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 ([60]). 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 [33, 37]. The original form of OT ($(\frac{1}{2})\text{-}\mathsf{RabinOT}^1$) has been introduced by Rabin in [47]. 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 ($\binom{2}{1}\text{-}\mathsf{OT}^1$) was defined in [28] (see also [52]). 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 $\binom{n}{t}\text{-}\mathsf{OT}^k$ where the inputs are strings of k bits and the receiver can choose $t < n$ out of n secrets and $(p)\text{-}\mathsf{RabinOT}^k$ 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 [18] 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 [7, 20, 12, 11], and $\binom{n}{1}$-OT^k can be implemented from $\binom{2}{1}$-$\mathsf{OT}^{k'}$ [10, 12, 26, 56]. 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 [17, 19, 23, 59], noisy correlations [54, 44], or weak variants of OT [17, 13, 25, 11, 24, 58].

In the quantum world, it has been shown in [8, 61, 22, 51] 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 [4]. 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 [26] (see also [42]) and generalized in [56, 55]. 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 [38]. Lower bounds on the number of ANDs needed to implement general functions have been presented in [6].

All these results only consider *perfect* protocols and do not give much insight into the case of statistical implementations. As pointed out in [38], their result *only* applies to the perfect case, because there is a statistical protocol that is more efficient ([21]). The bounds for perfect and statistical protocols can in fact be *very* far apart, as shown in [6]: 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 [6] 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 [43, 41]. Using a similar proof, it has been shown in [40] that general one-sided two-party computation and in particular oblivious transfer are also impossible to implement securely in the quantum setting.

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 [48] where Theorem 4.7 shows that important lower bounds for classical protocols also apply to *perfectly* secure quantum reductions.

[3] Note that in the computational setting, OT *can* be extended, see [4, 35].

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 2.5 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 [26, 56, 55] 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 [4] which states that OT cannot be extended.

In Appendix B, 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).

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 [12, 26] 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 [56] 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 [21] uses asymptotically (as k goes to infinity) the same amount of instances and is therefore asymptotically optimal.
- The protocol in [49] 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 $k = \Omega(\kappa)$.

[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 [46]. In Appendix A we show this implication for $\binom{n}{1}$-OT^k and (p)-$\mathsf{RabinOT}^k$ with explicit bounds on the simulation errors.

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 [8, 22], 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 $\kappa b = O(k + \log 1/\varepsilon)$.

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. Given the distribution P_{XY} over $\mathcal{X} \times \mathcal{Y}$, the marginal distribution is denoted by $P_X(x) := \sum_{y \in \mathcal{Y}} P_{XY}(x,y)$. 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 *statistical distance* between the distributions P_X and $P_{X'}$ over the domain $\mathcal{X}$ is defined as the maximum, over all (inefficient) distinguishers $D : \mathcal{X} \to \{0,1\}$, of the distinguishing advantage

$$\delta(P_X, P_{X'}) = \mid \Pr[D(X) = 1] - \Pr[D(X') = 1] \mid \; .$$

If $\delta(P_X, P_{X'}) \leq \varepsilon$, we may also say that P_X is ε-close to $P_{X'}$. 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

$$\mathrm{I}(X;Y) = \mathrm{H}(X) - \mathrm{H}(X \mid Y).$$

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

We use the notation

$$h(p) = -p \log p - (1-p)\log(1-p)$$

for the binary entropy function. We say that X, Y and Z form a *Markov-chain*, denoted by $X \leftrightarrow Y \leftrightarrow Z$, if X and Z are independent given Y, which means that $P_{X|Y=y} = P_{X|Y=y,Z=z}$ for all y, z (,or $P_{Z|Y=y} = P_{Z|X=x,Y=y}$ for all x, y, since the condition is symmetric in X and Z). 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.

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 $P_{\bar{X}\bar{Y}|X=x,Y=y}(\perp, f(x,y)) = 1$ 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 $x = (x_0, \ldots, x_{n-1}) \in \{0,1\}^{k \cdot n}$, and Bob has an input $c \subseteq \{0, \ldots, n-1\}$ 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

$$\mathsf{EQ}_n(x,y) = \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{otherwise .} \end{cases}$$

- 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 [8, 5]. 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 simulatedwith 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. This definition of security follows Definition 7.2.1 from [32], but is adapted to the case of computationally unbounded adversaries and statistical indistinguishability.

Definition 1. *Let π be a* protocol with black-box access to a primitive P_{UV} *that implements a primitive $P_{\bar{X}\bar{Y}|XY}$. $View_A^\pi(x,y)$ and $View_B^\pi(x,y)$ denote the views of the Alice and Bob on input (x,y) defined as $(x,u,m_1,\ldots,m_i,r_A)$ and $(x,v,m_1,\ldots,m_i,r_B)$ respectively where r_A and r_B is the private randomness of the players, m_i represents the i-th message and u,v is the output from P_{UV}. $Output_A^\pi(x,y)$ and $Output_B^\pi(x,y)$ denote the outputs (that are implicit in the views) of Alice and Bob respectively on input (x,y). The protocol is secure in the semi-honest model with an error of at most ε, if there exist two randomized functions S_A and S_B, called the simulators[6], such that for all x and y:*

$$\delta((View_A^\pi(x,y), Output_B^\pi(x,y)), ((\bar{x}, S_A(x,\bar{x})), \bar{y})) \leq \varepsilon,$$
$$\delta((\bar{x}, (\bar{y}, S_B(y,\bar{y}))), (Output_A^\pi(x,y), View_B^\pi(x,y))) \leq \varepsilon,$$

where $\bar{x}, \bar{y}$ are distributed according to $P_{\bar{X}\bar{Y}|X=x,Y=y}$.

2.2 Sufficient Statistics

Intuitively speaking, the *sufficient statistics*[7] of X with respect to Y, denoted $X \searrow Y$, is the part of X that is correlated with Y.

Definition 2. *Let X and Y be random variables, and let $f(x) := P_{Y|X=x}$. The sufficient statistics of X with respect to Y is defined as $X \searrow Y := f(X)$.*

It is easy to show (see for example [30]) that for any P_{XY}, we have $X \leftrightarrow X \searrow Y \leftrightarrow Y$. This immediately implies that any protocol with access to a primitive P_{UV} can be transformed into a protocol with access to $P_{U\searrow V, V\searrow U}$ (without compromising the security) because the players can compute P_{UV} from $P_{U\searrow V, V\searrow U}$ privately. Thus, in the following we only consider primitives P_{UV} where $U = U \searrow V$ and $V = V \searrow U$.

2.3 Common Part

Roughly speaking, the common part $X \wedge Y$ of X and Y is the maximal element of the set of all random variables (i.e., the *finest* random variable) that can be generated both from X and from Y without any error. For example, if $X = (X_0, X_1) \in \{0,1\}^2$ and $Y = (Y_0, Y_1) \in \{0,1\}^2$, and we have $X_0 = Y_0$ and $\Pr[X_1 \neq Y_1] = \varepsilon > 0$, then the common part of X and Y is equivalent to X_0. The common part was first introduced in [31]; in a cryptographic context, it was used in [54].

Definition 3. *Let X and Y be random variables with distribution P_{XY}. Let $\mathcal{X} := \operatorname{supp}(P_X)$ and $\mathcal{Y} := \operatorname{supp}(P_Y)$. Then $X \wedge Y$, the* common part *of X and Y, is constructed in the following way:*

- *Consider the bipartite graph G with vertex set $\mathcal{X} \cup \mathcal{Y}$, and where two vertices $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are connected by an edge if $P_{XY}(x,y) > 0$ holds.*
- *Let $f_X : \mathcal{X} \to 2^{\mathcal{X}\cup\mathcal{Y}}$ be the function that maps a vertex $v \in \mathcal{X}$ of G to the set of vertices in the connected component of G containing v. Let $f_Y : \mathcal{Y} \to 2^{\mathcal{X}\cup\mathcal{Y}}$ be the function that does the same for a vertex $w \in \mathcal{Y}$ of G.*
- *$X \wedge Y :\equiv f_X(X) \equiv f_Y(Y)$.*

[6] We do not require the simulator to be efficient.
[7] In [30], sufficient statistics has been called the *dependent part*.

2.4 Lower Bounds for Secure Function Evaluation

Let a protocol be an ε-secure implementation of a primitive $P_{\bar{X}\bar{Y}|XY}$ in the semi-honest model. Let P_{XY} be the input distribution and let $P_{\bar{X}\bar{Y}}$ be the corresponding output distribution of the ideal primitive, i.e., $P_{\bar{X}\bar{Y}} := P_{XY} P_{\bar{X}\bar{Y}|XY}$, and let M be the whole communication during the execution of the protocol. Then the security of the protocol implies the following lemma that we will use in our proofs.

Lemma 1.

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

Proof. The security of the protocol implies that there exists a randomized function S_B, such that $\delta(P_{XY\bar{Y}S_B(Y,\bar{Y})}, P_{XY\bar{Y}VM}) \leq \varepsilon$. Using Lemma B1 and (B.6), we get

$$\begin{aligned}\mathrm{H}(X \mid VM) &\geq \mathrm{H}(X \mid S_B(Y,\bar{Y})) - \varepsilon \log(|\mathcal{X}|) - h(\varepsilon)\\ &\geq \mathrm{H}(X \mid Y\bar{Y}) - \varepsilon \log(|\mathcal{X}|) - h(\varepsilon)\ .\end{aligned}$$

□

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.

Lemma 2. *For any protocol that is an ε-secure implementation of f in the semi-honest model,*

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

Proof. There exists a randomized function S_A such that $\delta(P_{XMU|Y=y}, P_{XS_A(X)}) \leq \varepsilon$ for all $y \in \mathcal{Y}$. Using the triangle inequality it follows that for any y, y'

$$\delta(P_{XMU|Y=y}, P_{XMU|Y=y'}) \leq 2\varepsilon\ . \tag{2.2}$$

It holds that $X \leftrightarrow UM \leftrightarrow YZ$. Furthermore, we have $\Pr[Z \neq f(X,Y) \mid Y = y] \leq \varepsilon$. Thus, it follows from (B.9) that

$$\mathrm{H}(f(X,y) \mid UM, Y = y) \leq \mathrm{H}(f(X,y) \mid Z, Y = y) \leq \varepsilon \cdot \log|\mathcal{Z}| + h(\varepsilon)\ . \tag{2.3}$$

Together with (2.2) and Lemma B1 this implies that for any y, y'

$$\begin{aligned}\mathrm{H}(f(X,y) \mid UM, Y = y') &\leq 3\varepsilon \log|\mathcal{Z}| + h(\varepsilon) + h(2\varepsilon)\\ &\leq 3(\varepsilon \log|\mathcal{Z}| + h(\varepsilon))\ ,\end{aligned}$$

where the second inequality follows from (B.1). Since X can be calculated from the values $f(X, y_1), \ldots, f(X, y_{|\mathcal{Y}|})$, we get

$$\begin{aligned}
\mathrm{H}(X \mid UM, Y = y) &\leq \mathrm{H}(f(X, y_1), \ldots f(X, y_{|\mathcal{Y}|}) \mid UM, Y = y) \\
&\leq \sum_{y' \in \mathcal{Y}} \mathrm{H}(f(X, y') \mid UM, Y = y) \\
&\leq (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \ .
\end{aligned}$$

□

The following theorem that gives a lower bound on the conditional entropy of P_{UV} can then be obtained from Lemma 2.

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*

$$\mathrm{H}(U \mid V) \geq \max_y \mathrm{H}(X \mid f(X, y)) - (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) - \varepsilon \log |\mathcal{X}| - h(\varepsilon) \ .$$

Proof. Let $y \in \mathcal{Y}$. From Lemma 2 and (B.3) follows that

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

Using (B.3), (B.2) and Lemma B1 , we get

$$\begin{aligned}
\mathrm{H}(X \mid VM, Y = y) &= \mathrm{H}(U \mid VM, Y = y) + \mathrm{H}(X \mid UVM, Y = y) - \mathrm{H}(U \mid XVM, Y = y) \\
&\leq \mathrm{H}(U \mid VM, Y = y) + (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \\
&\leq \mathrm{H}(U \mid V) + (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \ .
\end{aligned}$$

and from Lemma 1, we get

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

The statement follows by maximizing over all y. □

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). Clearly, if f can be computed from a primitive P_{UV} with an error ε in the semi-honest model, then f' can be computed with the same error. Thus, any lower bound for f' then 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*

$$\mathrm{H}(U \mid V) \geq (n - t)k - (3\lceil n/t \rceil - 2)(\varepsilon t k + h(\varepsilon)) - \varepsilon n k - h(\varepsilon) \ .$$

Proof. We can choose subsets $C_i \subseteq \{0, \ldots, n-1\}$, $1 \leq i \leq \lceil n/t \rceil$, of size t such that $\bigcup_{i=1}^{\lceil n/t \rceil} C_i = \{1, \ldots, n\}$, and restrict Bob to choose his input among these sets. It is easy to check that condition (2.1) is satisfied. The statement follows from Theorem 1. □

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

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

Proof. We can restrict the input domains of both players to the same subsets of size 2^k. Condition (2.1) will still be satisfied.[8] Thus, the corollary follows immediately from Theorem 1. □

There exists a secure reduction of EQ_n to EQ_k ([6]): 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[9] of at most $2^{-\kappa}$. Since there exists a circuit to implement EQ_k with k XOR gates and k AND gates, it follows from [33] 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* $\mathrm{H}(U|V) \geq n - 1 - 4n(\varepsilon + h(\varepsilon))$.

Proof. Let $e_i \in \{0,1\}^n$ be the string that has a one at the i-th position and is zero otherwise. Let $\mathcal{S} := \{e_i : \ 1 \leq i \leq n\}$. Then the protocol is an ε-secure implementation of the restriction $\mathsf{IP}_n^{\mathcal{S}}$ of the inner-product function to $\{0,1\}^n \times \mathcal{S}$. Since $\mathsf{IP}_n^{\mathcal{S}}$ satisfies condition (2.1), the statement follows from Theorem 1.

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 [6] 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 (see Appendix B.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

$$\forall x \neq x' \in \mathcal{X} : f(x, y_1) \neq f(x', y_1) \ , \tag{2.4}$$

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

$$\forall x, x' \in \mathcal{X} : f(x, y_2) = f(x', y_2) \ . \tag{2.5}$$

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.

Lemma 3.

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

[8] Note, however, that it is not possible to restrict Bob's input without also restricting the input of Alice as well to the same set.

[9] Note that our security definition is different from the one used in [6].

Proof. Let g_U, g_V be the functions that compute the common part of P_{UV}. As in the proof of Lemma 2 we get for all $y \neq y' \in \mathcal{Y}$ that

$$\delta(P_{XMU|Y=y}, P_{XMU|Y=y'}) \leq 2\varepsilon \ ,$$

which implies that

$$\delta(P_{XMg_U(U)|Y=y}, P_{XMg_U(U)|Y=y'}) \leq 2\varepsilon \ , \tag{2.6}$$

and

$$\delta(P_X P_{Mg_U(U)|Y=y}, P_X P_{Mg_U(U)|Y=y'}) \leq 2\varepsilon \ . \tag{2.7}$$

Because the protocol is secure, there exists a simulator S_B such that

$$\delta(P_{XMV|Y=y_2}, P_{XS_B(y_2,f(X,y_2))}) \leq \varepsilon \ ,$$

From (2.5) follows that $\delta(P_{XMV|Y=y_2}, P_X P_{S_B(y_2,f(X,y_2))}) \leq \varepsilon$. Therefore, using the triangle inequality we get that

$$\begin{aligned}
\delta(P_{XMg_U(U)|Y=y_2}, P_X P_{Mg_U(U)|Y=y_2}) &\leq \delta(P_{XMV|Y=y_2}, P_X P_{MV|Y=y_2}) && (2.8)\\
&\leq \delta(P_{XMV|Y=y_2}, P_X P_{S_B(y_2,f(X,y_2))})\\
&\quad + \delta(P_X P_{S_B(y_2,f(X,y_2))}, P_X P_{MV|Y=y_2})\\
&\leq 2\varepsilon. && (2.9)
\end{aligned}$$

Using the triangle inequality again it follows from (2.6), (2.7) and (2.9) that

$$\begin{aligned}
\delta(P_{XMg_U(U)|Y=y_1}, P_X P_{Mg_U(U)|Y=y_1}) &\leq \delta(P_{XMg_U(U)|Y=y_1}, P_{XMg_U(U)|Y=y_2})\\
&\quad + \delta(P_{XMg_U(U)|Y=y_2}, P_X P_{Mg_U(U)|Y=y_2})\\
&\quad + \delta(P_X P_{Mg_U(U)|Y=y_2}, P_X P_{Mg_U(U)|Y=y_1})\\
&\leq 6\varepsilon \ .
\end{aligned}$$

Using Lemma B1 we get

$$\begin{aligned}
H(f(X,y_1) \mid M, U \wedge V, Y = y_1) &= H(X \mid M, U \wedge V, Y = y_1)\\
&\geq \log|\mathcal{X}| - 6\varepsilon \log|\mathcal{X}| - h(6\varepsilon)\\
&\geq \log|\mathcal{X}| - 6\varepsilon \log|\mathcal{X}| - 6h(\varepsilon) \ .
\end{aligned}$$

□

The following lower bound on the mutual information of P_{UV} can then be obtained from Lemma 3.

Theorem 2. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function that satisfies (2.4) and (2.5). Then for any protocol that implements f from a primitive P_{UV} with an error of at most ε in the semi-honest model*

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

Proof. Let Alice's input X be uniformly distributed and Bob's input be fixed to y_1. Let Z be Bob's output and M the whole communication. Then Lemma 3 implies that

$$H(f(X,y_1) \mid M, U \wedge V) \geq \log|\mathcal{X}| - 6\varepsilon \log|\mathcal{X}| - 6h(\varepsilon) \ . \tag{2.10}$$

Since $\Pr[Z \neq f(X, y_1)] \leq \varepsilon$ and $X \leftrightarrow VM \leftrightarrow Z$, it follows from (B.6) and (B.9) that

$$H(f(X, y_1) \mid VM) \leq H(f(X, y_1) \mid Z) \leq \varepsilon \log |\mathcal{X}| + h(\varepsilon) \ . \tag{2.11}$$

(2.10) and (2.11) imply, using $X \leftrightarrow UM \leftrightarrow ZYV$, (B.8) and (B.4), that

$$\begin{aligned} \mathrm{I}(U; V \mid M, U \wedge V) &\geq \mathrm{I}(f(X, y_1); V \mid M, U \wedge V) \\ &= H(f(X, y_1) \mid M, U \wedge V) - H(f(X, y_1) \mid VM, U \wedge V) \\ &\geq \log |\mathcal{X}| - 7\varepsilon \log |\mathcal{X}| - 7h(\varepsilon) \ . \end{aligned}$$

Let $M^i := (M_1, \ldots, M_i)$, i.e., the sequence of all messages sent until the ith round. Without loss of generality, let us assume that Alice sends the message of the $(i+1)$th round. Since, we have $M^{i+1} \leftrightarrow M^i U \leftrightarrow V$, it follows from (B.7) that

$$I(U; V \mid M^{i+1}, U \wedge V) \leq I(U; V \mid M^i, U \wedge V) \ .$$

Then it follows by induction over all rounds that

$$I(U; V \mid M, U \wedge V) \leq I(U; V \mid U \wedge V) \ .$$

The statement follows. □

Since properties (2.4) and (2.5) 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*

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

Proof. Consider the function that is obtained by setting the first $n - t$ inputs to a fixed value (and choosing the remaining t inputs from $\{0, 1\}^{tk}$). □

We further generalize Theorem 2 to arbitrary functions $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ in Section B.3 in the appendix. 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 $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, which implies Theorem 4.11 from [6].

2.5 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 [57]. 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. We will show that a generalization of this bound also holds for $n > 2$. Note that we can assume that $k = 1$. The resulting bound then also implies a bound for $k > 1$ because one instance of $\binom{n}{1}$-OT^1 can be implemented from one instance of $\binom{n}{1}$-OT^k. Furthermore, we consider implementations of m independent copies of $\binom{n}{1}$-OT^k.

Lemma 4. *Let a protocol having access to P_{UV} be an ε-secure implementation of m independent copies of $\binom{n}{1}$-OT^1 in the semi-honest model. Then*

$$\mathrm{H}(V \mid U) \geq m \log n - m(4 \log n + 7)(\varepsilon + h(\varepsilon)).$$

Proof. Let Alice and Bob choose their inputs $X = (X^1, \ldots, X^m) = ((X_0^1, \ldots, X_{n-1}^1), \ldots, (X_0^m, \ldots, X_{n-1}^m)) \in \{0,1\}^{mn}$ and $C = (C^1, \ldots, C^m) \in \{0, \ldots, n-1\}^m$ uniformly at random. Let $Y = (Y^1, \ldots, Y^m)$ be the output of Bob at the end of the protocol. Let us for the moment look that the jth instance of $\binom{n}{1}$-OT^1, for $j \in \{1, \ldots, m\}$. Let $A_i := X_0^j \oplus X_i^j$ for all $i \in \{1, \ldots, n-1\}$. From the security of the protocol follows that there exist a randomized function $S_B(c, x_c)$ such that for all $a = (a_1, \ldots, a_{n-1}) \in \{0,1\}^{n-1}$,

$$\delta(P_{YCVM|A=a}, P_{X_C C S_B(C, X_C)}) \leq \varepsilon \; .$$

Hence, using the triangle inequality, we get for all a, a' that

$$\begin{aligned} \delta(P_{Y^j C^j VM|A=a}, P_{Y^j C^j VM|A=a'}) &\leq \delta(P_{YCVM|A=a}, P_{YCVM|A=a'}) && (2.12)\\ &\leq 2\varepsilon. && (2.13) \end{aligned}$$

We have $\Pr[Y^j \neq X_C^j \mid A = a] \leq \varepsilon$ for all a. If $A = (0, \ldots, 0)$, we have $X_C^j = X_0^j$. Since $X^j \leftrightarrow VM \leftrightarrow Y^j$, it follows from (B.3) and (B.9) that

$$\begin{aligned} H(Y^j \mid VM, A = (0, \ldots, 0)) &\leq H(Y^j \mid X^j, A = (0, \ldots, 0)) && (2.14)\\ &\leq H(Y^j \mid X_0^j, A = (0, \ldots, 0)) \leq \varepsilon + h(\varepsilon) \; . \end{aligned}$$

Now, let us map C^j to a bit-string of size $\lceil \log n \rceil$, and let C_b be the bth bit of that bit string, where $b \in \{0, \ldots, \lceil \log n \rceil - 1\}$. Let $a^b = (a_1^b, \ldots, a_{n-1}^b)$, where $a_i^b = 1$ if and only if the bth bit of i is 1. Conditioned on $A = a^b$, we have $X_C^j = X_0^j \oplus C_b$. It follows from $X^j \leftrightarrow VM \leftrightarrow Y^j C^j$, (B.3) and (B.9) that

$$H(Y^j \oplus C_b \mid VM, A = a^b) \leq H(Y^j \oplus C_b \mid X_0^j, A = a^b) \leq \varepsilon + h(\varepsilon) \; . \qquad (2.15)$$

From (2.12) and (2.14), we get

$$H(Y^j \mid VMA) \leq \varepsilon + h(\varepsilon) + 2\varepsilon + h(2\varepsilon) \leq 3\varepsilon + 3h(\varepsilon).$$

It follows from (2.12) and (2.15) that for all b

$$H(Y^j \oplus C_b \mid VMA) \leq 3\varepsilon + 3h(\varepsilon) \; .$$

Since (C^j, Y^j) can be calculated from $(Y^j, Y^j \oplus C_0, \ldots, Y^j \oplus C_{\lceil \log n \rceil - 1})$, this implies that

$$H(C^j Y^j \mid VMA) \leq 3(\lceil \log n \rceil + 1)(\varepsilon + h(\varepsilon)) \; .$$

From $A \leftrightarrow VM \leftrightarrow C^j Y^j$, (B.3) and $\lceil \log n \rceil \leq \log n + 1$ follows that

$$\mathrm{H}(C^j \mid VM) \leq 3(\log n + 2)(\varepsilon + h(\varepsilon)).$$

and, therefore,

$$\begin{aligned} \mathrm{H}(C \mid VM) &\leq \sum_{j=1}^{n} \mathrm{H}(C^j \mid VM)\\ &\leq 3m(\log n + 2)(\varepsilon + h(\varepsilon)). \end{aligned}$$

Using (B.3), (B.2) and Lemmas B1 and 1, we get

$$\begin{aligned} m(\log n - \varepsilon \log n) - h(\varepsilon) &\leq \mathrm{H}(C \mid UM) \\ &= \mathrm{H}(V \mid UM) + \mathrm{H}(C \mid UVM) - \mathrm{H}(V \mid CUM) \\ &\leq \mathrm{H}(V \mid UM) + 3m(\log n + 2)(\varepsilon + h(\varepsilon)) \\ &\leq \mathrm{H}(V \mid U) + 3m(\log n + 2)(\varepsilon + h(\varepsilon)) \ . \end{aligned}$$

□

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*

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

Since 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 $\mathrm{H}(V \mid U) = m \log n$, any protocol that implements M instances of $\binom{N}{1}$-OT^K from m instances of $\binom{n}{1}$-OT^k with an error of at most ε needs to fulfill

$$\begin{aligned} m(n-1)k &\geq M(N-1)K - (4N-2)(\varepsilon MK + h(\varepsilon)), \\ mk &\geq MK - 7\varepsilon MK - 7h(\varepsilon), \\ m \log n &\geq M \log N - M(4 \log N + 7)(\varepsilon + h(\varepsilon)) \ . \end{aligned}$$

Hence, we get

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

which is the statement of Corollary 1.

In Appendix B we also derive new bounds for protocols implementing (p)-$\mathsf{RabinOT}^k$ (Theorems B1-B2), and show that our bounds imply bounds for implementations of oblivious linear function evaluation (OLFE, Corollary B1). In Appendix A we show that our bounds on OT and RabinOT in the semi-honest model imply similar bounds in the malicious model.

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 [4, 26, 56, 55] to the statistical case, it is natural to ask whether similar bounds also hold for quantum protocols, i.e., if the bounds presented in [48] 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. Thereto we introduce the following functionality $\mathcal{F}_{\mathtt{MCOM}}^{A \to B, k}$ that can be implemented from $\binom{n}{1}$-OT^k as we will show.

Definition 4 (Multi-Commitment). *The functionality $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ behaves as follows: Upon (the first) input (*`commit`*, b) with $b \in \{0,1\}^k$ from Alice, send* `committed` *to Bob. Upon input (*`open`*,T) with $T \subseteq [k]$ from Alice send (*`open`*, b_T) to Bob. All communication/input/output is classical. We call Alice the sender and Bob the recipient.*

$\binom{2}{1}$-OT^k can be implemented from $m = O(k+\kappa)$ bit commitments with an error of $2^{-\Omega(\kappa)}$ [8, 61, 22]. 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 [22] for a complete description of the protocol.) This protocol implements oblivious transfer that is statistically secure in the quantum *universal composability* model [51]. Obviously the construction remains secure if we replace the commitment scheme with $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$. The following lemma that we prove in Appendix C shows that $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ can be implemented from the oblivious transfer functionality $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ (see [51] for a definition of $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$). Note that we assume as in the proofs of [51] that all communication between the players is over secure channels and we only consider static adversaries.

> **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 5. *There exists a protocol that is statistically secure and universally composable that realizes $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ with an error of $2^{-\kappa/2}$ using κ instances of $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$.*

Since any protocol that is also statistically secure in the classical universal composability model [14] is also secure in the quantum universal composability model [51], we get, together with the proofs from [22, 51], 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[10] commitments can be implemented from shared randomness P_{UV} that is distributed according to (p)-$\mathsf{RabinOT}$ at a rate of $H(U \mid V) = 1 - p$ [53]. 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.

[10] Stand-alone statistically secure commitments based on stateless two-party primitives are universally composable [27].

It has been an open question whether noiseless quantum communication can increase the commitment capacity [53]. 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 [48] 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.

3.3 Preliminaries

We use the notation ρ^{AB} for a state over the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and $\rho^A := \mathrm{tr}_B(\rho^{AB})$. Let d_A be the dimension of $\mathcal{H}_A$ (We assume that all Hilbert spaces are finite-dimensional.). Furthermore, we denote by $\tau^A = \frac{\mathbb{1}^A}{d_A}$ the fully mixed state on $\mathcal{H}_A$. We call a state ρ^{XA} a *cq-state*, if it has the form

$$\rho^{XA} = \sum_{x \in \{0,1\}} p_x \cdot |x\rangle\langle x|^X \otimes \rho_x^A \ .$$

The *statistical distance* between two states ρ and ϕ is defined as

$$\delta(\rho, \phi) := \max_D \big| \Pr[D(\rho) = 1] - \Pr[D(\phi) = 1] \big| \ .$$

where we maximize over all measurements $D(\cdot)$ that take a quantum state as input and output one bit.

We need the *von Neumann entropy*, defined as

$$H(A \mid B)_\rho := H(\rho^{AB}) - H(\rho^B) \ ,$$

where $H(\rho) := \mathrm{tr}(-\rho \log(\rho))$, and the following facts about the von Neumann entropy. First, from the Alicki-Fannes inequality [2] follows that for any state ρ^{AB}, $\delta(\rho^{AB}, \tau^A \otimes \rho^B) \leq \varepsilon$ implies

$$H(A \mid B)_\rho \geq (1 - 4\varepsilon) \cdot \log d_A - 2h(\varepsilon) \ . \tag{3.1}$$

If there exists a measurement on B with outcome X' such that $\Pr[X' \neq X] \leq \varepsilon$, then

$$H(X \mid B)_\rho \leq H(X \mid X') \leq h(\varepsilon) + \varepsilon \cdot k \tag{3.2}$$

for any cq-state ρ^{XB}. Finally, we use the fact that joint entropy of two systems satisfies subadditivity and the triangle inequality

$$H(AB) \leq H(A) + H(B), \tag{3.3}$$
$$H(AB) \geq |H(A) - H(B)|. \tag{3.4}$$

This implies

$$\begin{aligned}
H(A \mid B) - H(A \mid BC) &= H(AB) - H(B) - H(ABC) + H(BC) \\
&\leq H(AB) + H(C) - H(ABC) \\
&\leq H(AB) + H(C) - |H(AB) - H(C)| \\
&\leq 2\min\{H(AB), H(C)\} \\
&\leq 2H(C) \qquad (3.5)
\end{aligned}$$

for any state ρ^{ABC}.

3.4 Oblivious Transfer

A protocol is an ε-secure implementation of OT if for any adversary $\mathcal{A}$ attacking the protocol (real setting), there exists a *simulator* $\mathcal{S}$ 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. This definition implies the following three conditions (see also [29]).

- Correctness: If both players are honest, then in the ideal setting, the receiver always gets $y = x_c$. This implies that in an ε-secure protocol, Bob must output a value Y where
$$\Pr[Y \neq x_c] \leq \varepsilon \; . \qquad (3.6)$$
- Security for Alice: Let now Alice be honest and Bob malicious, and let Alice's input be chosen uniformly at random. In the ideal setting, the simulator must provide OT with a classical input $C' \in \{0,1\}$. He gets back the output Y and then outputs a quantum state that may depend on C' and Y. The output of the simulator together with classical values X_0, X_1 and C' now define the state $\sigma^{X_0X_1BC'}$.
Since $X_{1-C'}$ is random and independent of C' and Y, we must have
$$\sigma^{X_{1-C'}X_{C'}BC'} = \tau^{X_{1-C'}} \otimes \sigma^{X_{C'}BC'} \quad \text{and} \quad \delta(\sigma^{X_0X_1B}, \rho^{X_0X_1B}) \leq \varepsilon \qquad (3.7)$$
where $\rho^{X_0X_1B}$ is the resulting state of the protocol.[11]
- Security for Bob: If Bob is honest and Alice malicious, the simulator outputs a quantum state σ^A that is independent of Bob's input c. Let ρ_c^A be the state that Alice has at the end of the protocol if Bob's input is c. The security definition now requires that $\delta(\sigma^A, \rho_c^A) \leq \varepsilon$ for $c \in \{0,1\}$. By the triangle inequality, we get
$$\delta(\rho_0^A, \rho_1^A) \leq 2\varepsilon \; . \qquad (3.8)$$

Note that the Conditions (3.6), (3.7) and (3.8) are only necessary for the security of a protocol, they do *not* imply that a protocol is secure.

In the following we will give two lower bounds for quantum protocols that implement $\binom{2}{1}\text{-}\mathsf{OT}^k$ using a trusted resource such as trusted randomness distributed to the players or a bit commitment functionality. Our proofs use similar techniques as the impossibility results in [43, 41, 40]. 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

[11] The standard security definition of OT considered here requires Bob's choice bit to be fixed at the end of the protocol. To show that a protocol is insecure, it suffices therefore to show that Bob can still choose after the termination of the protocol if he wants to receive x_0 or x_1. Lo in [40] shows impossibility of OT in a stronger sense, namely that Bob can learn all of Alice's inputs.

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 [43, 41, 40] for details.

We use the following technical lemma that we prove in Appendix C which is also used in [43, 41, 40].

Lemma 6. *For $c \in \{0,1\}$ let the states $|\rho\rangle_c^{ABE}$ be given. If $\delta(\rho_0^A, \rho_1^A) \leq \varepsilon$, then there exist a unitary U^{BE} such that*

$$\delta(|\rho\rangle_0^{ABE}, (\mathbb{1}^A \otimes U^{BE})|\rho\rangle_1^{ABE}) \leq \sqrt{2\varepsilon}\ . \tag{3.9}$$

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.

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*

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

Proof. Let the final state of the protocol be $|\rho\rangle_c^{ABE}$, when both players are honest and Bob has input $c \in \{0,1\}$. If Bob is executing the protocol honestly using input $c = 1$, he must be able to calculate X_1 with an error of at most $1 - \varepsilon$. Since the protocol is ε-secure for Alice, it follows from Lemma 11 in Appendix F that

$$\delta(\rho_1^{X_0 B}, \tau^{X_0} \otimes \rho_1^B) \leq 5\varepsilon\ .$$

Eq. (3.1) implies that

$$H(X_0 \mid B)_{\rho_1} \geq (1 - 20\varepsilon) \cdot k - 2h(5\varepsilon) \geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon)\ .$$

Since the protocol is ε-secure for Bob, we have $\delta(\rho_0^A, \rho_1^A) \leq 2\varepsilon$. From Lemma 6 follows that there exists a unitary U^{BE} such that Bob could transform the state ρ_1 into the state ρ_0' with $\delta(\rho_0, \rho_0') \leq 2\sqrt{\varepsilon}$, if he had access to E. Since in $\rho_0^{X_0 B}$, X_0 can be guessed from ρ_0^B with probability $1 - \varepsilon$, it follows from Lemma 10 in Appendix F that X_0 can be guessed from ρ_1^{BE} with a probability of at least $1 - \varepsilon - 2\sqrt{\varepsilon}$. Using Eq. (3.2), we get

$$\begin{aligned} H(X_0 \mid BE)_{\rho_1} &\leq h(\varepsilon + 2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k \\ &\leq h(\varepsilon) + h(2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k\ . \end{aligned}$$

Hence, using (3.5) the statement follows

$$\begin{aligned} 2H(E)_\psi = 2H(E)_{\rho_1} &\geq H(X_0 \mid B)_{\rho_1} - H(X_0 \mid BE)_{\rho_1} \\ &\geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon) - h(\varepsilon) - h(2\sqrt{\varepsilon}) - (\varepsilon + 2\sqrt{\varepsilon}) \cdot k \\ &= (1 - 21\varepsilon - 2\sqrt{\varepsilon}) \cdot k - 11h(\varepsilon) - 2h(\sqrt{\varepsilon})\ . \end{aligned}$$

□

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 then 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.*

Proof. Let the final state of the protocol be $|\rho\rangle_c^{ABE}$, when both players are honest and Bob has input $c \in \{0, 1\}$. As in the proof of Theorem 5 we get that

$$H(X_0 \mid B)_{\rho_1} \geq (1 - 20\varepsilon) \cdot k - 2h(5\varepsilon) \geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon) .$$

and

$$H(X_0 \mid BE)_{\rho_1} \leq h(\varepsilon) + h(2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k .$$

Let E contain at most n qubits. Then it follows from Eq. (3.5) that

$$H(X_0 \mid SBE)_{\rho_1} \geq H(X_0 \mid SB)_{\rho_1} - 2n .$$

Hence, the statement follows from

$$\begin{aligned} 2n &\geq H(X_0 \mid B)_{\rho_1} - H(X_0 \mid BE)_{\rho_1} \\ &\geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon) - h(\varepsilon) - h(2\sqrt{\varepsilon}) - (\varepsilon + 2\sqrt{\varepsilon}) \cdot k \\ &= (1 - 21\varepsilon - 2\sqrt{\varepsilon}) \cdot k - 11h(\varepsilon) - 2h(\sqrt{\varepsilon}) . \end{aligned}$$

□

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 $\frac{10^{-10}}{m}$ 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 $2^{-\kappa}/36$.*

Proof. We assume that both Alice and Bob commit at most κ times. We will show that there exists a malicious Alice and a malicious Bob such that either Alice can break Bob's security condition or vice versa.

Let $|\rho\rangle_c^{ABE_AE_B}$ be the final state of the protocol when both players are honest and Bob has input $c \in \{0,1\}$. We distinguish two cases. In the first case we assume that an honest Alice could guess c with an advantage of at least $\varepsilon' := 1/18$, if she had access to AE_A, i.e.,

$$\delta(\rho_0^{AE_A}, \rho_1^{AE_A}) \geq \varepsilon' \ . \tag{3.10}$$

We let Bob be honest and let Alice apply the following strategy: She chooses a random subset $\mathcal{T}$ of $[k]$. She executes all commitments in $\mathcal{T}$ honestly, but for all commitments not in $\mathcal{T}$ she sends $|0\rangle$ to E_A and keeps her state in her quantum register. Otherwise, she follows the whole protocol honestly.

During the protocol, Bob may ask Alice to open certain commitments. Let $\mathcal{T}'$ be the set of commitments that Alice has to open. If $\mathcal{T}' = \mathcal{T}$, which happens with probability $2^{-\kappa}$ independent of everything else, then at the end of the protocol the global state is $|\rho\rangle_c$, with the difference that the values normally in E_A are now part of A. Therefore, Alice has an advantage of more than ε' to distinguish $c = 0$ from $c = 1$ in this case, and her total advantage is more than $\varepsilon' \cdot 2^{-\kappa} > 2\varepsilon$, which contradicts condition (3.8).

In the second case, we assume that $\delta(\rho_0^{AE_A}, \rho_1^{AE_A}) < \varepsilon'$. From condition (3.6) follows that honest Bob can guess X_1 with probability $1-\varepsilon$ if $c = 1$. We can apply Lemma 11, which tells us that X_1 should be 5ε-close to uniform with respect to ρ_1^B. To get a contradiction to the security condition (3.7), we can use equation (F.1) (which is implied by Lemma 10 in Appendix F): it suffices to show that Bob can guess the first bit of X_0 with a probability of at least $\frac{1}{2} + 5\varepsilon$.

Let Alice be honest and Bob do the same attack as Alice in the first case, choosing $c = 1$. Again, if Bob guesses the set $\mathcal{T}$ right, which happens with probability $2^{-\kappa}$, all qubits normally in E_B are in B. Then Lemma 6 tells us that there exist a unitary U^{BC_B} such Bob can transform the state ρ_1 into a state ρ_1' where $\delta(\rho_0, \rho_1') \leq \sqrt{2\varepsilon'}$. Bob can guess X_0 with an error of at most ε in ρ_0. Therefore, he can guess X_0 in ρ_1' with an error of at most $\sqrt{2\varepsilon'} + \varepsilon$.

If he fails to guess $\mathcal{T}$, he simply outputs a random bit as guess for the first bit of X_0. Since the probability that he guesses $\mathcal{T}$ correctly is exactly $2^{-\kappa}$, he can guess the first bit of X_0 with probability

$$\begin{aligned}
(1-2^{-\kappa}) \cdot \frac{1}{2} + 2^{-\kappa} \cdot (1 - \varepsilon - \sqrt{2\varepsilon'}) &= \frac{1}{2} + 2^{-\kappa} \cdot \left(\frac{1}{2} - \varepsilon - \sqrt{2\varepsilon'}\right) \\
&> \frac{1}{2} + 2^{-\kappa} \cdot \left(\frac{1}{2} - \varepsilon'/2 - \sqrt{2\varepsilon'}\right) \\
&= \frac{1}{2} + 2^{-\kappa} \cdot \frac{5}{36} = \frac{1}{2} + 5\varepsilon \ .
\end{aligned}$$

$\square$

3.5 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 [22] 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. The proof of the following corollary can be found in Appendix D.5.

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. Alicki, R., Fannes, M.: Continuity of quantum conditional information. Journal of Physics A: Mathematical and General 37(5), L55 (2004)

3. Babai, L., Hayes, T.P.: Near-independence of permutations and an almost sure polynomial bound on the diameter of the symmetric group. SODA '05 (2005)
4. 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)
5. Beaver, D.: Precomputing oblivious transfer. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 97–109. Springer (1995)
6. 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)
7. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM Journal on Computing 17(2), 210–229 (1988)
8. 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)
9. Bouman, N., Fehr, S.: Sampling in a quantum population, and applications. arXiv:0907.4246 (2009)
10. 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)
11. Brassard, G., Crépeau, C., Wolf, S.: Oblivious transfers and privacy amplification. Journal of Cryptology 16(4), 219–237 (2003)
12. Brassard, G., Crépeau, C., Santha, M.: Oblivious transfers and intersecting codes. IEEE Transactions on Information Theory 42(6), 1769–1780 (1996)
13. Cachin, C.: On the foundations of oblivious transfer. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 361–374. Springer (1998)
14. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: FOCS 2001. pp. 136–145 (2001)
15. Chernoff, H.: A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. Annals of Mathematical Statistics 23, 493–507 (1952)
16. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley-Interscience, New York, USA (1991)
17. 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)
18. Crépeau, C.: Equivalence between two flavours of oblivious transfers. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 350–354. Springer (1987)
19. 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)
20. 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)
21. 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)
22. 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)
23. 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)
24. 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)
25. 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)
26. Dodis, Y., Micali, S.: Lower bounds for oblivious transfer reductions. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 42–55. Springer (1999)
27. 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), http://eprint.iacr.org/
28. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Commun. ACM 28(6), 637–647 (1985)
29. Fehr, S., Schaffner, C.: Composing quantum protocols in a classical environment. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 350–367. Springer (2009)
30. Fitzi, M., Wolf, S., Wullschleger, J.: Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In: Advances in Cryptology — CRYPTO '04. Lecture Notes in Computer Science, vol. 3152, pp. 562–578. Springer-Verlag (2004)
31. Gacs, P., Körner, J.: Common information is far less than mutual information. Probl. Contr. Inform. Theory 2, 149–162 (1973)
32. Goldreich, O.: Foundations of Cryptography, vol. II: Basic Applications. Cambridge University Press (2004)
33. 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)

34. Hoeffding, W.: Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association 58(301), 13–30 (1963)
35. 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)
36. Jozsa, R.: Fidelity for mixed quantum states. Journal of Modern Optics 41, 2315–2323 (1994)
37. 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)
38. 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)
39. Kushilevitz, E.: Privacy and communication complexity. In: SFCS '89: Proceedings of the 30th Annual Symposium on Foundations of Computer Science. pp. 416–421. IEEE Computer Society, Washington, DC, USA (1989)
40. Lo, H.K.: Insecurity of quantum secure computations. Physical Review A 56, 1154 (1997)
41. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Physical Review Letters 78, 3410–3413 (1997)
42. Maurer, U.: Information-theoretic cryptography. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 47–64. Springer (1999)
43. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Physical Review Letters 78, 3414–3417 (1997)
44. 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)
45. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press (October 2000)
46. Prabhakaran, M., Rosulek, M.: Cryptographic complexity of multi-party computation problems: Classifications and separations. In: Wagner, D. (ed.) CRYPTO 2008. pp. 262–279 (2008)
47. Rabin, M.O.: How to exchange secrets by oblivious transfer. Tech. Rep. TR-81, Harvard Aiken Computation Laboratory (1981)
48. 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)
49. Savvides, G.: Interactive Hashing and reductions between Oblivious Transfer variants. Ph.D. thesis, McGill University, Montréal (2007)
50. Uhlmann, A.: The transition probability in the state space of *-algebra. Rep. Math. Phys. 9, 273–279 (1976)
51. Unruh, D.: Universally composable quantum multi-party computation. In: EUROCRYPT 2010. LNCS, Springer (June 2010), to appear.
52. Wiesner, S.: Conjugate coding. SIGACT News 15(1), 78–88 (1983)
53. Winter, A., Nascimento, A.C.A., Imai, H.: Commitment capacity of discrete memoryless channels. In: IMA Int. Conf. pp. 35–51 (2003)
54. Wolf, S., Wullschleger, J.: Zero-error information and applications in cryptography. In: Proceedings of 2004 IEEE Information Theory Workshop (ITW '04) (2004)
55. Wolf, S., Wullschleger, J.: New monotones and lower bounds in unconditional two-party computation. IEEE Transactions on Information Theory 54(6), 2792–2797 (2008)
56. 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)
57. Wolf, S., Wullschleger, J.: Oblivious transfer is symmetric. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 222–232. Springer (2006)
58. Wullschleger, J.: Oblivious-transfer amplification. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 555–572. Springer (2007)
59. Wullschleger, J.: Oblivious transfer from weak noisy channels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 332–349 (2009)
60. 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)
61. 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)

A Malicious OT implies Semi-honest OT

In the malicious model the adversary is not required to follow the protocol. Therefore, a protocol that is secure in the malicious model protects against a much bigger set of adversaries. On the other hand, the security definition in the malicious model only implies that for any (also semi-honest) adversary there exists a *malicious* simulator for the ideal primitive, i.e., the simulator is allowed to change his input or output from the ideal primitive. Since this is not allowed in the semi-honest model, security in the malicious model does not imply security in the semi-honest model in general. For implementations of OT[12], however, it has been shown in [46] that this implication *does* hold, because if the adversary is semi-honest, a simulator can only change the input with small probability. Otherwise, he is not able to correctly simulate the input or the output of the protocol. Therefore, any impossibility result for OT in the semi-honest model also implies impossibility in the malicious model.

We will state these results for $\binom{n}{1}$-OT^k and (p)-$\mathsf{RabinOT}^k$ with explicit bounds on the errors.

Lemma A1 *If a protocol implementing $\binom{n}{1}$-OT^k is secure in the malicious model with an error of at most ε, then it is also secure in the semi-honest model with an error of at most $(2n+1)\varepsilon$.*

Proof. From the security of the protocol we know that there exists a (malicious) simulator that simulates the view of honest Alice. If two honest players execute the protocol on input $(x_0, \ldots, x_{n-1})$ and c, then with probability $1-\varepsilon$ the receiver gets $y = x_c$. Thus, the simulator can change the input x_i with probability at most 2ε for all $0 \leq i < n-1$. We construct a new simulator that executes the malicious simulator but never changes the input. This simulation is $(2n+1)\varepsilon$-close to the distribution of the protocol. From the security of the protocol we also know that there exists a (malicious) simulator that simulates the view of honest Bob. If two honest players execute the protocol with uniform input $(X_0, \ldots, X_{n-1})$ and choice bit c, then with probability $1-\varepsilon$ the receiver gets $y = x_c$. If the simulator changes the choice bit c, he does not learn x_c and the simulated y is not equal to x_c with probability at least $1/2$. Therefore, the simulator can change c or the output with probability at most 4ε. As above we can construct a simulator for the semi-honest model with an error of at most 5ε. □

Lemma A2 *If a protocol implementing (p)-$\mathsf{RabinOT}^k$ is secure in the malicious model with an error of at most ε, then it is also secure in the semi-honest model with an error of at most* $\max(\frac{2^{k+1}}{2^k-1}\varepsilon + 2\varepsilon, 2\varepsilon/p)$.

Proof. From the security of the protocol we know that there exists a (malicious) simulator that simulates the view of honest Alice. If two honest players execute the protocol on input x, then with probability at most ε the receiver gets an output $x' \notin \{x, \Delta\}$. Thus, the simulator can change the input x with probability at most $2\varepsilon/p$. From the security of the protocol we also know that there exists a (malicious) simulator that simulates the view of honest Bob. Let the input be chosen uniformly. If the simulator changes the output from Δ to y', then with probability at most $1/2^k$ it holds that $y' = x$. Thus, the simulator may change the output with probability at most $\frac{2^{k+1}}{2^k-1}\varepsilon/(1-p)$ from Δ. Therefore the simulator may change an output $x \neq \Delta$ with probability at most $\frac{2^{k+1}}{2^k-1}\varepsilon/(1-p) + 2\varepsilon$. Otherwise the probability that $x' \notin \{x, \Delta\}$ is greater than 2ε. As in lemma A1 we can now construct semi-honest simulators with an error of at most $\max(\frac{2^{k+1}}{2^k-1}\varepsilon/(1-p) + 2\varepsilon, 2\varepsilon/p)$. □

Note that some of our proofs could easily be adapted to the malicious model to get slightly better bounds than the ones that follow from the combination of the bounds in the semi-honest model and Lemmas A1 and A2.

[12] And any other so-called deviation revealing functionality.

B Lower Bounds for Classical Two-Party Computation

B.1 Information Theory

We will use the following tools from information theory[13] in our proofs. The *conditional Shannon entropy* of X given Y is defined as[14]

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

and the *mutual information* of X and Y given Z as

$$\mathrm{I}(X;Y \mid Z) = \mathrm{H}(X \mid Z) - \mathrm{H}(X \mid YZ) \ .$$

We use the notation

$$h(p) = -p \log p - (1-p) \log(1-p)$$

for the binary entropy function, i.e., $h(p)$ is the Shannon entropy of a binary random variable that takes on one value with probability p and the other with $1-p$. Note that the function $h(p)$ is *concave*, which implies that for any $0 \leq p \leq 1$ and $0 \leq c \leq 1$, we have

$$h(c \cdot p) \geq c \cdot h(p) \ . \tag{B.1}$$

We will need the chain-rule

$$\mathrm{H}(XY \mid Z) = \mathrm{H}(X \mid Z) + \mathrm{H}(Y \mid XZ) \ , \tag{B.2}$$

and the following monotonicity inequalities

$$\mathrm{H}(XY \mid Z) \geq \mathrm{H}(X \mid Z) \geq \mathrm{H}(X \mid YZ) \ , \tag{B.3}$$

$$\mathrm{I}(WX;Y \mid Z) \geq \mathrm{I}(X;Y \mid Z) \ . \tag{B.4}$$

We will also need

$$\mathrm{H}(X \mid YZ) = \sum_z P_Z(z) \cdot H(X \mid Y, Z=z) \ . \tag{B.5}$$

$X \leftrightarrow Y \leftrightarrow Z$ implies that

$$H(X \mid Z) \geq H(X \mid YZ) = H(X \mid Y) \ . \tag{B.6}$$

It is easy to show that if $W \leftrightarrow XZ \leftrightarrow Y$, then

$$I(X;Y \mid ZW) \leq I(X;Y \mid Z) \text{ and} \tag{B.7}$$

$$I(W;Y \mid Z) \leq I(X;Y \mid Z) \ . \tag{B.8}$$

We will need the following lemma.

Lemma B1 *Let (X,Y), and $(\hat{X},\hat{Y})$ be random variables distributed according to P_{XY} and $P_{\hat{X}\hat{Y}}$, and let $\delta(P_{XY}, P_{\hat{X}\hat{Y}}) \leq \epsilon$. Then*

$$\mathrm{H}(\hat{X}|\hat{Y}) \geq \mathrm{H}(X|Y) - \epsilon \log(|\mathcal{X}|) - \mathrm{h}(\epsilon).$$

[13] See [16] for a good introduction into information theory.
[14] All logarithms are binary, and we use the convention that $0 \cdot \log 0 = 0$.

Proof. There exist random variables A, B such that $P_{XY|A=0} = P_{\hat{X}\hat{Y}|B=0}$ and $\Pr[A = 0] = \Pr[B = 0] = 1-\epsilon$. Thus, using the monotonicity of the entropy and the fact that $\mathrm{H}(X) \leq \log(|\mathcal{X}|)$ we get that

$$\begin{aligned}
\mathrm{H}(\hat{X}|\hat{Y}) &\geq (1-\varepsilon)\,\mathrm{H}(\hat{X}|\hat{Y}A=0) + \varepsilon\,\mathrm{H}(\hat{X}|\hat{Y}A=1) \\
&\geq (1-\epsilon)\,\mathrm{H}(X|YB=0) \\
&= \mathrm{H}(X|YB) - \epsilon\,\mathrm{H}(X|YB=1) \\
&= \mathrm{H}(XB|Y) - H(B|Y) - \epsilon\,\mathrm{H}(X|YB=1) \\
&\geq \mathrm{H}(X|Y) - \mathrm{h}(\epsilon) - \epsilon\log(|\mathcal{X}|).
\end{aligned}$$

□

Lemma (B1) implies Fano's inequality: For all $X, \hat{X} \in \mathcal{X}$ with $\Pr[X \neq \hat{X}] \leq \varepsilon$, we have

$$H(X \mid \hat{X}) \leq \varepsilon \cdot \log|\mathcal{X}| + h(\varepsilon)\ . \tag{B.9}$$

B.2 Inner Product from OT

Proposition 1. *There is a protocol that computes the function IP_n in the semi-honest model perfectly secure with n calls to $\binom{2}{1}$-OT^1.*

Proof. Consider the following protocol from [6] that is adapted to $\binom{2}{1}$-OT^1: Alice chooses $r = (r_1, \ldots, r_{n-1})$ uniformly at random and sets $r_n := \oplus_{i=1}^{n-1}$. Then, for each i Alice inputs $a_{i,0} := r_i$ and $a_{i,1} := x_i \oplus r_i$ to the OT and Bob inputs y_i. Bob receives z_i from the OTs and outputs $\oplus_{i=1}^n z_i$. Since $\oplus_{i=1}^n z_i = \oplus_{i=1}^n (x_i y_i \oplus r_i) = (\oplus_{i=1}^n x_i y_i) \oplus (\oplus_{i=1}^n r_i) = \oplus_{i=1}^n x_i y_i = \mathsf{IP}_n(x, y)$, the protocol is correct. The security for Alice follows from the fact that $z_1, \ldots, z_n$ is a uniformly random string subject to $\oplus_{i=1}^n z_i = \mathsf{IP}_n(x, y)$.

B.3 Generalization of Theorem 2

Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function. Then we represent f by a $|\mathcal{X}| \times |\mathcal{Y}|$- matrix M_f with $M_f(x, y) = f(x, y)$. In order to generalize Theorem 2 we define the following relation on the rows of a matrix M_f.

Definition 5 ([39]). *The relation $\sim$ on the rows of a matrix M_f is defined as follows: $x, x' \in \mathcal{X}$ satisfy $x \sim x'$ if there exists $y \in \mathcal{Y}$ such that $M_f(x, y) = M_f(x', y)$. The equivalence relation $\equiv_r$ on the rows of M_f is defined as the transitive closure of $\sim$, i.e., $x, x' \in \mathcal{X}$ satisfy $x \equiv_r x'$ if there exist $x_1, \ldots, x_\ell$ such that $x \sim x_1 \sim \cdots \sim x_\ell \sim x'$. Furthermore, we say that $x, x' \in \mathcal{X}$ are c-equivalent with respect to $\equiv_r$ with $c \in \mathbb{N}$, if there exist $x_1, \ldots, x_\ell$ such that $x \sim x_1 \sim \cdots \sim x_\ell \sim x'$ and $\ell \leq c$.*

Lemma 7. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function such that all rows of M_f are c-equivalent with respect to $\equiv_r$. Let X and Y be chosen uniformly at random. Then for all $x, x' \in \mathcal{X}$ and all $y \in \mathcal{Y}$*

$$\delta(P_{M|X=x,Y=y}, P_{M|X=x',Y=y}) \leq 2(1 + 2(c+1))\varepsilon = (6 + 4c)\varepsilon.$$

Proof. As in the proof of Lemma 2 we get for all $y \neq y' \in \mathcal{Y}$ that

$$\delta(P_{M|X=x,Y=y}, P_{M|X=x,Y=y'}) \leq 2\varepsilon\ ,$$

From the security of the protocol there exists a simulator S_B such that for all x, y

$$\delta(P_{M|X=x,Y=y}, P_{S_B(y,f(x,y))}) \leq \varepsilon.$$

Thus, for all x, x', y with $f(x, y) = f(x', y)$, we have

$$\delta(P_{M|X=x,Y=y}, P_{M|X=x',Y=y}) \leq 2\varepsilon.$$

Since all all rows of M_f are c-equivalent with respect to $\equiv_r$, we get

$$\delta(P_{M|X=x,Y=y}, P_{M|X=x',Y=y}) \leq 2(1 + 2(c+1))\varepsilon = (6 + 4c)\varepsilon.$$

□

Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function such that there exists $\bar{y} \in \mathcal{Y}$ with $|\{f(x, \bar{y}) : \ x \in \mathcal{X}\}| \geq t$ and all rows of M_f are c-equivalent with respect to $\equiv_r$. There exists $\mathcal{X}' \subseteq \mathcal{X}$ with $|\mathcal{X}'| = t$ and $f(x, \bar{y}) \neq f(x', \bar{y})$ for all $x \neq x' \in \mathcal{X}'$. Let Alice's input X be uniformly distributed over $\mathcal{X}'$. Let Bob's input be fixed to $\bar{y}$. Let M be the whole communication. Then the following lemma holds for any ε-secure implementation of f.

Lemma 8.

$$H(f(X, \bar{y}) \mid M) \geq \log(t) - (6 + 4c)\varepsilon \log(t) - (6 + 4c)h(\varepsilon).$$

Proof. From Lemma 7, we have

$$\delta(P_{M|X=x}, P_{M|X=x'}) \leq 2(1 + 2(c+1))\varepsilon = (6 + 4c)\varepsilon.$$

This implies that

$$\delta(P_{XM}, P_X P_M) \leq (6 + 4c)\varepsilon.$$

Using Lemma B1 we get

$$\begin{aligned} H(f(X, \bar{y}) \mid M) &= H(X \mid M) \\ &\geq \log(t) - (6 + 4c)\varepsilon \log(t) - (6 + 4c)h(\varepsilon). \end{aligned}$$

□

The following theorem follows from Lemma 8 using the proof of Theorem 2.

Theorem 9. *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function such that all rows of M_f are c-equivalent with respect to $\equiv_r$ and such that there exists $\bar{y} \in \mathcal{Y}$ with $|\{f(x, \bar{y}) : \ x \in \mathcal{X}\}| \geq t$. Then for any protocol that implements f with an error of at most ε in the semi-honest model from a primitive P_{UV}*

$$\mathrm{I}(U; V) \geq \log(t) - (7 + 4c)\varepsilon \log(t) - (7 + 4c)h(\varepsilon).$$

B.4 Lower Bounds for Protocols implementing RabinOT

Let a protocol P having access to P_{UV} be an ε-secure implementation of (p)-$\mathsf{RabinOT}^k$ in the semi-honest model. In the following we assume $0 \leq \varepsilon < \min(p, 1-p)$. Let $X \in \{0,1\}^k$ be the uniformly distributed input of Alice and $Y \in \{0,1\}^k \cup \Delta$ the output of Bob. Let M be the whole communication during the execution of the protocol. Let $P_{\bar{Y}|X}$ be the conditional distribution of an ideal RabinOT and $P_{\bar{Y}X} := P_X P_{\bar{Y}|X}$. Then the following two lemmas hold for any protocol.

Lemma B2

$$\mathrm{H}(X \mid UM) \leq \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon}.$$

Proof. From the security of the protocol follows that there exists a simulator $S_A(x)$ such that $\delta(P_{XS_A(X)\bar{Y}}, P_{XUMY}) \leq \varepsilon$. Let $D = 1$ if $Y \neq \Delta$ and 0 otherwise, and $\bar{D} = 1$ if $\bar{Y} \neq \Delta$ and 0 otherwise. We have $P_{XS_A(X)\bar{D}} = P_{XS_A(X)} P_{\bar{D}}$. From Lemma F2 follows that

$$\delta(P_{XMU|D=0}, P_{XMU|D=1}) \leq \frac{2\varepsilon}{\min(p, 1-p) - \varepsilon} \ . \tag{B.10}$$

Since $\delta(P_{XY}, P_{X\bar{Y}}) \leq \varepsilon$, we have

$$\Pr[Y \neq X \mid D = 1] \leq \frac{\varepsilon}{\Pr[D = 1]} \leq \frac{\varepsilon}{p - \varepsilon} \ .$$

We have $X \leftrightarrow UM \leftrightarrow Y$. Thus, it follows from (B.6) and (B.9) that

$$\begin{aligned} \mathrm{H}(X \mid UM, Y \neq \Delta) &\leq \mathrm{H}(X \mid Y, Y \neq \Delta) \\ &\leq \frac{\varepsilon k}{p - \varepsilon} + h\left(\frac{\varepsilon}{p - \varepsilon}\right) \leq \frac{\varepsilon k + h(\varepsilon)}{p - \varepsilon} \ . \end{aligned} \tag{B.11}$$

Together (B.10) and (B.11) imply that

$$\begin{aligned} \mathrm{H}(X \mid UM, Y = \Delta) &\leq \frac{\varepsilon k + h(\varepsilon)}{p - \varepsilon} + \frac{2(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \\ &\leq \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \ , \end{aligned} \tag{B.12}$$

and (B.5), (B.11) and (B.12) imply that

$$\mathrm{H}(X \mid UMD) \leq \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \ .$$

Using $X \leftrightarrow UM \leftrightarrow YD$ and (B.6) we get that $\mathrm{H}(X \mid UM) = \mathrm{H}(X \mid UMD)$. The statement follows. □

Lemma B3

$$\mathrm{H}(X \mid VM) \leq (1-p)k + \varepsilon k + h(\varepsilon) \ .$$

Proof. There exists a simulator $S_B(\bar{y})$ such that $\delta(P_{X\bar{Y}S_B(\bar{Y})}, P_{XYVM}) \leq \varepsilon$. Since $X \leftrightarrow VM \leftrightarrow Y$, it follows from (B.6) and Lemma B1 that

$$\begin{aligned} \mathrm{H}(X \mid VM) &\leq \mathrm{H}(X \mid Y) \\ &\leq \mathrm{H}(X \mid \bar{Y}) + \varepsilon k + h(\varepsilon) \\ &= (1-p) \cdot k + \varepsilon k + h(\varepsilon) \ . \end{aligned}$$

□

Theorem B1 *Let a protocol having access to P_{UV} be an ε-secure implementation of (p)-$\mathsf{RabinOT}^k$ in the semi-honest model. Then*

$$\mathrm{H}(U \mid V) \geq (1-p)k - \frac{4(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \ .$$

Proof. From Lemma B2 and (B.3)

$$\mathrm{H}(X \mid UVM) \le \mathrm{H}(X \mid UM) \le \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \,.$$

Using Lemmas B1 and 1, (B.3) and (B.2) we get

$$\begin{aligned} m(1-p)k - \varepsilon k - h(\varepsilon) &= \mathrm{H}(X \mid \bar{Y}) - \varepsilon k - h(\varepsilon) \\ &\le \mathrm{H}(X \mid VM) \\ &= \mathrm{H}(U \mid VM) + \mathrm{H}(X \mid UVM) - \mathrm{H}(U \mid XVM) \\ &\le \mathrm{H}(U \mid VM) + \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \\ &\le \mathrm{H}(U \mid V) + \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \,. \end{aligned}$$

The statement follows now from $1/(\min(p, 1-p) - \varepsilon) \ge 1$. □

Lemma B4

$$H(X \mid M) \ge k - \frac{5(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} \,.$$

Proof. Let D be defined as before. Since the protocol is secure, there exists a simulator $S_B(\bar{y})$ such that $\delta(P_{XYMV}, P_{X\bar{Y}M_BV_B}) \le \varepsilon$, where $(M_B, V_B) := S_B(\bar{Y})$. There also exists a simulator $S_A(x)$ such that $\delta(P_{X\bar{Y}M_AU_A}, P_{XYMU}) \le \varepsilon$, where $(M_A, U_A) := S_A(X)$. Let $\bar{D} = 1$ if $\bar{Y} \ne \varDelta$ and 0 otherwise. We have $P_{XM_A\bar{D}} = P_{XM_A}P_{\bar{D}}$. We have

$$\delta(P_{X\bar{Y}M_A}, P_{X\bar{Y}M_B}) \le 2\varepsilon$$

since $\delta(P_{X\bar{Y}M_A}, P_{XYM}) \le \varepsilon$ and $\delta(P_{X\bar{Y}M_B}, P_{XYM}) \le \varepsilon$. Together with Lemma F2 it follows that

$$\delta(P_{XM_B|\bar{D}=0}, P_{XM_B|\bar{D}=1}) \le \frac{4\varepsilon}{\min(p, 1-p) - 2\varepsilon} \,.$$

Since $H(X \mid M_B, \bar{Y} = \varDelta) = k$, together with Lemma B1 this implies

$$H(X \mid M_B, \bar{Y} \ne \varDelta) \ge k - \frac{4(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} \,.$$

From (B.5) follows

$$H(X \mid M_B\bar{D}) \ge k - \frac{4(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} \,.$$

Therefore, using Lemma B1 again,

$$\begin{aligned} H(X \mid M) &\ge H(X \mid MD) \\ &\ge k - \varepsilon k - h(\varepsilon) - \frac{4(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} \,. \end{aligned}$$

The statement follows now from $1/(\min(p, 1-p) - 2\varepsilon) \ge 1$. □

Theorem B2 *Let a protocol having access to P_{UV} be an ε-secure implementation of (p)-$\mathsf{RabinOT}^k$ in the semi-honest model. Then*

$$\mathrm{I}(U;V) \geq pk - \frac{6(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} \ .$$

Proof. Let Alice input X be uniformly distributed. Let Y be Bob's outputs and M be the whole communication. Then Lemma B4 implies that

$$\mathrm{H}(X \mid M) \geq k - \frac{5(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon},$$

and from Lemma B3 we have

$$\mathrm{H}(X \mid VM) \leq (1-p)k + \varepsilon k + h(\varepsilon).$$

Together this implies

$$\begin{aligned}
\mathrm{I}(U;V \mid M) &\geq \mathrm{I}(X;V \mid M) \\
&= \mathrm{H}(X \mid M) - \mathrm{H}(X \mid VM) \\
&\geq pk - \varepsilon k - h(\varepsilon) - \frac{5(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} \ .
\end{aligned}$$

Let $M^i := (M_1, \ldots, M_i)$, i.e., the sequence of all messages sent until the ith round. Without loss of generality, let us assume that Alice sends the message of the $(i+1)$th round. Since, we have $M^{i+1} \leftrightarrow M^i U \leftrightarrow V$, it follows from (B.7) that

$$I(U;V \mid M^{i+1}) \leq I(U;V \mid M^i) \ .$$

Then it follows by induction over all rounds that

$$I(U;V \mid M) \leq I(U;V) \ .$$

The statement follows now from $1/(\min(p, 1-p) - 2\varepsilon) \geq 1$. □

Note that as in the case of $\binom{n}{1}$-OT^k, the statement of these theorems can be generalized to m independent instances. We leave this to the full version [**severin: ?**] of this work.

B.5 Lower Bounds for Protocols implementing OLFE

We will now show that Theorem 3 also implies bounds for oblivious linear function evaluation ((q)-OLFE), which is defined as follows:

– For any finite field $GF(q)$ of size q, (q)-OLFE is the primitive where Alice has an input $a, b \in GF(q)$ and Bob has an input $c \in GF(q)$. Bob receives $d = a + b \cdot c \in GF(q)$.

Our lower bound is a simple consequence of the fact that (q)-OLFE can be used to implement $\binom{2}{1}$-$\mathsf{OT}^{\log(q)}$.

Corollary B1 *Let a protocol having access to P_{UV} be an ε-secure implementation of m instances of (q)-OLFE in the semi-honest model. Then*

$$\mathrm{H}(U \mid V) \geq m \log q - 5(\varepsilon m \log q + h(\varepsilon)) \ , \tag{B.13}$$
$$\mathrm{H}(V \mid U) \geq m \log q - 5(\varepsilon m \log q + h(\varepsilon)) \ , \tag{B.14}$$
$$\mathrm{I}(U;V) \geq m \log q - 7(\varepsilon m \log q + h(\varepsilon)) \ . \tag{B.15}$$

Proof. First of all, note that $\binom{2}{1}$-OT^k can easily be generalized to the case where $x_0, x_1 \in \{0, \ldots, q^m - 1\}$, for any $q, m > 0$. Theorem 1 and Theorem 2 easily generalize to this variant of oblivious transfer. There exists a simple reduction from this oblivious transfer to m instances of (q)-OLFE: Alice gets input $x = (x_0, x_1) \in \{0, \ldots, q^m - 1\}^2$. We can write $x_i = (x_i^0, \ldots, x_i^{m-1})$, where $x_i^j \in \{0, \ldots, q-1\}$. Alice sends $a^j := x_0^j$ and $b^j := x_1^j - x_0^j$ to the jth instance of (q)-OLFE. Bob sends $c \in \{0,1\}$ to all instances of (q)-OLFE. Bob receives $y^j \in GF(q)$ and outputs $y := (y^0, \ldots, y^{m-1})$. We have $y = x_c$, since for $c = 0$, $y^j = x_0^j + (x_1^j - x_0^j) \cdot 0 = x_0^j$ and for $c = 1$, $y^j = x_0^j + (x_1^j - x_0^j) \cdot 1 = x_1^j$. It is easy to see that the protocol is also secure. Therefore, a violation of (B.13) or (B.15) would imply a violation of Theorem 1 or Theorem 2. Furthermore, it has been shown in [57] that (q)-OLFE is symmetric. Hence, a violation of (B.14) would imply a violation of (B.13). $\square$

From Corollary B1 follows immediately that

Corollary B2 *Let a protocol P having access to m instances of (q)-OLFE be an ε-secure implementation of $m+1$ instances of (q)-OLFE in the semi-honest model. Then*

$$\varepsilon \cdot m \log q + h(\varepsilon) \geq \frac{\log q}{5} .$$

C Quantum Reductions

Lemma 5. The protocol of Section 3.1 statistically UC-realizes $\mathcal{F}_{\texttt{MCOM}}^{A\to B,k}$ with an error of $2^{-\kappa/2}$ using κ instances of $\mathcal{F}_{\texttt{OT}}^{A\to B,k}$.

Proof. Note that we assume that all communication between the players is over secure channels and we only consider static adversaries. The statement is obviously true in the case of no corrupted parties and in the case of both the sender and the recipient being corrupted. We construct for any adversary $\mathcal{A}$ a simulator $\mathcal{S}$ that runs a copy of $\mathcal{A}$ as a black-box: In the case where the sender is corrupted, the simulator $\mathcal{S}$ can extract the commitment b from the input to $\mathcal{F}_{\texttt{OT}}^{A\to B,k}$ and the messages except with probability $2^{-\kappa/2}$ as follows: Define the extracted commitment as $b_i := \mathrm{maj}(m_i^1 \oplus x_{0,i}^1 \oplus x_{1,i}^1, \ldots, m_i^\kappa \oplus x_{0,i}^\kappa \oplus x_{1,i}^\kappa)$ for all $1 \leq i \leq k$ where maj denotes the majority function. Let T be a (non-empty) subset of $[k]$ and let $\tilde{b} \in \{0,1\}^k$ such that $\tilde{b}|_T \neq b|_T$. Then an honest recipient accepts $\tilde{b}|_T$ together with T in `Open` with probability at most $2^{-\kappa/2}$ as follows: There must exist $j \in T$ such that $b_j \neq \tilde{b}_j$. Then the sender needs to change either $x_{0,j}^i$ or $x_{1,j}^i$ for at least $\kappa/2$ indices i. Thus, the simulator extracts the bit b in the commit phase as specified before and gives $(\texttt{commit}, b)$ to $\mathcal{F}_{\texttt{MCOM}}^{A\to B,k}$. Upon getting $(\tilde{b}, T)$ from the adversary, the simulator gives $(\texttt{open}, T)$ to $\mathcal{F}_{\texttt{MCOM}}^{A\to B,k}$, if $\tilde{b}|_T = b|_T$, otherwise it stops. Therefore, any environment can distinguish the simulation and the real execution with an advantage of at most $2^{-\kappa/2}$. In the case where the recipient is corrupted, the simulator $\mathcal{S}$, upon getting the message `committed` from $\mathcal{F}_{\texttt{MCOM}}^{A\to B,k}$ and the choice bits c^i, chooses the outputs y^i from $\mathcal{F}_{\texttt{OT}}^{A\to B,k}$ and the messages m^i uniformly and independently at random for all i. In the open phase the simulator $\mathcal{S}$ gets (T, b_T) and simulates the messages of an honest sender by setting $x_{1-c^i}^i|_T := m^i|_T \oplus y^i|_T \oplus b|_T$ and $x_{c^i}^i|_T := y^i|_T$ for all i. This simulation is perfectly indistinguishable from the real execution. $\square$

D Lower Bounds for Quantum Protocols

D.1 Proof of Lemma 6

The *fidelity* between ρ and ϕ is defined as

$$F(\rho, \sigma) := \operatorname{tr} \sqrt{\sqrt{\phi}\rho\sqrt{\phi}} .$$

The following lemma follows from Uhlmann's theorem [50, 36].

Lemma D1 *For any two pure states $|\rho\rangle^{AB}$ and $|\phi\rangle^{AB}$ there exists a unitary U^B, such that*

$$F(|\rho^{AB}\rangle, (\mathbb{1}^A \otimes U^B)|\phi^{AB}\rangle) = F(\rho^A, \phi^A) .$$

We say that ρ is ε-close to ϕ if $\delta(\rho, \phi) \leq \varepsilon$. It can be shown (see for example [45]) that

$$\delta(\rho, \phi) = \frac{1}{2}\|\rho - \phi\|_1 = \frac{1}{2} \operatorname{tr} \sqrt{(\rho - \phi)^\dagger(\rho - \phi)} .$$

F and δ are related by

$$1 - F(\rho, \phi) \leq \delta(\rho, \phi) \leq \sqrt{1 - F(\rho, \phi)^2}$$

and

$$1 - \delta(\rho, \phi) \leq F(\rho, \phi) \leq \sqrt{1 - \delta(\rho, \phi)^2} .$$

Lemma 6. For $c \in \{0, 1\}$ the states $|\rho\rangle_c^{ABC}$ be given. If $\delta(\rho_0^A, \rho_1^A) \leq \varepsilon$, then there exist a unitary U^{BC} such that

$$\delta(|\rho\rangle_0^{ABC}, (\mathbb{1}^A \otimes U^{BC})|\rho\rangle_1^{ABC}) \leq \sqrt{2\varepsilon} . \tag{D.1}$$

Proof. $\delta(\rho_0^A, \rho_1^A) \leq \varepsilon$ implies that $F(\rho_0^A, \rho_1^A) \geq 1 - \varepsilon$. We can apply Lemma D1, which tells us that there exists a unitary U^{BC}, such that

$$F(|\rho\rangle_0^{ABC}, (\mathbb{1}^A \otimes U^{BC})|\rho\rangle_1^{ABC}) \geq 1 - \varepsilon .$$

It follows that

$$\sqrt{1 - \delta^2(|\rho\rangle_0^{ABC}, (\mathbb{1}^A \otimes U^{BC})|\rho\rangle_1^{ABC})} \geq 1 - \varepsilon$$

and hence,

$$\delta(|\rho\rangle_0^{ABC}, (\mathbb{1}^A \otimes U^{BC})|\rho\rangle_1^{ABC} \leq \sqrt{1 - (1 - \varepsilon)^2} \leq \sqrt{2\varepsilon} .$$

□

D.2 Proof of Corollary 10

Corollary 10. Any (quantum) protocol that implements $m+1$ instances of $\binom{2}{1}$-OT^1 from m instances of $\binom{2}{1}$-OT^1 must have an error of at least $\frac{5 \cdot 10^{-6}}{m}$.

Proof. Let us assume that there exists a protocol that implements $m+1$ instances of $\binom{2}{1}$-OT^1 with an error of ε. We can apply this protocol iteratively, to implement $8m$ instances of $\binom{2}{1}$-OT^1 with an error of $7m\varepsilon$. There exists a trivial protocol that implements $\binom{n}{1}$-OT^{8m} from $8m$ instances of $\binom{n}{1}$-OT^1: Bob simply inputs always the same choice bit. From Corollary 9 follows that for any reduction of $\binom{2}{1}$-OT^{8m} to m instances of $\binom{2}{1}$-OT^1 with an error of at most ε', we have

$$184\sqrt{\varepsilon'} + 13 \cdot h(\sqrt{\varepsilon'})/m \geq 2.$$

Note that this bound also holds when Bob chooses his inputs in the reduction above honestly. This implies that $\varepsilon' \geq 4 \cdot 10^{-5}$ and, therefore, $\varepsilon \geq \frac{5 \cdot 10^{-6}}{m}$. □

D.3 Proof of Corollary 11

Corollary 11. Any (quantum) protocol that implements $m+1$ bit commitments out of m commitments must have an error of at least $\frac{1}{5800 \cdot 28 \cdot (4m+50058)}$ for any $m > 0$.

Proof. We assume that there exists a protocol that implements $m+1$ bit commitments out of m with an error of ε. We can apply this protocol iteratively, to implement $n := 28 \cdot (4m + 50058)$ bit commitments with an error of at most $n\varepsilon$. Then, we can apply the protocol from [8] to implement $\binom{2}{1}$-OT^k. Using the analysis from [9] we get an error of at most

$$\frac{1}{2} 2^{-\frac{1}{2}((1/4 - \bar{\varepsilon}/2 - h(\delta))(n-\kappa)-k)} + \sqrt{6}\exp(-\delta^2 \kappa/100) + 2\exp(-2\bar{\varepsilon}^2(n-\kappa)) \ .$$

We choose $\kappa := 140000$, $\delta := 0.026$, $\bar{\varepsilon} := 0.07$ and $k := 4m + 28$. Since $(1/4 - \bar{\varepsilon}/2 - h(\delta)) \geq 1/28$ we get

$$(1/4 - \varepsilon/2 - h(\delta))(n - \kappa) - k \geq \frac{n}{28} - \frac{\kappa}{28} - k = 30 \ .$$

So the error of the last step is at most

$$\sqrt{6}\exp(-\delta^2\kappa/100) + 2\exp(-2\bar{\varepsilon}^2(n-\kappa)) + \frac{1}{2} \cdot 2^{-15} \leq 0.0003$$

and the total error is at most

$$\varepsilon' := 28 \cdot (4m + 50058)\varepsilon + 0.0003 \ .$$

But any quantum reduction of $\binom{2}{1}$-OT^{4m+28} to m commitments must have an error of at least 1/2116, since otherwise we would have

$$(1 - 23\sqrt{\varepsilon'})(4m + 28)/2 - 7h(\sqrt{\varepsilon'}) > \frac{1}{4}(4m + 28) - 7 \geq m \ ,$$

which contradicts Theorem 6. It follows that

$$n\varepsilon + 0.0003 \geq 1/2116$$

or

$$\varepsilon \geq \frac{1/2116 - 0.0003}{n} \geq \frac{1}{5800 \cdot n} = \frac{1}{5800 \cdot 28 \cdot (4m + 50058)} \ .$$

□

D.4 Proof of Theorem 8

We now give a formal statement for the only part that needs to be modified in the security proof of [22], which is the last part of the proof of Lemma 4.3. We need the following sampling lemma.

Lemma 9. *Let $\alpha \in [0, \frac{1}{2}]$. Let us take a bit-strings $y = (y_1, \dots y_m)$ of length $m := b\kappa$, that we group into κ blocks of size b. Let $\mathcal{T}^*$ be a random subset of $[\kappa]$ of size $\alpha\kappa$, $\mathcal{T}$ the corresponding set of bits in $[m]$ and $\bar{\mathcal{T}}$ the complement of $\mathcal{T}$. Let $\mathcal{T}'$ be a random subset of $\mathcal{T}$, where every element is chosen to be in $\mathcal{T}'$ with probability $\frac{1}{2}$, independent of everything else. With $\alpha' := (1/2 - \varepsilon)\alpha$ we have for any $\varepsilon > 0$*

$$\Pr\left[\frac{1}{|\mathcal{T}'|}\sum_{i \in T'} y_i \leq \frac{1}{(1-\alpha)m}\sum_{i \in \bar{\mathcal{T}}} y_i - 2\varepsilon\right] \leq 3e^{-\alpha'\kappa\varepsilon^2/2} \ .$$

In the last part of Lemma 4.3 in [22], it is stated that

$$\delta(\rho_{TestAE}, \tilde{\rho}_{TestAE}) \leq \sum_{test} P_{Test}(test)|\varepsilon_{test}^{\perp}|^2 = \Pr[X \notin B_{test}] \ ,$$

where $B_{test} = \{x \in \{0,1\}^m | r_H(x|_{\bar{T}}, \hat{x}|_{\bar{T}}) \leq r_H(x|_{T'}, \hat{x}|_{T'}) + \varepsilon\}$ and $r_H(x, x')$ is the hamming distance between x and x', divided by their length. If we choose $y := x \oplus \hat{x}$, Lemma 9 implies that

$$\Pr[x \notin B_{test}] \leq 3e^{-\alpha'\kappa\varepsilon^2/8} \leq \left(2e^{-\alpha'\kappa\varepsilon^2/16}\right)^2 .$$

Therefore, ρ_{TestAE} and $\tilde{\rho}_{TestAE}$ are still $2^{-\Omega(\kappa)}$-close to each other. Everything else in the proof in [22] remains the same. Therefore, we get

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 $\kappa b = O(k + \log 1/\varepsilon)$.

D.5 Proof of Corollary 12

Using the sampling strategy of Lemma 9 and the proof of Theorem 4 from [9] we get the following corollary.

Corollary 13. *Consider an execution of the above described implementation of $\binom{2}{1}$-OT^k from string commitments. Let X_0 and X_1 be the strings from $\{0,1\}^k$ output by Alice. Then there exists a bit c such that X_{1-c} is close to uniform with respect to Bob's view (given X_c), i.e., for any $\varepsilon, \delta > 0$:*

$$\begin{aligned}\delta(\rho_{X_{1-c}X_cE}, &\frac{1}{2^k}\mathbb{1} \otimes \rho_{X_cE}) \\ &\leq \frac{1}{2} \cdot 2^{-\frac{1}{2}((\frac{1}{4}-\frac{\varepsilon}{2}-h(\delta))(1-\alpha)\kappa b - k)} + 2e^{-(1-\delta)\alpha\kappa\delta^2/32} + 2e^{-2\varepsilon^2(1-\alpha)\kappa b}.\end{aligned}$$

where E denotes the quantum state output by Bob and $\mathbb{1}$ the identity operator on $\mathbb{C}^{2^k}$.

Proof. As in the proof of Theorem 4 from [9] we consider the equivalent EPR-version of the protocol. Let

$$|\varphi_{AE_o}\rangle \in \mathcal{H}_{A_1} \otimes \ldots \mathcal{H}_{A_m} \otimes \mathcal{H}_{E_o},$$

be the state shared between Alice and Bob after Bob has committed to the bases $\hat{\theta}$ and the measurement outcomes $\hat{x}$ where we can assume $\hat{\theta} = \hat{x} = (0, \ldots, 0)$. Alice now chooses a subset $\mathcal{T}$ of size $\alpha\kappa b$ to be opened by Bob. Let $\alpha' := (1/2 - \delta/2)\alpha$. Using Lemma 9 we can conclude that the state $|\varphi_{A_{\bar{\mathcal{T}}}E_o}\rangle$ is

$$\varepsilon_{\text{quant}}^{\delta} \leq \sqrt{\varepsilon_{\text{class}}^{\delta}} \leq \sqrt{3\exp(-\alpha'\kappa\delta^2/8)}$$

close to being a superposition of states with Hamming weight of at most δ within $A_{\bar{\mathcal{T}}}$ (if Alice does not abort). The statement then follows from the proof given in [9].

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

$$\varepsilon \geq \frac{c}{m}.$$

Proof. We assume that there exists a protocol that implements string commitments of length $m'+1$ out of string commitments of length m' with an error of at most ε for any $m' \geq m$. Then we can start with κ string commitments of length m and implement κ string commitments of length $n := 25(4m+1)$ with an error of at most $\kappa n \cdot \varepsilon$. Then, we can apply the protocol from [8] using string commitments to implement $\binom{2}{1}$-OT^k. Using Corollary 13 we get an error of at most

$$\frac{1}{2} \cdot 2^{-\frac{1}{2}((\frac{1}{4}-\frac{\bar{\varepsilon}}{2}-h(\delta))(1-\alpha)\kappa n-k)} + 2\exp(-(1-\delta)\alpha\kappa\delta^2/32) + 2\exp(-2\bar{\varepsilon}^2(1-\alpha)\kappa m).$$

for any $\bar{\varepsilon}, \delta > 0$. We choose $\kappa := 1300000$, $\delta := 0.02$, $\bar{\varepsilon} := 0.01$, $\alpha := 0.6$, and $k := 4m\kappa + 28$. Since $((\frac{1}{4}-\frac{\bar{\varepsilon}}{2}-h(\delta))(1-\alpha) \geq 1/25$ we get

$$\left(\frac{1}{4}-\frac{\bar{\varepsilon}}{2}-h(\delta)\right)(1-\alpha)\kappa n - k \geq \frac{\kappa n}{25} - k \geq 60 \; .$$

So the error of the last step is at most

$$2\exp(-(1-\delta)\alpha\kappa\delta^2/32) + 2\exp(-2\bar{\varepsilon}^2(1-\alpha)\kappa m) + \frac{1}{2} \cdot 2^{-30} \leq 0.00015$$

and the total error is at most

$$\varepsilon' := \kappa n \cdot \varepsilon + 0.00015 \; .$$

But any quantum reduction of $\binom{2}{1}$-OT^{4m+28} to m commitments must have an error of at least $1/2116$, since otherwise we would have

$$(1-23\sqrt{\varepsilon'})(4m+28)/2 - 7h(\sqrt{\varepsilon'}) > \frac{1}{4}(4m+28) - 7 \geq m \; ,$$

which contradicts Theorem 6. It follows that

$$\kappa n \cdot \varepsilon + 0.00015 \geq 1/2116$$

or

$$\varepsilon \geq \frac{1/2116 - 0.00015}{25\kappa(4m+1)} \geq \frac{1}{3100 \cdot 25\kappa(4m+1)} \; .$$

The statement follows. □

E Proof of Lemma 9

We need the following two inequalities: The Chernoff/Hoeffding inequality and a uniform sampling lemma, which follows from the Hoeffding-Azuma inequality.

Lemma E1 (Chernoff/Hoeffding Inequality [15, 34]) *Let $X_0, \ldots, X_{n-1}$ be independent random variables with $X_i \in [0,1]$. Let $X := \frac{1}{n}\sum_{i=0}^{n-1} X_i$, and $\mu = E[X]$. Then, for any $\varepsilon > 0$, $\Pr[X \geq \mu + \varepsilon] \leq e^{-2n\varepsilon^2}$ and $\Pr[X \leq \mu - \varepsilon] \leq e^{-2n\varepsilon^2}$.*

Lemma E2 (Uniform Sampling [3]) *Let $(\beta_1, \ldots, \beta_n) \in [0,1]^n$. Let $\mathcal{T}$ be a random subset of $[n]$ of size s.*

$$\Pr\left[\frac{1}{s}\sum_{i \in \mathcal{T}} \beta_i \leq \frac{1}{n}\sum_{i=1}^{n} \beta_i - \varepsilon\right] \leq e^{-s\varepsilon^2/2} \; .$$

Lemma 9. Let $\alpha \in [0, \frac{1}{2}]$. Let us take a bit-strings $y = (y_1, \dots y_m)$ of length $m := b\kappa$, that we group into κ blocks of size b. Let $\mathcal{T}^*$ be a random subset of $[\kappa]$ of size $\alpha\kappa$, $\mathcal{T}$ the corresponding set of bits in $[m]$ and $\bar{\mathcal{T}}$ the complement of $\mathcal{T}$. Let $\mathcal{T}'$ be a random subset of $\mathcal{T}$, where every element is chosen to be in $\mathcal{T}'$ with probability $\frac{1}{2}$, independent of everything else. With $\alpha' := (1/2 - \varepsilon)\alpha$ we have for any $\varepsilon > 0$

$$\Pr\left[\frac{1}{|\mathcal{T}'|}\sum_{i \in T'} y_i \leq \frac{1}{(1-\alpha)m}\sum_{i \in \bar{\mathcal{T}}} y_i - 2\varepsilon\right] \leq 3e^{-\alpha'\kappa\varepsilon^2/2} \, .$$

Proof. Let a_j be the number bits where y is equal to 1 in the jth block, for $j \in [\kappa]$, and let $\bar{\mathcal{T}}^*$ be the complement of $\mathcal{T}^*$. We apply Lemma E2 choosing $\beta_j := 1 - a_j/b$ and get

$$\Pr\left[\frac{1}{(1-\alpha)m}\sum_{i \in \bar{\mathcal{T}}} y_i \geq \frac{1}{m}\sum_{i=1}^{m} y_i + \varepsilon\right] = \Pr\left[\frac{1}{(1-\alpha)m}\sum_{j \in \bar{\mathcal{T}}^*} a_j \geq \frac{1}{m}\sum_{j=1}^{\kappa} a_j + \varepsilon\right] \tag{E.1}$$
$$\leq e^{-(1-\alpha)\kappa\varepsilon^2/2} \, . \tag{E.2}$$

Let $S \in \{0, \dots, \alpha m\}$ be the size of $\mathcal{T}'$. Even if we condition on the event that $\mathcal{T}'$ has size s, i.e, $S = s$, $\mathcal{T}'$ is still a random subset of $[m]$. Hence, we can apply Lemma E2 again and get

$$\Pr\left[\frac{1}{s}\sum_{i \in \mathcal{T}'} y_i \leq \frac{1}{m}\sum_{i=1}^{m} y_i - \varepsilon \middle| S = s\right] \leq e^{-s\varepsilon^2/2} \, ,$$

which implies that

$$\Pr\left[\frac{1}{S}\sum_{i \in \mathcal{T}'} y_i \leq \frac{1}{m}\sum_{i=1}^{m} y_i - \varepsilon \middle| S \geq \alpha' m\right] \leq e^{-\alpha' m\varepsilon^2/2} \, .$$

From Lemma E1 follows that

$$\Pr[S \leq \alpha' m] = \Pr\left[\frac{S}{\alpha m} \leq \frac{1}{2} - \varepsilon\right] \leq e^{-2\alpha m\varepsilon^2} \, .$$

Hence,

$$\Pr\left[\frac{1}{S}\sum_{i \in \mathcal{T}'} y_i \leq \frac{1}{m}\sum_{i=1}^{m} y_i - \varepsilon\right] \leq e^{-2\alpha m\varepsilon^2} + e^{-\alpha'\kappa\varepsilon^2/2} \leq 2e^{-\alpha' m\varepsilon^2/2} \, . \tag{E.3}$$

Combining Eqs. (E.1) and (E.3), we get

$$\Pr\left[\frac{1}{S}\sum_{i \in \mathcal{T}'} y_i \leq \frac{1}{(1-\alpha)m}\sum_{i \in \bar{\mathcal{T}}} y_i - 2\varepsilon\right] \leq 2e^{-\alpha' m\varepsilon^2/2} + e^{-(1-\alpha)\kappa\varepsilon^2/2} \tag{E.4}$$
$$\leq 3e^{-\alpha'\kappa\varepsilon^2/2} \, .$$

□

F Some Lemmas

F.1 Lemma 10

Lemma 10 shows that if two cq-states are close, then the probability to guess the classical bit from the quantum part are close as well.

Lemma 10. *For any two cq-states ρ^{XA} and σ^{XA}, $\delta(\rho^{XA}, \sigma^{XA}) \leq \varepsilon$ implies that for any measurement G on system A that outputs a bit, we have*

$$\big|\Pr[G(\rho^A) = X] - \Pr[G(\sigma^A) = X]\big| \leq \varepsilon \ .$$

Proof. Let us assume that there exists a measurement G that outputs a bit such that

$$\big|\Pr[G(\rho^A) = X] - \Pr[G(\sigma^A) = X]\big| > \varepsilon \ .$$

We can define the measurement D which on an input ψ^{XA} outputs 1 if $X = G(\psi^A)$, and 0 otherwise. We get

$$\big|\Pr[D(\rho^{XA}) = 1] - \Pr[D(\sigma^{XA}) = 1]\big| = \big|\Pr[G(\rho^A) = X] - \Pr[G(\sigma^A) = X]\big| > \varepsilon \ ,$$

which contradicts the assumption that $\delta(\rho^{XA}, \sigma^{XA}) \leq \varepsilon$. □

If we choose $\sigma^{XA} := \tau^X \otimes \sigma^A$, then X cannot be guessed from σ^A with probability bigger than 1/2. Lemma 10 therefore implies that if $\delta(\rho^{XA}, \tau^X \otimes \sigma^A) \leq \varepsilon$, then

$$\Pr[G(\rho^A) = X] \leq \frac{1}{2} + \varepsilon \ . \tag{F.1}$$

F.2 Lemma 11

Lemma 11 shows that if Bob knows X_1 with a small error, then the security condition implies that X_0 is close to uniform with respect to his state, if Alice chooses her inputs at random.

Lemma 11. *Let $\rho^{X_0X_1B}$ satisfy condition (3.7). If there exists a measurement G on system B such that $\Pr[G(\rho^B) = X_1] \geq 1 - \varepsilon$, then*

$$\delta(\rho^{X_0X_1B}, \tau^{X_0} \otimes \rho^{X_1B}) \leq 5\varepsilon \ .$$

Proof. Let $\sigma^{X_0X_1BC'}$ be the state in condition (3.7). Using Lemma 10, we get

$$\Pr[G(\sigma^B) = X_1] \geq \Pr[G(\rho^B) = X_1] - \varepsilon \geq 1 - 2\varepsilon \ .$$

In the state $\sigma^{X_0X_1BC'}$, we can guess the first bit of $X_{1-C'}$ if we output the first bit of $G(\sigma^B)$ whenever $C' = 0$ and a random bit otherwise. We succeed with a probability of

$$\begin{aligned} g :=& \frac{1}{2} \cdot \Pr[C' = 1] + \Pr[G(\sigma^B) = X_1 \wedge C' = 0] \\ =& \frac{1}{2} \cdot (1 - \Pr[C' = 0]) + \Pr[C' = 0] - \Pr[G(\sigma^B) \neq X_1 \wedge C' = 0] \\ \geq& \frac{1}{2} \cdot (1 - \Pr[C' = 0]) + \Pr[C' = 0] - 2\varepsilon \\ =& \frac{1}{2} + \frac{\Pr[C' = 0]}{2} - 2\varepsilon \ . \end{aligned}$$

Since $X_{1-C'}$ is completely random and independent of the rest, we have $g \leq \frac{1}{2}$, and hence $\Pr[C' = 0] \leq 4\varepsilon$. This implies that for $\hat{\sigma}^{X_0X_1BC'} := \tau^{X_0} \otimes \sigma^{X_1B} \otimes |1\rangle\langle 1|$ we have

$$\delta(\sigma^{X_{1-C'}X_{C'}BC'}, \hat{\sigma}^{X_{1-C'}X_{C'}BC'}) \leq 4\varepsilon$$

and hence

$$\begin{aligned} \delta(\rho^{X_0X_1B}, \tau^{X_0} \otimes \rho^{X_1B}) &\leq \delta(\rho^{X_0X_1B}, \sigma^{X_0X_1B}) + \delta(\sigma^{X_0X_1B}, \hat{\sigma}^{X_0X_1B}) \\ &\leq 5\varepsilon \ . \end{aligned}$$

□

F.3 Lemma F1

Lemma F1 *Let P_{XY} be a distribution over $\mathcal{X} \times \{0,1\}$. Then for any $P_{X'}$ over $\mathcal{X}$, we have*

$$\delta(P_{X|Y=0}, P_{X|Y=1}) \leq \frac{\delta(P_{XY}, P_{X'}P_Y)}{\min(P_Y(0), P_Y(1))}$$

Proof. For $y \in \{0,1\}$, we have

$$\begin{aligned}
\delta(P_{X|Y=y}, P_{X'}) =& \frac{1}{2}\sum_x \left| \frac{P_{XY}(x,y)}{P_Y(y)} - P_{X'}(x) \right| \\
=& \frac{1}{2P_Y(y)} \sum_x |P_{XY}(x,y) - P_{X'}(x)P_Y(y)| \\
\leq& \frac{1}{\min(P_Y(0), P_Y(1))} \frac{1}{2} \sum_x |P_{XY}(x,y) - P_{X'}(x)P_Y(y)| \ .
\end{aligned}$$

Hence,

$$\begin{aligned}
\delta(P_{X|Y=0}, P_{X|Y=1}) &\leq \delta(P_{X|Y=0}, P_{X'}) + \delta(P_{X|Y=1}, P_{X'}) \\
&\leq \frac{1}{\min(P_Y(0), P_Y(1))} \frac{1}{2} \sum_{xy} |P_{XY}(x,y) - P_{X'}(x)P_Y(y)| \\
&= \frac{1}{\min(P_Y(0), P_Y(1))} \delta(P_{XY}, P_{X'}P_Y) \ .
\end{aligned}$$

□

F.4 Lemma F2

Lemma F2 *Let P_{XY} be a distribution over $\mathcal{X} \times \{0,1\}$, $P_{X'}$ over $\mathcal{X}$ and $P_{Y'}$ over $\{0,1\}$. Then $\delta(P_{XY}, P_{X'}P_{Y'}) \leq \varepsilon$ implies*

$$\delta(P_{X|Y=0}, P_{X|Y=1}) \leq \frac{2\varepsilon}{\min(P_{Y'}(0), P_{Y'}(1)) - \varepsilon} \ .$$

Proof (Proof of Lemma F2). $\delta(P_{XY}, P_{X'}P_{Y'}) \leq \varepsilon$ implies $\delta(P_X, P_{X'}) \leq \varepsilon$ and hence

$$\delta(P_X P_{Y'}, P_{X'}P_{Y'}) = \delta(P_X, P_{X'}) \leq \varepsilon \ .$$

We get

$$\delta(P_{XY}, P_{X'}P_Y) \leq \delta(P_X P_Y, P_{X'}P_{Y'}) + \delta(P_{X'}P_{Y'}, P_{X'}P_Y) \leq 2\varepsilon \ .$$

$\delta(P_{XY}, P_{X'}P_{Y'}) \leq \varepsilon$ also implies $\delta(P_Y, P_{Y'}) \leq \varepsilon$, from which follows that for $y \in \{0,1\}$, $|P_Y(y) - P_{Y'}(y)| \leq \varepsilon$. We get

$$\frac{1}{\min(P_Y(0), P_Y(1))} \leq \frac{1}{\min(P_{Y'}(0), P_{Y'}(1)) - \varepsilon}$$

The statement follows now by applying Lemma F1. □