{11}\rangle$, and $|\psi_{10}\rangle$. Independent of D , the success probability for the square-root measurement for symmetric states can be obtained as

$$\begin{aligned} p_r &= \frac{1}{16} |\sqrt{\lambda_0} + \sqrt{\lambda_1} + \sqrt{\lambda_2} + \sqrt{\lambda_3}|^2 \\ &= \frac{1}{16} |\sqrt{1 + g + 2\text{Re}f} + \sqrt{1 + g - 2\text{Re}f} \\ &\quad + \sqrt{1 - g + 2\text{Im}f} + \sqrt{1 - g - 2\text{Im}f}|^2. \end{aligned} \quad (23)$$

This is Bob's optimal cheating probability in a noninteractive protocol using symmetric pure states.

To determine the value of the first bit, an honest Bob needs to distinguish between the equiprobable states

$$\frac{1}{2}(\sigma_{00} + \sigma_{01}) \quad \text{and} \quad \frac{1}{2}(\sigma_{10} + \sigma_{11}), \quad (24)$$

where $\sigma_{ij} = |\psi_{ij}\rangle\langle\psi_{ij}|$. To determine the second bit, he needs to distinguish between the equiprobable states

$$\frac{1}{2}(\sigma_{00} + \sigma_{10}) \quad \text{and} \quad \frac{1}{2}(\sigma_{01} + \sigma_{11}). \quad (25)$$

Since all states $|\psi_{ij}\rangle$ are equiprobable and symmetric, his failure probability p_f is the same in each case. For determining the first bit, the failure probability is given by

$$p_{f,0} = \frac{1}{2} \left(1 - \frac{1}{4} \text{Tr}[\sigma_{00} + \sigma_{01} - \sigma_{10} - \sigma_{11}] \right). \quad (26)$$

The analogous expression for the failure probability for determining the second bit, $p_{f,1}$, is obtained by swapping σ_{01} and σ_{10} . The failure probability $p_f = p_{f,0} = p_{f,1}$ for symmetric pure states is calculated in Appendix A and is given by

$$\begin{aligned} p_f &= \frac{1}{2} \left[1 - \frac{1}{4} \sqrt{(\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) + \sqrt{(\lambda_0 + \lambda_2)^2(\lambda_1 + \lambda_3)^2 - 16\lambda_0\lambda_1\lambda_2\lambda_3}} \right. \\ &\quad \left. - \frac{1}{4} \sqrt{(\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) - \sqrt{(\lambda_0 + \lambda_2)^2(\lambda_1 + \lambda_3)^2 - 16\lambda_0\lambda_1\lambda_2\lambda_3}} \right] \\ &= \frac{1}{2} \left[1 - \frac{1}{2} \sqrt{1 - g^2 + 2\sqrt{(1+g)^2(\text{Im}f)^2 + (1-g)^2(\text{Re}f)^2 - 4(\text{Re}f)^2(\text{Im}f)^2}} \right. \\ &\quad \left. - \frac{1}{2} \sqrt{1 - g^2 - 2\sqrt{(1+g)^2(\text{Im}f)^2 + (1-g)^2(\text{Re}f)^2 - 4(\text{Re}f)^2(\text{Im}f)^2}} \right] \\ &= \frac{1}{2} \left[1 - \frac{1}{2} \sqrt{1 - g^2 + 2\sqrt{|f|^2(1+g^2) + 2g[(\text{Im}f)^2 - (\text{Re}f)^2] - 4(\text{Re}f)^2(\text{Im}f)^2}} \right. \\ &\quad \left. - \frac{1}{2} \sqrt{1 - g^2 - 2\sqrt{|f|^2(1+g^2) + 2g[(\text{Im}f)^2 - (\text{Re}f)^2] - 4(\text{Re}f)^2(\text{Im}f)^2}} \right]. \end{aligned} \quad (27)$$

This is the probability that an honest Bob obtains an incorrect bit value.

Using the expressions in Eqs. (23) and (27), one can investigate how low p_r can be for a given p_f , whether quantum protocols using symmetric pure states can be better than classical protocols, and what the corresponding sets of pure symmetric states are. In Appendix B, we show that in the range $(1 - 1/\sqrt{2})/2 \leq p_f \leq 1/2$, the lowest possible cheating probability p_r for protocols using symmetric pure states is given by

$$\begin{aligned} p_r &= \frac{1}{4}(1 + \sqrt{2}) - \frac{1}{\sqrt{2}}p_f \\ &= \frac{1}{4}(1 - \sqrt{2}) + \frac{1}{\sqrt{2}}(1 - p_f), \end{aligned} \quad (28)$$

which we also wrote in terms of the protocol success probability $1 - p_f$. Bob's cheating probability is then in the range $1/4 \leq p_r \leq 1/2$. Moreover, we learn from the analysis in Appendix B that the corresponding optimal states $|\psi_{ij}\rangle$ span a two-dimensional space, since two of the eigenvalues of their Gram matrix are equal to zero. If all four states are equal, then $p_r = 1/4$ and $p_f = 1/2$. The value $p_f = (1 - 1/\sqrt{2})/2 \approx 0.15$ corresponds to $p_r = 1/2$ (which Bob could also achieve with a random guess).

Let us check when Bob's cheating probability for this class of optimal quantum protocols is lower than that in the corresponding classical protocols. For a quantum protocol to be better than classical protocols, it should hold that $p_r < 1 - 2p_f$. Combined with Eq. (28), this gives $p_f < (3 - \sqrt{2})/(8 - 2\sqrt{2}) \approx 0.31$, corresponding to $1 - p_f > 0.69$. In this range, Bob's cheating probability is therefore lower in the quantum protocols. When $p_f \gtrsim 0.31$, protocols using symmetric pure states are not optimal, which is also interesting. Mixedness and/or asymmetry must then be useful and might

of course be useful also for other values of p_f . In the classical protocols, Alice uses the equivalent of mixed states.

When $0 \leq p_f \leq (1 - 1/\sqrt{2})/2 \approx 0.15$, which corresponds to $1/2 \leq p_r \leq 1$, the lowest possible p_f is given by

$$p_f = \frac{1}{2} \left[1 - \sqrt{p_r^2 + (1 - p_r)^2} \right]. \quad (29)$$

The optimization in Appendix B also tells us that the states $|\psi_{ij}\rangle$ now span a four-dimensional space. Geometrically, if p_r and $1 - p_r$ are the lengths of two sides of a right-angled triangle, then the length of the hypotenuse is given by $1 - 2p_f$. Hence, p_r is always less than $1 - 2p_f$, meaning that for these optimal quantum protocols using symmetric pure states, Bob always has a lower cheating probability than in classical protocols with the same failure probability p_f . To summarize, protocols using symmetric pure quantum states are better than corresponding classical protocols when $0 < p_f \lesssim 0.31$. When $0.31 \lesssim p_f < 1/2$, classical protocols are better, meaning that mixedness and/or asymmetry must be useful in more general quantum protocols (which must be at least as good as classical protocols). The optimal p_r for symmetric pure states is plotted in Fig. 1 as a function of the protocol success probability $1 - p_f$.

VI. OPTIMAL PROTOCOLS USING SYMMETRIC PURE STATES

In this section, we will describe sets of four symmetric pure states that are optimal in the sense that for a given failure probability p_f , Bob's cheating probability p_r is as low as possible. Alternatively, for a given p_r , Bob's p_f is as low as possible. We also describe a set of qutrit states that is suboptimal, but is related to the states used in the semirandom oblivious transfer protocol in Ref. [12].

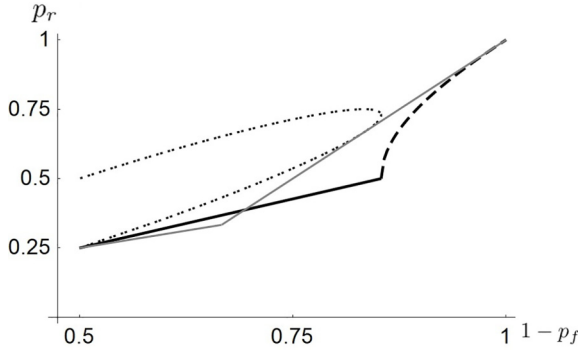


FIG. 1. The lowest possible cheating probability p_r for the receiver Bob, as a function of the protocol success probability $1 - p_f$, in noninteractive protocols for oblivious transfer. The sender Alice can only cheat with probability $p_s = 1/2$ (a random guess). The gray line shows the lowest possible p_r in classical protocols. The solid black line and dashed black line show the lowest possible p_r for quantum protocols using symmetric pure states, in the ranges $1/4 \leq p_r \leq 1/2$ and $1/2 \leq p_r \leq 1$, respectively. For the solid black line, the states $|\psi_{ij}\rangle$ span a two-dimensional space, and for the dashed line, a four-dimensional space. The dotted line shows the cheating probability achieved by the family of states in Sec. VIC, spanning a three-dimensional space.

A. BB84 or “Wiesner” states

Suppose that Alice encodes her two bits x_0 and x_1 in the states

$$|\psi_{00}\rangle = |0\rangle, \quad |\psi_{01}\rangle = \sqrt{i}|+\rangle, \quad (30)$$

$$|\psi_{11}\rangle = i|1\rangle, \quad |\psi_{10}\rangle = i\sqrt{i}|-\rangle, \quad (31)$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Apart from the overall phase factors that have been included to make the states symmetric according to the definition at the start of Sec. V, this set of states is identical to the one used for “conjugate coding” by Wiesner [1], in the Bennett-Brassard protocol for quantum cryptography (BB84) [20] and for quantum random access codes [15]. Here, we only reinterpret the situation as imperfect 1-out-of-2 oblivious transfer. Depending on which bit value an honest Bob wishes to obtain, he measures in a basis rotated by $\pi/8$ from the basis $\{|0\rangle, |1\rangle\}$ to obtain the first bit or rotated by $3\pi/8$ to obtain the second bit. Either of these measurements succeed with probability $\cos^2(\pi/8) \approx 0.85$. Consequently, the protocol’s inherent failure probability p_f^W is given by

$$p_f^W = 1 - \cos^2\left(\frac{\pi}{8}\right) \approx 0.15. \quad (32)$$

As before, no signaling prohibits Alice from cheating so that $p_s = 1/2$. The success probability of Bob’s minimum-error measurement for distinguishing between all four states is

$$p_r^W = \frac{1}{2}, \quad (33)$$

which is his cheating probability. It holds that $p_r^W < 1 - 2p_f^W \approx 0.7$. This protocol therefore is better than classical protocols. In fact, as is confirmed by the results in the previous section and in Appendix B, it is optimal in the sense that for

this value of p_f , no choice of four symmetric pure states can give a lower p_r .

B. Qubit states

To obtain protocols with p_f in the range $p_f^W \leq p_f \leq 1/2$, we will look at symmetric qubit states given by

$$\begin{aligned} |\psi_{00}\rangle &= a|0\rangle + b|1\rangle, & |\psi_{01}\rangle &= a|0\rangle + ib|1\rangle, \\ |\psi_{11}\rangle &= a|0\rangle - b|1\rangle, & |\psi_{10}\rangle &= a|0\rangle - ib|1\rangle, \end{aligned} \quad (34)$$

where $0 \leq |a|$ and $|b| \leq 1$, with $|a|^2 + |b|^2 = 1$. This set of states is symmetric with the symmetry operation $U = |0\rangle\langle 0| + i|1\rangle\langle 1|$. 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 p_r and higher p_f than for the “Wiesner” states. 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 holds that $f = |a|^2 + i|b|^2$ and $g = |a|^2 - |b|^2$. From Eqs. (23) and (27), we obtain

$$\begin{aligned} p_f &= \frac{1}{2}(1 - \sqrt{2}|ab|), \\ p_r &= \frac{1}{4}(|a| + |b|)^2 = \frac{1}{4}(1 + 2|ab|), \end{aligned} \quad (35)$$

and it therefore also holds that

$$p_r = \frac{1}{\sqrt{2}}(1 - p_f) + \frac{1}{4}(1 - \sqrt{2}); \quad (36)$$

that is, Bob’s cheating probability p_r is a straight line as a function of the protocol success probability $1 - p_f$. As shown in Appendix B and given in Eq. (28), this is the lowest possible p_r for a given p_f with p_f in the range $p_f^W \leq p_f \leq 1/2$. It follows that the qubit states in Eq. (34) are indeed optimal. Moreover, it holds that

$$1 - 2p_f = \sqrt{2}|ab| < p_r \quad (37)$$

when $|ab| > 1/(4\sqrt{2} - 2) \approx 0.273$, which corresponds to $p_f \lesssim 0.31$. As mentioned above, this is the range where this class of protocols outperform classical protocols.

C. Ququart states

We will now look at a set of states that makes it possible to reach $p_f = 0$ (when it must hold that $p_r = 1$). For this limit, it is necessary that all four states become orthogonal, and we also know from the optimization in Appendix B that the corresponding sets of states need to span a four-dimensional space. We will choose

$$\begin{aligned} |\psi_{00}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & |\psi_{01}\rangle &= \frac{a}{\sqrt{2}}(|0\rangle + i|1\rangle) + b|2\rangle, \\ |\psi_{11}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & |\psi_{10}\rangle &= \frac{a}{\sqrt{2}}(|0\rangle - i|1\rangle) + b|3\rangle, \end{aligned} \quad (38)$$

where $0 \leq |a|, |b| \leq 1$, and $|a|^2 + |b|^2 = 1$. For $a = 1$, we obtain the eigenstates of σ_x and σ_y , connecting with the qubit

states considered above. The pairwise overlaps are now

$$\begin{aligned}\langle\psi_{00}|\psi_{01}\rangle &= \langle\psi_{11}|\psi_{10}\rangle = \frac{a}{2}(1+i), \\ \langle\psi_{01}|\psi_{11}\rangle &= \langle\psi_{10}|\psi_{00}\rangle = \frac{a^*}{2}(1+i), \\ \langle\psi_{00}|\psi_{11}\rangle &= \langle\psi_{01}|\psi_{10}\rangle = 0.\end{aligned}\quad (39)$$

That is, the set of states is symmetric without further modifications if a is real. In this case, we obtain $f = (a/2)(1+i)$ and $g = 0$, and

$$\begin{aligned}p_f &= \frac{1}{4}(2 - \sqrt{1+a\sqrt{2-a^2}} - \sqrt{1-a\sqrt{2-a^2}}), \\ p_r &= \frac{1}{4}(\sqrt{1+a} + \sqrt{1-a})^2 = \frac{1}{2}(1 + \sqrt{1-a^2}).\end{aligned}\quad (40)$$

The above relations imply that

$$(1 - 2p_f)^2 = p_r^2 + (1 - p_r)^2 = 1 - \frac{a^2}{2}. \quad (41)$$

This agrees with Eq. (29), and the above choice of ququart states is therefore optimal for $0 \leq p_f \leq p_f^W$. For this set of states, it holds that $1 - 2p_f \geq p_r$ for the whole range $0 \leq a \leq 1$, with equality for $a = 0$, when $p_f = 0$ and $p_r = 1$. The resulting quantum protocol therefore outperforms classical protocols for the whole range $0 < p_f \leq p_f^W$.

D. Qutrit states

As an example of symmetric pure states that turn out to not be optimal for the type of protocols we are considering, we will look at the set of states

$$\begin{aligned}|\psi_{00}\rangle &= a|0\rangle + b|1\rangle, & |\psi_{01}\rangle &= a|0\rangle + b|2\rangle, \\ |\psi_{11}\rangle &= a|0\rangle - b|1\rangle, & |\psi_{10}\rangle &= a|0\rangle - b|2\rangle,\end{aligned}\quad (42)$$

where $0 \leq |a|, |b| \leq 1$, and $|a|^2 + |b|^2 = 1$. One reason to investigate this set of states is that for $a = b = 1/\sqrt{2}$, it is equivalent to two copies of the same ‘‘Wiesner’’ states, that is, the states $|00\rangle, |++\rangle, |11\rangle$, and $|--\rangle$, since all pairwise overlaps match. These states are used in an oblivious transfer protocol in Ref. [12], which has the lowest known cheating probabilities for a complete 1-out-of-2 quantum oblivious transfer protocol where the parties are not restricted. It is therefore interesting to see how well the same set of states performs for an incomplete oblivious transfer protocol.

If Bob is given two copies of a ‘‘Wiesner’’ or BB84 state, we might expect that an honest Bob will obtain a correct bit value more often than if he is given a single copy, but also that it becomes easier for a dishonest Bob to cheat. However, one can easily verify that this is not the case. While an additional copy helps a dishonest Bob cheat, as we will see, it does not lower an honest Bob’s failure probability. An honest Bob can ignore the second copy. On the other hand, with two copies of a ‘‘Wiesner’’ or BB84 state, the semirandom oblivious transfer protocol with $p_f = 0$ in Ref. [12] is possible. In a semirandom protocol, Bob does not choose whether he obtains the first or the second bit value, but obtains a bit value at random. Bob’s overall measurement is then no longer from Alice’s point of view equivalent to Bob choosing between two measurements. Instead, Bob makes one fixed measurement with four outcomes. Therefore, while $p_f = 0$ becomes possible,

Bob’s and also Alice’s cheating probabilities increase, becoming equal to ≈ 0.729 and $3/4$, respectively, if the states $|00\rangle, |++\rangle, |11\rangle$, and $|--\rangle$ are used.

Returning to nonrandom protocols where Bob chooses between learning the first or the second bit, an honest Bob does not benefit from using the qutrit states in Eq. (42), as compared with the qubit states in Eq. (34). This may seem counterintuitive, but is analogous to a scenario where Bob is sent a classical bit value that might have been flipped with some probability p . His probability to read out the bit value correctly does not increase if he is sent a second copy of the same bit value, which might have also been flipped independently with probability p . Both bits are then incorrect (and the two incorrect values agree) with probability p^2 . If one bit value is correct and the other one not, then Bob will have to guess what the correct value is. His overall probability to arrive at the incorrect bit value is then $p^2 + 2p(1-p)/2 = p$, the same as if he had been sent only one bit.

For the states in Eq. (42), we obtain $f = \langle\psi_{00}|\psi_{01}\rangle = |a|^2$ and $g = \langle\psi_{00}|\psi_{11}\rangle = |a|^2 - |b|^2$. This gives

$$\begin{aligned}p_f &= \frac{1}{2}(1 - \sqrt{2}|ab|), \\ p_r &= \frac{1}{4}(|a| + \sqrt{2}|b|)^2 = \frac{1}{4}(1 + |b|^2 + 2\sqrt{2}|ab|).\end{aligned}\quad (43)$$

That is, as a function of $|a|$ and $|b|$, we obtain the same p_f as for the qubit states in Eq. (34), but a higher p_r . This set of qutrit states therefore never outperforms the qubit states. Bob’s cheating probability for this set of qutrit states is plotted in Fig. 1, along with the lowest possible cheating probabilities for the optimal qubit and ququart states, and the lowest possible cheating probability for classical protocols.

VII. CONCLUSION AND OUTLOOK

We have demonstrated that for oblivious transfer protocols that sometimes fail, quantum protocols may outperform classical ones, in the sense that for protocols where the sender can only cheat with probability $1/2$, Bob’s cheating probability in quantum protocols can be lower than in any classical non-interactive protocol with the same failure probability p_f . We fully characterized noninteractive quantum protocols that use symmetric pure states and gave examples of optimal protocols, which use qubits and ququarts, respectively. When $p_f \lesssim 0.31$, Bob’s cheating probability in these protocols is lower than in classical protocols.

Incomplete 1-out-of-2 oblivious transfer of the type we are considering, where the sender can only cheat with probability $p_s = 1/2$, can be seen as a generalization of complete oblivious transfer, but also as a generalization of RACs [1,15]. 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 the values of two bits. 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 QRAC [1,15], the sender is restricted to using one qubit for encoding two classical bit values. Probabilistic one-time programs [21,22] are a related functionality, which reduces to a QRAC in the case relevant here.

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. However, 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 the type of oblivious transfer protocols we have been considering, however, 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, the type of incomplete oblivious transfer we have considered, with $p_s = 1/2$, is a generalization of a QRAC (as well as being a generalization of complete or “perfect” oblivious transfer). That is, for the type oblivious transfer we have considered, we are concerned with (1) maximizing the probability that the receiver correctly obtains their chosen bit value, as in a RAC, but also (2) minimizing the probability that they correctly obtain both bit values, which generalizes the restriction of sending a single bit or qubit. A remaining difference is that in complete protocols for oblivious transfer, the receiver should always correctly retrieve their chosen bit value, whereas in a RAC or QRAC, or in an

incomplete protocol for oblivious transfer, the probability for the bit value to be correct is generally lower than 1. Our protocols interpolate between or “connect” random access codes and oblivious transfer, generalizing both functionalities.

To summarize, we have obtained bounds on cheating probabilities for incomplete (imperfect) quantum oblivious transfer and derived optimal protocols that use pure symmetric states. Cheating probabilities can be lower for incomplete protocols than for complete protocols. The optimal symmetric-state protocols use qubit or ququart (two-qubit) states and could be implemented with existing experimental techniques; ququart states can, for example, be realized as single-photon states, using four different spatial modes or polarization and two spatial modes. The honest receiver’s measurements are easy-to-realize projective measurements, since the task is to distinguish between only two mixed states. As is well known and also discussed above, the optimal measurement is in this case simply a projective measurement in a particular basis. The type of incomplete oblivious transfer we have considered can be seen as generalizing both complete oblivious transfer and random access codes, and connecting these two functionalities.

ACKNOWLEDGMENT

I.V.P and E.A. acknowledge support by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant No. EP/T001011/1.

APPENDIX A: PROTOCOL FAILURE PROBABILITY FOR SYMMETRIC PURE STATES

To calculate the protocol failure probability, we construct the states

$$\begin{aligned} 2\sqrt{\lambda_0}|A_0\rangle &= |\psi_{00}\rangle + |\psi_{01}\rangle + |\psi_{11}\rangle + |\psi_{10}\rangle, \\ 2\sqrt{\lambda_1}|A_1\rangle &= |\psi_{00}\rangle + i|\psi_{01}\rangle - |\psi_{11}\rangle - i|\psi_{10}\rangle, \\ 2\sqrt{\lambda_2}|A_2\rangle &= |\psi_{00}\rangle - |\psi_{01}\rangle + |\psi_{11}\rangle - |\psi_{10}\rangle, \\ 2\sqrt{\lambda_3}|A_3\rangle &= |\psi_{00}\rangle - i|\psi_{01}\rangle - |\psi_{11}\rangle + i|\psi_{10}\rangle, \end{aligned} \quad (A1)$$

where λ_i are the previously given eigenvalues of the Gram matrix for the states $|\psi_{ij}\rangle$. If the space spanned by $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{11}\rangle$, and $|\psi_{10}\rangle$ is four dimensional, then the states $|A_0\rangle, |A_1\rangle, |A_2\rangle, |A_3\rangle$ are orthonormal. If the space is less than four dimensional, then some of the eigenvalues λ_i are equal to zero, but the four states $|A_i\rangle$ can still be chosen orthonormal and used as a basis. Independent of dimension, we have

$$\begin{aligned} |\psi_{00}\rangle &= \frac{1}{2}(\sqrt{\lambda_0}|A_0\rangle + \sqrt{\lambda_1}|A_1\rangle + \sqrt{\lambda_2}|A_2\rangle + \sqrt{\lambda_3}|A_3\rangle), \\ |\psi_{01}\rangle &= \frac{1}{2}(\sqrt{\lambda_0}|A_0\rangle - i\sqrt{\lambda_1}|A_1\rangle - \sqrt{\lambda_2}|A_2\rangle + i\sqrt{\lambda_3}|A_3\rangle), \\ |\psi_{11}\rangle &= \frac{1}{2}(\sqrt{\lambda_0}|A_0\rangle - \sqrt{\lambda_1}|A_1\rangle + \sqrt{\lambda_2}|A_2\rangle - \sqrt{\lambda_3}|A_3\rangle), \\ |\psi_{10}\rangle &= \frac{1}{2}(\sqrt{\lambda_0}|A_0\rangle + i\sqrt{\lambda_1}|A_1\rangle - \sqrt{\lambda_2}|A_2\rangle - i\sqrt{\lambda_3}|A_3\rangle). \end{aligned} \quad (A2)$$

Using the basis $\{|A_0\rangle, |A_1\rangle, |A_2\rangle, |A_3\rangle\}$, we therefore have

$$\frac{1}{2}(\sigma_{00} + \sigma_{01}) = \frac{1}{8} \begin{pmatrix} 2\lambda_0 & \sqrt{\lambda_{01}}(1+i) & 0 & \sqrt{\lambda_{03}}(1-i) \\ \sqrt{\lambda_{01}}(1-i) & 2\lambda_1 & \sqrt{\lambda_{12}}(1+i) & 0 \\ 0 & \sqrt{\lambda_{12}}(1-i) & 2\lambda_2 & \sqrt{\lambda_{23}}(1+i) \\ \sqrt{\lambda_{03}}(1+i) & 0 & \sqrt{\lambda_{23}}(1-i) & 2\lambda_3 \end{pmatrix}, \quad (A3)$$

$$\frac{1}{2}(\sigma_{10} + \sigma_{11}) = \frac{1}{8} \begin{pmatrix} 2\lambda_0 & \sqrt{\lambda_{01}}(-1-i) & 0 & \sqrt{\lambda_{03}}(-1+i) \\ \sqrt{\lambda_{01}}(-1+i) & 2\lambda_1 & \sqrt{\lambda_{12}}(-1-i) & 0 \\ 0 & \sqrt{\lambda_{12}}(-1+i) & 2\lambda_2 & \sqrt{\lambda_{23}}(-1-i) \\ \sqrt{\lambda_{03}}(-1-i) & 0 & \sqrt{\lambda_{23}}(-1+i) & 2\lambda_3 \end{pmatrix}, \quad (\text{A4})$$

$$\frac{1}{4}(\sigma_{00} + \sigma_{01} - \sigma_{10} - \sigma_{11}) = \frac{1}{8} \begin{pmatrix} 0 & \sqrt{\lambda_{01}}(1+i) & 0 & \sqrt{\lambda_{03}}(1-i) \\ \sqrt{\lambda_{01}}(1-i) & 0 & \sqrt{\lambda_{12}}(1+i) & 0 \\ 0 & \sqrt{\lambda_{12}}(1-i) & 0 & \sqrt{\lambda_{23}}(1+i) \\ \sqrt{\lambda_{03}}(1+i) & 0 & \sqrt{\lambda_{23}}(1-i) & 0 \end{pmatrix}, \quad (\text{A5})$$

where we have used the shorthand $\lambda_{ij} = \lambda_i \lambda_j$. The eigenvalue equation for the last matrix above is given by $|\frac{1}{4}(\sigma_{00} + \sigma_{01} - \sigma_{10} - \sigma_{11}) - \Lambda \mathbf{1}| = 0$, which, when evaluating the determinant, gives

$$(8\Lambda)^4 - 2(8\Lambda)^2(\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) + 16\lambda_{0123} = 0, \quad (\text{A6})$$

where $\lambda_{0123} = \lambda_0 \lambda_2 \lambda_1 \lambda_3$. The four eigenvalues of the matrix in Eq. (A5) are consequently given by the solutions to

$$\begin{aligned} \Lambda^2 &= \frac{1}{8^2} [(\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) \pm \sqrt{(\lambda_0 + \lambda_2)^2(\lambda_1 + \lambda_3)^2 - 16\lambda_0\lambda_1\lambda_2\lambda_3}] \\ &= \frac{1}{8^2} [4(1 - g^2) \pm 8\sqrt{(1 + g)^2(\text{Im}f)^2 + (1 - g)^2(\text{Re}f)^2 - 4(\text{Re}f)^2(\text{Im}f)^2}]. \end{aligned}$$

The failure probability for the protocol is therefore given by

$$\begin{aligned} p_f &= \frac{1}{2} \left[1 - \frac{1}{4} \sqrt{(\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) + \sqrt{(\lambda_0 + \lambda_2)^2(\lambda_1 + \lambda_3)^2 - 16\lambda_0\lambda_1\lambda_2\lambda_3}} \right. \\ &\quad \left. - \frac{1}{4} \sqrt{(\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) - \sqrt{(\lambda_0 + \lambda_2)^2(\lambda_1 + \lambda_3)^2 - 16\lambda_0\lambda_1\lambda_2\lambda_3}} \right] \\ &= \frac{1}{2} \left[1 - \frac{1}{2} \sqrt{1 - g^2 + 2\sqrt{|f|^2(1 + g^2) + 2G[(\text{Im}f)^2 - (\text{Re}f)^2] - 4(\text{Re}f)^2(\text{Im}f)^2}} \right. \\ &\quad \left. - \frac{1}{2} \sqrt{1 - g^2 - 2\sqrt{|f|^2(1 + g^2) + 2G[(\text{Im}f)^2 - (\text{Re}f)^2] - 4(\text{Re}f)^2(\text{Im}f)^2}} \right]. \end{aligned} \quad (\text{A7})$$

This is the probability that an honest Bob obtains an incorrect bit value.

APPENDIX B: OPTIMAL PURE-STATE PROTOCOLS

For an optimal protocol, it holds that for a given failure probability p_f , Bob's cheating probability p_r is as low as possible, and vice versa. The failure probability p_f and the cheating probability p_r are given in Eqs. (27) [which is the same as Eq. (A7)] and (23), respectively. We will minimize p_f for a given (fixed) $p_r = |\sum_i \sqrt{\lambda_i}|^2/16$. We first rewrite Eq. (A7) in the more convenient form

$$8(1 - 2p_f)^2 = (\lambda_0 + \lambda_2)(\lambda_1 + \lambda_3) + 4\sqrt{\lambda_{0123}}. \quad (\text{B1})$$

In the range $0 \leq p_f \leq 1/2$, minimizing p_f is equivalent to maximizing $(1 - 2p_f)^2$. It holds that

$$\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 4, \quad (\text{B2})$$

where we note that λ_i are all real and $\lambda_i \geq 0$. We define

$$\begin{aligned} a &= (\sqrt{\lambda_0} + \sqrt{\lambda_1} + \sqrt{\lambda_2} + \sqrt{\lambda_3})/4, \\ b &= (\sqrt{\lambda_0} - \sqrt{\lambda_1} + \sqrt{\lambda_2} - \sqrt{\lambda_3})/4, \\ c &= (\sqrt{\lambda_0} + \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3})/4, \\ d &= (\sqrt{\lambda_0} - \sqrt{\lambda_1} - \sqrt{\lambda_2} + \sqrt{\lambda_3})/4, \end{aligned} \quad (\text{B3})$$

which means that $a^2 = p_r$ is a constant. We also obtain

$$a^2 + b^2 + c^2 + d^2 = \frac{1}{4}(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3) = 1, \quad (\text{B4})$$

which together means that

$$b^2 + c^2 + d^2 = 1 - p_r \quad (\text{B5})$$

is also a constant. Equation (B1) becomes

$$(1 - 2p_f)^2 = (a^2 - b^2)^2 + (c^2 - d^2)^2, \quad (\text{B6})$$

which should be maximized. Recall that $a^2 = p_r$ and $b^2 + c^2 + d^2 = 1 - p_r$ are constant. Clearly, $(1 - 2p_f)^2$ will be maximized if we can choose $b = 0$, and either $c = 0$ and $d^2 = 1 - p_r$, or $c^2 = 1 - p_r$ and $d = 0$. If this is possible, then we obtain

$$(1 - 2p_f)^2 = p_r^2 + (1 - p_r)^2. \quad (\text{B7})$$

It is, however, not always possible to choose $b = 0$, and either $c = 0$ or $d = 0$. For example, if $b = d = 0$, then $a = \sqrt{p_r}$ and $c = \sqrt{1 - p_r}$, and we obtain

$$\begin{aligned} \sqrt{\lambda_0} &= a + b + c + d = \sqrt{p_r} + \sqrt{1 - p_r}, \\ \sqrt{\lambda_1} &= a - b + c - d = \sqrt{p_r} + \sqrt{1 - p_r}, \\ \sqrt{\lambda_2} &= a + b - c - d = \sqrt{p_r} - \sqrt{1 - p_r}, \\ \sqrt{\lambda_3} &= a - b - c + d = \sqrt{p_r} - \sqrt{1 - p_r}. \end{aligned} \quad (\text{B8})$$

Since $\lambda_i \geq 0$, it must hold that $1/2 \leq p_r \leq 1$ for this to be possible. This corresponds to $0 \leq p_f \leq (1 - 1/\sqrt{2})/2 \approx$

0.15, where it then holds that

$$p_f = \frac{1}{2} [1 - \sqrt{p_r^2 + (1 - p_r)^2}]. \quad (\text{B9})$$

When $1/2 < p_r$, the space spanned by the corresponding optimal states $|\psi_{ij}\rangle$ is four dimensional, and becomes two dimensional for $p_r = 1/2$ (equivalent to the “Wiesner” states).

When $1/4 \leq p_r < 1/2$, we must instead choose $a^2 = c^2 = p_r$ and $b^2 = d^2 = 1/2 - p_r$ to maximize $(1 - 2p_f)^2$ (equivalently, to minimize p_f). Alternatively, we can choose $a^2 = d^2$ and $b^2 = c^2$. It will hold either

that $\lambda_1 = \lambda_2 = 0$ or that $\lambda_2 = \lambda_3 = 0$, meaning that the corresponding optimal sets of states $|\psi_{ij}\rangle$ span a two-dimensional space. It then holds that

$$p_r = \frac{1}{4}(1 + \sqrt{2}) - \frac{1}{\sqrt{2}}p_f, \quad (\text{B10})$$

which is the lowest possible cheating probability p_r in the range $(1 - 1/\sqrt{2})/2 \leq p_f \leq 1/2$, corresponding to $1/4 \leq p_r \leq 1/2$, for protocols using symmetric pure states. The results in this Appendix have also been verified numerically.

-
- [1] S. Wiesner, Conjugate coding, *ACM Sigact News* **15**, 78 (1983).
 - [2] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, *Commun. ACM* **28**, 637 (1985).
 - [3] M. O. Rabin, How to exchange secrets with oblivious transfer, Cryptology ePrint Archive: Report 2005/187 (2005), <https://eprint.iacr.org/2005/187>.
 - [4] J. Kilian, Founding cryptography on oblivious transfer, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, 1988), pp. 20–31.
 - [5] D. Mayers, Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78**, 3414 (1997).
 - [6] H.-K. Lo, Insecurity of quantum secure computations, *Phys. Rev. A* **56**, 1154 (1997).
 - [7] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded-quantum-storage model, *SIAM J. Comput.* **37**, 1865 (2008).
 - [8] D. Pitalúa-García, Spacetime-constrained oblivious transfer, *Phys. Rev. A* **93**, 062346 (2016).
 - [9] J. Sikora, On the existence of loss-tolerant quantum oblivious transfer protocols, *Quantum Info. & Comput.* **12**, 136 (2012).
 - [10] A. Chailloux, I. Kerenidis, and J. Sikora, Lower bounds for quantum oblivious transfer, *Quantum Info. & Comput.* **13**, 180 (2013).
 - [11] A. Chailloux, G. Gutoski, and J. Sikora, Optimal bounds for semi-honest quantum oblivious transfer, *Chicago J. Theor. Comp. Sci.* **1** (2016).
 - [12] R. Amiri, R. Stárek, D. Reichmuth, I. V. Puthoor, M. Mičuda, L. Mišta, Jr., M. Dušek, P. Wallden, and E. Andersson, Imperfect 1-out-of-2 quantum oblivious transfer: Bounds, a protocol, and its experimental implementation, *PRX Quantum* **2**, 010335 (2021).
 - [13] L. Stroh, N. Horová, R. Stárek, I. V. Puthoor, M. Mičuda, M. Dušek, and E. Andersson, Noninteractive XOR quantum oblivious transfer: optimal protocols and their experimental implementations, *PRX Quantum* **4**, 020320 (2023).
 - [14] L. Stroh, J. T. Peat, M. Kroneberg, I. V. Puthoor, and E. Andersson, Quantum Rabin oblivious transfer using two pure states, *Phys. Rev. Res.* **6**, 043004 (2024).
 - [15] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and quantum finite automata, *J. ACM* **49**, 496 (2002).
 - [16] A. Huang, S. Barz, E. Andersson, and V. Makarov, Implementation vulnerabilities in general quantum cryptography, *New J. Phys.* **20**, 103016 (2018).
 - [17] G. C. Ghirardi, A. Rimini, and T. Weber, A general argument against superluminal transmission through the quantum mechanical measurement process, *Lett. Nuovo Cimento* **27**, 293 (1980).
 - [18] 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).
 - [19] P. Wallden, V. Dunjko, and E. Andersson, Minimum-cost measurements for quantum information, *J. Phys. A: Math. Theor.* **47**, 125303 (2014).
 - [20] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
 - [21] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, One-time programs, in *Advances in Cryptology CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA* (2008), pp. 39–56.
 - [22] 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).