On the Efficiency of Classical and Quantum Oblivious Transfer Reductions

Severin Winkler and Jürg Wullschleger

[1] ETH Zurich, Switzerland
swinkler@ethz.ch
[2] University of Bristol, United Kingdom
j.wullschleger@bristol.ac.uk

Abstract. Due to its universality oblivious transfer (OT) is a primitive of great importance in secure multi-party computation. OT is impossible to implement from scratch in an unconditionally secure way, but there are many reductions of OT to other variants of OT, as well as other primitives such as noisy channels. It is important to know how efficient such unconditionally secure reductions can be in principle, i.e., how many instances of a given primitive are at least needed to implement OT. For perfect (error-free) implementations good lower bounds are known, e.g. the bounds by Beaver (STOC '96) or by Dodis and Micali (EUROCRYPT '99). However, in practice one is usually willing to tolerate a small probability of error and it is known that these *statistical* reductions can in general be much more efficient. Thus, the known bounds have only limited application. In the first part of this work we provide bounds on the efficiency of secure (one-sided) two-party computation of arbitrary finite functions from distributed randomness in the statistical case. From these results we derive bounds on the efficiency of protocols that use (different variants of) OT as a black-box. When applied to implementations of OT, our bounds generalize known results to the statistical case. Our results hold in particular for transformations between a finite number of primitives and for *any* error. Furthermore, we provide bounds on the efficiency of protocols implementing Rabin OT.

In the second part we study the efficiency of quantum protocols implementing OT. Recently, Salvail, Schaffner and Sotakova (ASIACRYPT '09) showed that most classical lower bounds for *perfectly* secure reductions of OT to distributed randomness still hold in a quantum setting. We present a statistically secure protocol that violates these bounds by an arbitrarily large factor. We then present a weaker lower bound that *does* hold in the statistical quantum setting. We use this bound to show that even quantum protocols cannot extend OT. Finally, we present two lower bounds for reductions of OT to commitments and a protocol based on string commitments that is optimal with respect to both of these bounds.

Keywords. Unconditional Security, Oblivious Transfer, Lower Bounds, Quantum Cryptography, Two-Party Computation.

1 Introduction

Secure multi-party computation allows two or more distrustful players to jointly compute a function of their inputs in a secure way [48]. Security here means that the players compute the value of the function correctly without learning more than what they can derive from their own input and output.

A primitive of central importance in secure multi-party computation is *oblivious transfer* (OT), as it is sufficient to execute any multi-party computation securely [25, 27]. The original form of OT ($(\frac{1}{2})$-$\mathsf{RabinOT}^1$) has been introduced by Rabin in [35]. It allows a sender to send a bit x, which the receiver will get with probability $\frac{1}{2}$. Another variant of OT, called one-out-of-two bit-OT ($\binom{2}{1}$-OT^1) was defined in [23] (see also [39]). Here, the sender has two input bits x_0 and x_1. The receiver gives as input a choice bit c and receives x_c without learning x_{1-c}. The sender gets no information about the choice bit c. Other important variants of OT are $\binom{n}{t}$-OT^k where the inputs are strings of k bits and the receiver can choose $t < n$ out of n secrets and (p)-$\mathsf{RabinOT}^k$ where the inputs are strings of k bits and the erasure probability is $p \in [0, 1]$.

If the players have access to noiseless (classical or quantum) communication only, it is impossible to implement unconditionally secure OT, i.e. secure against an adversary with unlimited computing power. It has been shown in [13] that (p)-$\mathsf{RabinOT}^k$ and $\binom{2}{1}$-OT^1 are equally powerful, i.e., one can be implemented from the other. Numerous reductions between different variants of $\binom{n}{1}$-OT^k are known as well: $\binom{2}{1}$-OT^k can be implemented from $\binom{2}{1}$-OT^1 [5, 15, 9, 8], and $\binom{n}{1}$-OT^k can be implemented from $\binom{2}{1}$-$\mathsf{OT}^{k'}$ [7, 9, 21, 44]. There has also been a lot of interest in reductions of OT to weaker primitives. It is known that OT can be realized from noisy channels [12, 14, 18, 47], noisy correlations [42, 33], or weak variants of OT [12, 10, 20, 8, 19, 46].

In the quantum world, it has been shown in [6, 49, 17, 38] that OT can be implemented from black-box commitments, something that is impossible in the classical setting.

Given these positive results it is natural to ask how efficient such reductions can be in principle, i.e., how many instances of a given primitive are needed to implement OT.

1.1 Previous Results

In the classical setting, several lower bounds for OT reductions are known. The first impossibility result for unconditionally secure reductions of OT has been presented in [2]. There it has been shown that the number of $\binom{2}{1}$-OT^1 cannot be *extended*[3], i.e., there does not exist a protocol using n instances of $\binom{2}{1}$-OT^1 that perfectly implements $m > n$ instances. Lower bounds for the number of instances of OT needed to perfectly implement other variants of OT have been presented in [21] (see also [31]) and generalized in [44, 43]. These bounds apply to both the semi-honest (where dishonest players follow the protocol) and the malicious (where dishonest players behave arbitrarily) model. If we restrict ourselves to the malicious model these bounds can be improved, as shown in [28]. Lower bounds on the number of ANDs needed to implement general functions have been presented in [4].

All these results only consider *perfect* protocols and do not give much insight into the case of statistical implementations. As pointed out in [28], their result *only* applies to the perfect case, because there is a statistical protocol that is more efficient [16]. The bounds for perfect and statistical protocols can in fact be *very* far apart, as shown in [4]: The amount of OTs needed to compute the equality function is exponentially bigger in the perfect case than in the statistical case. Therefore, it is not true in general that a bound in the perfect case implies a similar bound in the statistical case.

So far very little is known in the statistical case. In [1] a proof sketch of a lower bound for statistical implementations of $\binom{2}{1}$-OT^k has been presented. However, this result only holds in the asymptotic case, where the number n of resource primitives goes to infinity and the error goes to zero as n goes to infinity. In [4] a non-asymptotic lower bound on the number of ANDs needed for one-sided secure computation of arbitrary functions with *boolean* output has been shown. This result directly implies lower bounds for protocols that use $\binom{n}{t}$-OT^k as a black-box. However, besides being restricted to boolean-valued functions this result is not strong enough to show optimality of several known reductions and it does not provide bounds for reductions to randomized primitives such as $(\frac{1}{2})$-$\mathsf{RabinOT}^1$.

In the quantum setting almost all negative results known show that a certain primitive is impossible to implement from scratch. Commitment has been shown to be impossible in the quantum setting in [32, 30]. Using a similar proof, it has been shown in [29] that general one-sided two-party computation and in particular oblivious transfer are also impossible to implement securely in the quantum setting.

[3] Note that in the computational setting, OT *can* be extended, see [2, 26].

To our knowledge, the only lower bounds for quantum protocols where the players have access to resource primitives (such as different variants of OT) have been presented in [36] where Theorem 4.7 shows that important lower bounds for classical protocols also apply to *perfectly* secure quantum reductions.

1.2 Contribution

Classical Reductions. In Section 2 we consider statistically secure protocols in the semi-honest model that compute a function between two parties from trusted randomness distributed to the players. We provide two bounds on the efficiency of such reductions that allow in particular to derive bounds on the minimal number of $\binom{n}{t}$-OT^k or (p)-$\mathsf{RabinOT}^k$ needed to compute any given function securely. Our bounds do not involve any asymptotics, i.e., we consider a finite number of resource primitives and our results hold for *any* error.

In Section 2.3 we provide an additional bound for the special case of statistical implementations of $\binom{n}{1}$-OT^k. Note that for implementations of OT bounds in the semi-honest model imply similar bounds in the malicious model [4]. The bounds for implementations of $\binom{n}{1}$-OT^k (Theorem 3) imply the following corollary that gives a general bound on the conversion rate between different variants of OT.

Corollary 1. *For any reduction that implements M instances of $\binom{N}{1}$-OT^K from m instances of $\binom{n}{1}$-OT^k in the semi-honest model with an error of at most ε, we have*

$$\frac{m}{M} \geq \max\left(\frac{(N-1)K}{(n-1)k}, \frac{K}{k}, \frac{\log N}{\log n}\right) - 7NK \cdot (\varepsilon + h(\varepsilon)) \, .$$

Corollary 1 generalizes the lower bounds from [21, 44, 43] to the statistical case and is strictly stronger than the impossibility bounds from [1]. If we let $M = m + 1$, $N = n = 2$ and $K = k = 1$, we obtain a stronger version of Theorem 3 from [2] which states that OT cannot be extended.

In the full version of this paper [40], we also derive new bounds in the statistical case for protocols implementing (p)-$\mathsf{RabinOT}^k$, and show that our bounds imply bounds for implementations of oblivious linear function evaluation (OLFE).

[4] For implementations of OT (and any other so-called deviation revealing functionality) security in the malicious model implies security in the semi-honest model [34]. In [40] we show this implication for $\binom{n}{1}$-OT^k and (p)-$\mathsf{RabinOT}^k$ with explicit bounds on the simulation errors.

Our lower bounds show that the following protocols are (close to) optimal in the sense that they use the minimal number of instances of the given primitive.

- The protocol in [9, 21] which uses $\frac{N-1}{n-1}$ instances of $\binom{n}{1}$-OT^k to implement $\binom{N}{1}$-OT^k is optimal.
- The protocol in [44] which uses t instances of $\binom{n}{1}$-$\mathsf{OT}^{kn^{t-1}}$ to implement $\binom{n^t}{1}$-OT^k is optimal.
- In the semi-honest model, the trivial protocol that implements $\binom{2}{1}$-OT^k from k instances of $\binom{2}{1}$-OT^1 is optimal. In the malicious case, the protocol in [16] uses asymptotically (as k goes to infinity) the same amount of instances and is therefore asymptotically optimal.
- The protocol in [37] that implements $\binom{2}{1}$-OT^k from $(\frac{1}{2})$-$\mathsf{RabinOT}^1$ in the malicious model is asymptotically optimal.

Quantum Reductions. While previous result show that quantum protocols show similar limits as classical protocols for reductions between different variants of oblivious transfer, we present in Section 3.1 a statistically secure protocol that violates the classical bounds and the bound for perfectly secure quantum protocols by an arbitrarily large factor. More precisely, we prove that, in the quantum setting, string oblivious transfer can be reversed much more efficiently than by any classical protocol.

Theorem 4. There exists a protocol that implements $\binom{2}{1}$-$\mathsf{OT}^{k'}$ with an error ε from $\kappa = O(\log 1/\varepsilon)$ instances of $\binom{2}{1}$-OT^k in the opposite direction where $k' = \Omega(k)$ if $k = \Omega(\kappa)$.

For classical and perfect quantum protocols k' is essentially upper bounded by κ. In Theorem 5 we show that a weaker lower bound for quantum reductions holds also for quantum protocols in the statistical setting. Theorem 5 implies that quantum protocols cannot extend oblivious transfer, i.e., we show that there exists a constant $c > 0$ such that any quantum reduction of $m+1$ instances of $\binom{2}{1}$-OT^1 to m instances of $\binom{2}{1}$-OT^1 must have an error of at least $\frac{c}{m}$.

Furthermore, Theorem 5 implies a lower bound for reductions between different variants of OT.

Corollary 2. *For any quantum reduction that implements $\binom{2}{1}$-OT^K from m instances of $\binom{n}{1}$-OT^k with an error smaller than ε, we have*

$$m \geq \frac{K}{2nk + 2\log n} - 3K\sqrt{\varepsilon} - 13h(\sqrt{\varepsilon}) \ .$$

Finally, we also derive a lower bound on the number of commitments (Theorem 7) and on the total number of bits the players need to commit to (Theorem 6) in any ε-secure implementation of $\binom{2}{1}$-OT^k from commitments.

Corollary 3. *A protocol that implements $\binom{2}{1}$-OT^k, using commitments only, with an error of at most ε must use at least $\log(1/\varepsilon)-6$ commitments and needs to commit to at least $k/2 - 12k\sqrt{\varepsilon} - 7h(\sqrt{\varepsilon})$ bits in total.*

Corollary 3 implies that bit commitments cannot be extended. More precisely, there exists a constant $c > 0$ such that any protocol that implements $m+1$ bit commitments out of m bit commitments must have an error of at least $\frac{c}{m}$. Finally, in Section 8 we show that there exists a protocol that is essentially optimal with respect to Corollary 3. We use the protocol from [6, 17], but let the receiver commit to blocks of measurements at once, to prove the following theorem.

Theorem 8. There exists a quantum protocol that implements $\binom{2}{1}$-OT^k with an error of at most ε, using $\kappa = O(\log 1/\varepsilon)$ commitments to strings of size b, where $\kappa b = O(k + \log 1/\varepsilon)$.

All proofs are in the full version of this work [40].

1.3 Notation

We use calligraphic letters to denote sets. We denote the distribution of a random variable X over $\mathcal{X}$ by P_X. A conditional distribution $P_{X|Y}(x, y)$ over $\mathcal{X} \times \mathcal{Y}$ defines for every $y \in \mathcal{Y}$ a distribution $P_{X|Y=y}$. $P_{X|Y}$ can be seen as a randomized function that has input y and output x. The *conditional Shannon entropy* of X given Y is defined as[5]

$$\mathrm{H}(X \mid Y) := -\sum_{x,y} P_{XY}(x,y) \log P_{X|Y}(x,y) \ ,$$

and the *mutual information* of X and Y as $\mathrm{I}(X;Y) = \mathrm{H}(X) - \mathrm{H}(X \mid Y)$. We use the notation $h(p) = -p\log p - (1-p)\log(1-p)$ for the binary entropy function. Furthermore, we write $[k]$ to denote the set $\{1, \ldots, k\}$. If $x = (x_1, \ldots, x_n)$ and $T := \{i_1, \ldots, i_k\} \subseteq [n]$, then $x|_T$ denotes the substring $(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ of x. If $x, y \in \{0,1\}^n$, then $x \oplus y$ denotes the bitwise XOR of x and y.

[5] All logarithms are binary, and we use the convention that $0 \cdot \log 0 = 0$.

1.4 Primitives and Randomized Primitives

In the following we consider two-party primitives that take inputs x from Alice and y from Bob and outputs $\bar{x}$ to Alice and $\bar{y}$ to Bob, where $(\bar{x}, \bar{y})$ are distributed according to $P_{\bar{X}\bar{Y}|XY}$. For simplicity, we identify such a primitive with $P_{\bar{X}\bar{Y}|XY}$. If the primitive has no input and outputs values (u, v) distributed according to P_{UV}, we may simply write P_{UV}. If the primitive is deterministic and only Bob gets an output, i.e., if there exists a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ such that $P_{\bar{X}\bar{Y}|X=x,Y=y}(\bot, f(x, y)) = 1$ for all x, y, then we identify the primitive with the function f.

Examples of such primitives are $\binom{n}{t}$-OT^k, (p)-$\mathsf{RabinOT}^k$, EQ_n and IP_n.

- $\binom{n}{t}$-OT^k is the primitive where Alice has an input $x = (x_0, \dots, x_{n-1}) \in \{0,1\}^{k \cdot n}$, and Bob has an input $c \subseteq \{0, \dots, n-1\}$ with $|c| = t$. Bob receives $y = x|_c \in \{0,1\}^{tk}$.
- (p)-$\mathsf{RabinOT}^k$ is the primitive where Alice has an input $x \in \{0,1\}^k$. Bob receives y which is equal to x with probability p and Δ otherwise.
- The *equality* function $\mathsf{EQ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as $\mathsf{EQ}_n(x, y) = 1$ if $x = y$ and $\mathsf{EQ}_n(x, y) = 0$ otherwise.
- The *inner product modulo two* function $\mathsf{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is defined as $\mathsf{IP}_n(x, y) = \oplus_{i=1}^n x_i y_i$.

We often allow a protocol to use a primitive P_{UV} that does not have any input. This is enough to model reductions to $\binom{n}{t}$-OT^k and (p)-$\mathsf{RabinOT}^k$, since these primitives are equivalent to distributed randomness P_{UV}, i.e., there exist two protocols that are secure in the semi-honest model: one that generates the distributed randomness using *one* instance of the primitive, and one that implements *one* instance of the primitive using the distributed randomness as input to the two parties. The fact that $\binom{2}{1}$-OT^1 is equivalent to distributed randomness has been presented in [6, 3]. The generalization to $\binom{n}{t}$-OT^k is straightforward. The randomized primitives are obtained by simply choosing all inputs uniformly at random. For (p)-$\mathsf{RabinOT}^k$ the implementation is straightforward. Hence, any protocol that uses some instances of $\binom{n}{t}$-OT^k or (p)-$\mathsf{RabinOT}^k$ can be converted into a protocol that only uses a primitive P_{UV} without any input.

2 Lower Bounds for Classical Two-Party Computation

2.1 Protocols and Security in the Semi-Honest Model

We will consider the *semi-honest model*, where both players behave honestly, but may save all the information they get during the protocol to obtain extra information about the other player's input or output. A protocol securely implements $P_{\bar{X}\bar{Y}|XY}$ with an error of ε, if the entire view of each player can be simulated[6] with an error of at most ε in an ideal setting, where the players only have black-box access to the primitive $P_{\bar{X}\bar{Y}|XY}$. Note that this simulation is not allowed to change neither the input nor the output. (See the full version [40] for a formal definition.) This definition of security follows Definition 7.2.1 from [24], but is adapted to the case of computationally unbounded adversaries and statistical indistinguishability.

2.2 Lower Bounds for Secure Function Evaluation

We will now give lower bounds for ε-secure implementations of functions $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ from a primitive P_{UV} in the semi-honest model. A function f has no redundant inputs for Alice if

$$\forall x \neq x' \in \mathcal{X}\ \exists y \in \mathcal{Y} :\ f(x,y) \neq f(x',y)\ . \tag{2.1}$$

Clearly, a function f can be computed from a primitive P_{UV} with an error ε in the semi-honest model if and only if the function f' obtained by combining all redundant inputs for Alice can be computed with the same error.

Let Alice's and Bob's inputs X and Y be independent and uniformly distributed and let M be the whole communication in the protocol. Loosely speaking, Alice must enter (almost) all the information about X into the protocol as follows: If Bob's input is y, then he must be able to compute $f(X,y)$. But, as Alice must not learn y, she has to enter all information about $f(X,y)$ into the protocol independent of Bob's input. Thus, Alice must input all information about $f(X,y)$ into the protocol for all y. If f satisfies (2.1), then $\{f(x,y) :\ y \in \mathcal{Y}\}$ allows to compute x. Thus, Alice must enter all information about X into the protocol. More precisely, it can be shown that

$$H(X \mid UM, Y = y) \leq (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon))\ .$$

Since the protocol is secure against Bob, one can prove that for all y

$$\mathrm{H}(X \mid VM, Y = y) \geq \mathrm{H}(X \mid f(X,y)) - \varepsilon \log |\mathcal{X}| - h(\varepsilon)\ .$$

The following theorem that gives a lower bound on the conditional entropy of P_{UV} can then be obtained from these two inequalities.

[6] The simulation is not required to be efficient.

Theorem 1. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function that satisfies (2.1). Let a protocol having access to P_{UV} be an ε-secure implementation of f in the semi-honest model. Then*

$$\mathrm{H}(U \mid V) \geq \max_y \mathrm{H}(X \mid f(X,y)) - 3|\mathcal{Y}|(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) - \varepsilon \log |\mathcal{X}| \ .$$

Note that for some functions the bound of Theorem 1 can be improved by maximizing over all restrictions of the function f, i.e., over all functions $f'(x,y) : \mathcal{X}' \times \mathcal{Y}' \to \mathcal{Z}'$ where $\mathcal{X}' \subset \mathcal{X}$, $\mathcal{Y}' \subset \mathcal{Y}$ and $\mathcal{Z}' \subset \mathcal{Z}$ with $f'(x,y) = f(x,y)$ that still satisfy condition (2.1).

Any lower bound for f' implies a lower bound for f. The following corollaries follow immediately from Theorem 1.

Corollary 4. *Let a protocol having access to P_{UV} be an ε-secure implementation of $\binom{n}{t}$-OT^k in the semi-honest model. Then*

$$\mathrm{H}(U \mid V) \geq (n-t)k - 3\lceil n/t \rceil(\varepsilon t k + h(\varepsilon)) - \varepsilon n k \ .$$

Corollary 5. *Let a protocol having access to P_{UV} be an ε-secure implementation of EQ_n in the semi-honest model. Then*

$$\mathrm{H}(U|V) \geq \max_{0<k\leq n} ((1-\varepsilon)k - 3 \cdot 2^k(\varepsilon + h(\varepsilon)) - 1 \ .$$

There exists a secure reduction of EQ_n to EQ_k [4]: Alice and Bob compare k inner products of their inputs with random strings using EQ_k. This protocol is secure in the semi-honest model with an error[7] of at most $2^{-\kappa}$. Since there exists a circuit to implement EQ_k with k XOR and k AND gates, it follows from [25] that EQ_k can be securely implemented using k instances to $\binom{4}{1}$-OT^1 or $3k$ instances of $\binom{2}{1}$-OT^1 in the semi-honest model. Since m instances of $\binom{2}{1}$-OT^1 are equivalent to a primitive P_{UV} with $H(U|V) = m$, the bound of Corollary 5 is optimal up to a factor of 3. This implies that the term $|\mathcal{Y}|$ in the statement of the bound given in Theorem 1 cannot be reduced significantly, i.e., it is not possible to replace $|\mathcal{Y}|$ with $\log |\mathcal{Y}|$ for example.

Corollary 6. *Let a protocol having access to a primitive P_{UV} be an ε-secure implementation of the inner product function IP_n in the semi-honest model. Then $\mathrm{H}(U|V) \geq n - 1 - 4n(\varepsilon + h(\varepsilon))$.*

[7] Note that our security definition is different from the one used in [4].

If $\varepsilon + h(\varepsilon) \leq 1/8$, then it immediately follows from Corollary 6 that we need at least $n/2 - 1$ calls to $\binom{2}{1}$-OT^1 to compute IP_n with an error of at most ε. From the protocol presented in [4] we know that there exists a perfectly secure protocol that computes IP_n from n instances of $\binom{2}{1}$-OT^1. Therefore, the bound is optimal up to a factor of 2.

For our next lower-bound, the function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ must satisfy the following property. There exist $y_1 \in \mathcal{Y}$ such that

$$\forall x \neq x' \in \mathcal{X} : f(x, y_1) \neq f(x', y_1) \ , \tag{2.2}$$

and $y_2 \in \mathcal{Y}$ such that

$$\forall x, x' \in \mathcal{X} : f(x, y_2) = f(x', y_2) \ . \tag{2.3}$$

Let Alice's input X be uniformly distributed. Loosely speaking, the security of the protocol implies that the communication gives (almost) no information about Alice's input X if Bob's input is y_2. But the communication must be (almost) independent of Bob's input, otherwise Alice could learn Bob's input. Thus, Alice's input X is uniform with respect to the whole communication even when Bob's input is y_1. Let now Bob's input be fixed to y_1 and let M be the whole communication. Then the following lower bound can be proved using the given intuition.

$$H(f(X, y_1) \mid M) \geq \log |\mathcal{X}| - 6\varepsilon \log |\mathcal{X}| - 6h(\varepsilon) \ .$$

As Bob must be able to compute the correct output, one can show that

$$\mathrm{H}(f(X, y_1) \mid VM) \leq \varepsilon \log |\mathcal{X}| + h(\varepsilon) \ .$$

The following lower bound on the mutual information of P_{UV} can be obtained from these two inequalities.

Theorem 2. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function that satisfies (2.2) and (2.3). Then for any protocol that implements f from a primitive P_{UV} with an error of at most ε in the semi-honest model*

$$\mathrm{I}(U; V) \geq \log |\mathcal{X}| - 7\varepsilon \log |\mathcal{X}| - 7h(\varepsilon) \ .$$

Since properties (2.2) and (2.3) can be satisfied by restricting Alice's input in $\binom{n}{t}$-OT^k, we obtain the following corollary.

Corollary 7. *Let a protocol having access to P_{UV} be an ε-secure implementation of $\binom{n}{t}$-OT^k in the semi-honest model where $t \leq \lfloor n/2 \rfloor$. Then*

$$I(U; V) \geq tk - 7\varepsilon tk - 7h(\varepsilon) \ .$$

We further generalize Theorem 2 to arbitrary functions $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ in [40]. In the case of perfect implementations the bound $H(U) = H(U|V) + I(U;V) \geq \log|\mathcal{X}|$ follows from Theorem 1 and the generalization of Theorem 2. From this bound we get that any perfectly secure protocol needs at least $\log|\mathcal{X}|$ instances of $\binom{2}{1}$-OT^1 to implement a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, which implies Theorem 4.11 from [4].

2.3 Lower Bounds for Protocols implementing OT

$\binom{2}{1}$-OT^1 can be implemented from one instance of $\binom{2}{1}$-OT^1 in the opposite direction [45]. Therefore, it follows immediately from Corollary 4 that for any ε-secure reduction of $\binom{2}{1}$-OT^1 to P_{UV}, we must also have

$$\mathrm{H}(V \mid U) \geq 1 - 5(\varepsilon + h(\varepsilon)) ,$$

since any violation of this bound could be used to construct a violation of the bound from Corollary 4. This bound can be generalized to $n > 0$. Together with the bounds from Theorem 1 and 2 we get the following theorem.

Theorem 3. *Let a protocol having access to P_{UV} be an ε-secure implementation of m instances of $\binom{n}{1}$-OT^k in the semi-honest model. Then*

$$\begin{aligned} \mathrm{H}(U \mid V) &\geq m(n-1)k - 4n(\varepsilon mk + h(\varepsilon)), \\ \mathrm{H}(V \mid U) &\geq m \log n - m(4 \log n + 7)(\varepsilon + h(\varepsilon)), \\ \mathrm{I}(U;V) &\geq mk - 7\varepsilon mk - 7h(\varepsilon) . \end{aligned}$$

The statement of Corollary 1 follows from the fact that m instances of $\binom{n}{1}$-OT^k are equivalent to a primitive P_{UV} with $\mathrm{H}(U \mid V) = m(n-1)k$, $\mathrm{I}(U;V) = mk$ and $\mathrm{H}(V \mid U) = m \log n$.

In the full version of this paper [40], we show that the bounds of Theorem 1-3 can be generalized to the monotones from [43]. Furthermore, we derive new bounds for protocols implementing (p)-$\mathsf{RabinOT}^k$, and show that our bounds imply bounds for implementations of oblivious linear function evaluation (OLFE).

3 Quantum Reductions

3.1 Reversing String OT Efficiently

As the bounds of the last section generalize the known bounds for perfect implementations of OT from [2, 21, 44, 43] to the statistical case, it is natural to ask whether similar bounds also hold for quantum protocols, i.e., if the bounds presented in [36] can be generalized to the statistical case. We give a negative answer to this question by presenting a statistically secure quantum protocol that violates these bounds.

$\binom{2}{1}$-OT^k can be implemented from $m = O(k + \kappa)$ bit commitments with an error of $2^{-\Omega(\kappa)}$ [6, 49, 17]. In the protocol, Alice sends m BB84-states to Bob who measures them either in the computational or in the diagonal basis. To ensure that he really measures Bob has to commit to the basis he has measured in and the measurement outcome for every qubit received. Alice then asks Bob to open a small subset $\mathcal{T}$ of size αm of these pairs of commitments. OT can then be implemented using further classical processing. (See [17] for a complete description of the protocol.) This protocol implements oblivious transfer that is statistically secure in the quantum *universal composability* model [38]. Obviously the m instances of bit commitments can be replaced by a single functionality, denoted by $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,m}$, which allows one player to commit to a bit string of length m and later open an arbitrary substring. The following protocol implements $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ from the oblivious transfer functionality $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ (see [38] for a definition of $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$).

Inputs: Alice has an input $b = (b_1, \ldots, b_k) \in \{0,1\}^k$ in `Commit`. Bob has an input $T \subseteq [k]$ in `Open`.
`Commit(`b`)`:
For all $1 \leq i \leq \kappa$:

1. Alice and Bob invoke $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ with random inputs $x_0^i, x_1^i \in \{0,1\}^k$ and $c^i \in_R \{0,1\}^k$.
2. Bob receives $y^i = x_{c^i}^i$ from $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$.
3. Alice sends $m^k := x_0^i \oplus x_1^i \oplus b$ to Bob.

`Open`(T):

1. Alice sends $b|_T$, T and $x_0^i|_T, x_1^i|_T$ for all $1 \leq i \leq \kappa$ to Bob.
2. If $m^i|_T = x_0^i|_T \oplus x_1^i|_T \oplus b^i|_T$ and $y^i|_T = x_c^i|_T$ for all $1 \leq i \leq \kappa$, Bob accepts and outputs b_T, otherwise he rejects.

Lemma 1. *There exists a protocol that is statistically secure and universally composable that realizes $\mathcal{F}_{\mathit{MCOM}}^{A\to B,k}$ with an error of $2^{-\kappa/2}$ using κ instances of $\mathcal{F}_{\mathit{OT}}^{A\to B,k}$.*

Since any protocol that is also statistically secure in the classical universal composability model [11] is also secure in the quantum universal composability model [38], we get, together with the proofs from [17, 38], the following theorem.

Theorem 4. *There exists a protocol that implements* $\binom{2}{1}$-$\mathsf{OT}^{k'}$ *with an error* ε *from* $\kappa = O(\log 1/\varepsilon)$ *instances of* $\binom{2}{1}$-OT^{k} *in the opposite direction where* $k' = \Omega(k)$ *if* $k = \Omega(\kappa)$.

Since we can choose $k \gg \kappa$, this immediately implies that the bound of Corollary 4 does not hold for quantum protocols. Similar violations can be shown for the other two lower bounds given in Theorem 7. For example, statistically secure and universally composable[8] commitments can be implemented from shared randomness P_{UV} that is distributed according to (p)-$\mathsf{RabinOT}$ at a rate of $H(U \mid V) = 1 - p$ [41]. Using Theorem 8, one can implement $\mathcal{F}_{\mathtt{OT}}^{B \to A, k}$ with $k \in \Omega(n(1-p))$ from n copies of P_{UV}. Since $\mathrm{I}(U;V) = p$, quantum protocols can also violate the bound of Corollary 7.

It has been an open question whether noiseless quantum communication can increase the commitment capacity [41]. Our example implies a positive answer to this question.

3.2 Lower Bounds

The protocols presented in the previous section prove that the known impossibility results for perfectly secure oblivious transfer reductions from [36] do not hold for statistically secure quantum protocols. Thus, it is natural to ask whether quantum protocols can even extend oblivious transfer or, more generally, how efficient statistically secure quantum protocols can be. In this section we prove an impossibility result that holds for statistically secure quantum protocols and that implies in particular that also quantum protocols *cannot* extend OT. Since, in contrast to the classical case, security against semi-honest adversaries can be trivially achieved in the quantum setting, we consider in the following protocols that are secure against malicious adversaries in the stand-alone model. A protocol is an ε-secure implementation of OT if for any adversary attacking the protocol (real setting), there exists a simulator using the ideal OT (ideal setting) such that for all inputs of the honest players the real and the ideal setting can be distinguished with an advantage of at most ε.

In the following we will give two lower bounds for quantum protocols that implement $\binom{2}{1}$-OT^k using a trusted resource such as trusted randomness distributed to the players or a bit commitment functionality.

[8] Stand-alone statistically secure commitments based on stateless two-party primitives are universally composable [22].

Our proofs use similar techniques as the impossibility results in [32, 30, 29]. First, the protocol is replaced by a purified version of the protocol that is equivalent in a certain sense. In particular the purified version has the same security properties as the original protocol and the impossibility of the former implies the impossibility of the latter. In this protocol the players defer all of their measurements to the very end of the protocol. See [32, 30, 29] for details.

We use the notation ρ^{AB} for a state in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and $\rho^A := \mathrm{tr}_B(\rho^{AB})$. The *conditional von Neumann entropy* is defined as $H(A \mid B)_\rho := H(\rho^{AB}) - H(\rho^B)$, where $H(\rho) := \mathrm{tr}(-\rho \log(\rho))$.

We first consider protocols where the players have access to a primitive that generates a pure state $|\psi\rangle^{ABE}$, distributes registers A and B to Alice and Bob respectively and keeps the purification in its register E.

Let Alice choose her inputs X_0 and X_1 uniformly at random and let Bob's input be c. When Alice and Bob execute the purified protocol honestly the final state just before the honest players perform their measurements is a pure state $|\rho\rangle_c^{ABE}$, where A and B are the registers of Alice and Bob and E is the register of the trusted resource.

Loosely speaking, security for Alice guarantees that Bob has (almost) no information about X_0 if $c = 1$, i.e., the entropy $H(X_0 \mid B)_{\rho_1}$ is almost maximal. On the other hand, Alice must not be able to learn Bob's choice bit. Therefore, we have $\rho_0^A \approx \rho_1^A$. As shown in [32, 30, 29], this implies that there exists a unitary on system BE that transforms $|\rho\rangle_1^{ABE}$ into a state close to $|\rho\rangle_0^{ABE}$. Since Bob can learn X_0 if $c = 0$, this implies that $H(X_0 \mid BE)_{\rho_1}$ is small. Using these two facts, one can then prove the following lower bound on the entropy of E.

Theorem 5. *To implement one instance of $\binom{2}{1}$-OT^k over strings of size k with an error of at most ε from a primitive $|\psi\rangle^{ABE}$ with a quantum protocol we need*

$$2H(E)_\psi \geq (1 - 21\varepsilon - 2\sqrt{\varepsilon}) \cdot k - 11h(\varepsilon) - 2h(\sqrt{\varepsilon}) \ .$$

A classical primitive P_{UV} can be modeled by the quantum primitive

$$|\psi\rangle^{ABE} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle^{AB} \otimes |u,v\rangle^{E}$$

that distributes the values u and v and keeps the purification in its register E. Therefore, we get the following corollary from Theorem 5.

Corollary 8. *To implement one instance of* $\binom{2}{1}$*-*OT^k *with an error of at most* ε *from* P_{UV} *with a quantum protocol, we need*

$$2H(UV) \geq (1 - 21\varepsilon - 2\sqrt{\varepsilon}) \cdot k - 11h(\varepsilon) - 2h(\sqrt{\varepsilon}) \; .$$

Since m instances of $\binom{2}{1}$-OT^k can be implemented from shared randomness with $H(UV) = 2k + 1$ we get the following corollary.

Corollary 9. *To implement one instance of* $\binom{2}{1}$*-*OT^k *with an error of at most* ε *from* n *instances of* $\binom{2}{1}$*-*$\mathsf{OT}^{k'}$ *in either direction with a quantum protocol, we need*

$$2n(2k' + 1) \geq (1 - 21\varepsilon - 2\sqrt{\varepsilon}) \cdot k - 11h(\varepsilon) - 2h(\sqrt{\varepsilon}) \; .$$

Next, we present a bound for implementations of $\binom{2}{1}$-OT^k from commitments. We can model black-box commitments by a trusted functionality that receives bits over a classical channel and stores them in a register E. When the committer sends the open command, the functionality sends the bits to the receiver. We can replace the two classical channels with a quantum channel where the players measure the qubits when sending and after receiving them. These measurements can then be purified by the players. The following bound can be obtained by adapting the proof of Theorem 5 to this scenario.

Theorem 6. *To implement a* $\binom{2}{1}$*-*OT^k *with an error of at most* ε *we need to commit to at least* $(1 - 21\varepsilon - 2\sqrt{\varepsilon})k/2 - 6h(\varepsilon) - h(\sqrt{\varepsilon})$ *bits in total.*

From Corollary 9 and Theorem 6 follows that OTs and commitments cannot be extended by quantum protocols.

Corollary 10. *Any quantum protocol that implement* $m + 1$ *instances of* $\binom{2}{1}$*-*OT^1 *from* m *instances of* $\binom{2}{1}$*-*OT^1 *must have an error of at least* $\frac{5 \cdot 10^{-6}}{m}$ *for any* $m > 0$*.*

Corollary 11. *Any quantum protocol that implements* $m+1$ *bit commitments out of* m *commitments must have an error of at least* $\frac{10^{-9}}{m}$ *for any* $m > 0$*.*

Next, we give an additional lower bound for reductions of OT to commitments that shows that the *number* of commitments (of arbitrary size) used in any ε-secure protocol must be at least $\Omega(\log(1/\varepsilon))$. We model the commitments as before, but store the commitments of Alice and Bob separately in E_A and E_B. The proof idea is the following: We let the adversary guess a subset $\mathcal{T}$ of commitments that he will be required to open during the protocol. He honestly executes all commitments in $\mathcal{T}$, but cheats in all others. If the adversary guesses $\mathcal{T}$ right, he is able to cheat in the same way as in any protocol that does not use any commitments.

Theorem 7. *Any quantum protocol that implements $\binom{2}{1}$-OT^k using κ commitments (of arbitrary length) must have an error of at least $2^{-\kappa}/36$.*

3.3 Reduction of OT to String-Commitments

The protocol we described in Section 3.1 uses $m = O(k + \kappa)$ commitments to 2 bits to implement $\binom{2}{1}$-OT^k with an error of $2^{-\Omega(\kappa)}$. If $k = \omega(\kappa)$ this it is not optimal with respect to Theorem 7. We will now show how to construct a protocol that is optimal with respect to the lower bounds of both Theorem 6 and Theorem 7. We modify the protocol by grouping the m pairs into κ blocks of size $b := m/\kappa$. We let Bob commit to the blocks of b pairs of values at once. The subset $\mathcal{T}$ is now of size $\alpha\kappa$, and defines the blocks to be opened by Bob. If Bob is able to open all commitments in $\mathcal{T}$ correctly, then with high probability, he must have correctly measured almost all qubits. We only need to estimate the error probability of the sampling strategy that corresponds to the new checking procedure which Alice applies and apply the proof of [17] to get the following theorem.

Theorem 8. *There exists a quantum protocol that implements $\binom{2}{1}$-OT^k with an error of at most ε out of $\kappa = O(\log 1/\varepsilon)$ commitments of size b, where $\kappa b = O(k + \log 1/\varepsilon)$.*

Using Theorem 8, it can be shown that string-commitments cannot be extended.

Corollary 12. *Let $m > 0$. If there exists a (quantum) protocol that implements string commitments of length $m' + 1$ out of string commitments of length m' for all $m' > m$ with an error of at most ε, then there exists a constant $c > 0$ such that $\varepsilon \geq \frac{c}{m}$.*

4 Conclusions

The main contribution of this work are impossibility proofs for statistical oblivious transfer reductions. In the classical case we have generalized several known lower bounds for perfect reductions to statistical security. In the quantum case we have shown that the known bound for perfect reductions does not apply to statistical reductions, and have presented a new bound that *does* hold in the statistical quantum setting. Our bounds imply several important impossibility results, for example, that OT cannot be extended, neither in the classical nor in the quantum setting.

There are many interesting open questions. For example, it is not known whether more than two instances of $\binom{2}{1}$-OT^1 can be implemented (in the classical or the quantum setting) from two instances of $\binom{2}{1}$-OT^ℓ, one in each direction.

Acknowledgments

We thank Esther Hänggi, Thomas Holenstein and Stephanie Wehner for helpful discussions, and the referees for their useful comments. This work was funded by the Swiss National Science Foundation (SNSF) and the U.K. EPSRC, grant EP/E04297X/1. Part of this work was done while JW was visiting McGill University.

References

1. Ahlswede, R., Csiszar, I.: On oblivious transfer capacity. In: Networking and Information Theory, 2009. ITW 2009. IEEE Information Theory Workshop on. pp. 1 –3 (12-10 2009)
2. Beaver, D.: Correlated pseudorandomness and the complexity of private computations. In: STOC 1996: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. pp. 479–488. ACM Press (1996)
3. Beaver, D.: Precomputing oblivious transfer. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 97–109. Springer (1995)
4. Beimel, A., Malkin, T.: A quantitative approach to reductions in secure computation. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 238–257. Springer (2004)
5. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM Journal on Computing 17(2), 210–229 (1988)
6. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366 (1991)
7. Brassard, G., Crépeau, C., Robert, J.M.: Information theoretic reductions among disclosure problems. In: Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science (FOCS '86). pp. 168–173 (1986)
8. Brassard, G., Crépeau, C., Wolf, S.: Oblivious transfers and privacy amplification. Journal of Cryptology 16(4), 219–237 (2003)
9. Brassard, G., Crépeau, C., Santha, M.: Oblivious transfers and intersecting codes. IEEE Transactions on Information Theory 42(6), 1769–1780 (1996)
10. Cachin, C.: On the foundations of oblivious transfer. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 361–374. Springer (1998)
11. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: FOCS 2001. pp. 136–145 (2001)

12. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions (extended abstract). In: Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS '88). pp. 42–52 (1988)
13. Crépeau, C.: Equivalence between two flavours of oblivious transfers. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 350–354. Springer (1987)
14. Crépeau, C., Morozov, K., Wolf, S.: Efficient unconditional oblivious transfer from almost any noisy channel. In: Blundo, C., Cimato, S. (eds.) SCN 2004. pp. 47–59. LNCS, Springer (2004)
15. Crépeau, C., Santha, M.: On the reversibility of oblivious transfer. In: Davies, D.W. (ed.) EUROCRYPT 1991. Lecture Notes in Computer Science, vol. 547, pp. 106–113. Springer (1991)
16. Crépeau, C., Savvides, G.: Optimal reductions between oblivious transfers using interactive hashing. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 201–221. Springer (2006)
17. Damgård, I., Fehr, S., Lunemann, C., Salvail, L., Schaffner, C.: Improving the security of quantum protocols via commit-and-open. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 408–427. Springer (2009)
18. Damgård, I., Fehr, S., Morozov, K., Salvail, L.: Unfair noisy channels and oblivious transfer. In: Naor, M. (ed.) TCC 2004. pp. 355–373. LNCS, Springer (2004)
19. Damgård, I., Fehr, S., Salvail, L., Schaffner, C.: Oblivious transfer and linear functions. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 427–444. Springer (2006)
20. Damgård, I., Kilian, J., Salvail, L.: On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 56–73 (1999)
21. Dodis, Y., Micali, S.: Lower bounds for oblivious transfer reductions. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 42–55. Springer (1999)
22. Dowsley, R., van de Graaf, J., Müller-Quade, J., Nascimento, A.C.A.: On the composability of statistically secure bit commitments. Cryptology ePrint Archive, Report 2008/457 (2008)
23. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Commun. ACM 28(6), 637–647 (1985)
24. Goldreich, O.: Foundations of Cryptography, vol. II: Basic Applications. Cambridge University Press (2004)
25. Goldreich, O., Vainish, R.: How to solve any protocol problem - an efficiency improvement. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 73–86. Springer (1987)
26. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 145–161. Springer (2003)
27. Kilian, J.: Founding cryptography on oblivious transfer. In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88). pp. 20–31. ACM Press (1988)
28. Kurosawa, K., Kishimoto, W., Koshiba, T.: A combinatorial approach to deriving lower bounds for perfectly secure oblivious transfer reductions. IEEE Transactions on Information Theory 54(6), 2566–2571 (2008)
29. Lo, H.K.: Insecurity of quantum secure computations. Physical Review A 56, 1154 (1997)
30. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Physical Review Letters 78, 3410–3413 (1997)

31. Maurer, U.: Information-theoretic cryptography. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 47–64. Springer (1999)
32. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Physical Review Letters 78, 3414–3417 (1997)
33. Nascimento, A., Winter, A.: On the oblivious transfer capacity of noisy correlations. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT '06) (2006)
34. Prabhakaran, M., Rosulek, M.: Cryptographic complexity of multi-party computation problems: Classifications and separations. In: Wagner, D. (ed.) CRYPTO 2008. pp. 262–279 (2008)
35. Rabin, M.O.: How to exchange secrets by oblivious transfer. Tech. Rep. TR-81, Harvard Aiken Computation Laboratory (1981)
36. Salvail, L., Schaffner, C., Sotáková, M.: On the power of two-party quantum cryptography. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 70–87 (2009)
37. Savvides, G.: Interactive Hashing and reductions between Oblivious Transfer variants. Ph.D. thesis, McGill University, Montréal (2007)
38. Unruh, D.: Universally composable quantum multi-party computation. In: EUROCRYPT 2010. LNCS, Springer (June 2010), to appear.
39. Wiesner, S.: Conjugate coding. SIGACT News 15(1), 78–88 (1983)
40. Winkler, S., Wullschleger, J.: On the efficiency of classical and quantum oblivious transfer reductions. Cryptology ePrint Archive, Report 2009/508 (2009)
41. Winter, A., Nascimento, A.C.A., Imai, H.: Commitment capacity of discrete memoryless channels. In: IMA Int. Conf. pp. 35–51 (2003)
42. Wolf, S., Wullschleger, J.: Zero-error information and applications in cryptography. In: Proceedings of 2004 IEEE Information Theory Workshop (ITW '04) (2004)
43. Wolf, S., Wullschleger, J.: New monotones and lower bounds in unconditional two-party computation. IEEE Transactions on Information Theory 54(6), 2792–2797 (2008)
44. Wolf, S., Wullschleger, J.: New monotones and lower bounds in unconditional two-party computation. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 467–477. Springer (2005)
45. Wolf, S., Wullschleger, J.: Oblivious transfer is symmetric. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 222–232. Springer (2006)
46. Wullschleger, J.: Oblivious-transfer amplification. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 555–572. Springer (2007)
47. Wullschleger, J.: Oblivious transfer from weak noisy channels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 332–349 (2009)
48. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82). pp. 160–164 (1982)
49. Yao, A.C.C.: Security of quantum protocols against coherent measurements. In: STOC 1995: Proceedings of the 27th Annual ACM Symposium on Theory of Computing. pp. 67–75. ACM Press (1995)