Statistical Impossibility Results for 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). But since in practice one is usually willing to tolerate a small probability of error and since these *statistical* reductions can be much more efficient, the known bounds have only limited application. In this work we provide lower bounds on the efficiency of 1-out-of-n OT and Rabin-OT reductions to distributed randomness in the statistical case. From these results we derive bounds on reductions to different variants of OT that generalize known bounds to the statistical case. Our bounds hold in particular for transformations between a finite number of primitives and for *any* error.

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

1 Introduction

Secure multi-party computation has been introduced by Yao ([Yao82]). It allows two or more distrustful players to jointly compute a function of their inputs in a secure way. 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 [GV88,Kil88]. The original form of OT ($(\frac{1}{2})$-$\mathsf{RabinOT}^1$) has been introduced by Rabin in [Rab81]. It allows a sender to send a bit x, which the receiver will get with probability $\frac{1}{2}$. Another variant of OT, called one-out-of-two bit-OT ($\binom{2}{1}$-OT^1) was defined in [EGL85] (see also [Wie83]). 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 $\binom{n}{1}$-OT^k where the inputs are strings of k bits and the receiver can choose from $n > 2$ secrets and (p)-$\mathsf{RabinOT}^k$ where the inputs are strings of k bits and the erasure probability is different from $\frac{1}{2}$.

If the players have access to noiseless 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 [Cré88] 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 [BBR88,CS91,BCS96,BCW03], and $\binom{n}{1}$-OT^k can be implemented from $\binom{2}{1}$-$\mathsf{OT}^{k'}$ [BCR86,BCS96,DM99,WW05]. 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 [CK88,CMW04,DFMS04], noisy correlations [WW04,NW06], or weak variants of OT [CK88,BCW03,Cac98,DFSS06,DKS99,Wul07].

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

Previous Results. The first impossibility result for unconditionally secure reductions of OT has been presented in [Bea96]. There it has been shown that the number of $\binom{2}{1}\text{-}\mathsf{OT}^1$ cannot be *extended*[3], i.e., there does not exist a protocol using n instances of $\binom{2}{1}\text{-}\mathsf{OT}^1$ 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 [DM99] (see also [Mau99]) and generalized in [WW05,WW08]. 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 [KK07]. Lower bounds for general functions have been presented in [BM04].

All these results only consider *perfect* protocols and do not give much insight into the case of statistical implementations. As pointed out in [KK07], their result *only* applies to the perfect case, because the protocol in [CS06] is more efficient. The bounds for perfect and statistical protocols can in fact be *very* far apart, as shown in [BM04]: 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 [AC07] a proof sketch of a lower bound for statistical implementations of $\binom{2}{1}\text{-}\mathsf{OT}^k$ 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 [BM04] a non-asymptotic lower bound on the number of ANDs needed to implement functions with boolean output has been shown. But this result can only be applied to protocols implementing one instance of $\binom{n}{1}\text{-}\mathsf{OT}^1$ and does not lead to an optimal bound.

Contribution. We provide general impossibility results for statistical implementations of $\binom{n}{1}\text{-}\mathsf{OT}^k$ and $(p)\text{-}\mathsf{RabinOT}^k$ in the semi-honest model[4]. In particular our bounds do not involve any asymptotics, i.e., we consider a finite number of primitives and our results hold for *any* error. The bounds for implementations of $\binom{n}{1}\text{-}\mathsf{OT}^k$ (Theorems 1 - 3) imply the following two corollaries, which generalize Theorem 3 from [Bea96] and the lower bounds from [DM99,WW05,WW08] to the statistical case.

Corollary 1. *If $\varepsilon m + h(\varepsilon) < 1/5$, then there does not exist a reduction of $m+1$ instances of $\binom{2}{1}\text{-}\mathsf{OT}^1$ to m instances of $\binom{2}{1}\text{-}\mathsf{OT}^1$ in the semi-honest model for any $m > 0$.*

Corollary 2. *For any reduction that implements $\binom{N}{1}\text{-}\mathsf{OT}^K$ from m instances of $\binom{n}{1}\text{-}\mathsf{OT}^k$ in the semi-honest model with an error smaller than ε, we have*

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

[3] Note that in the computational setting, OT *can* be extended, see [Bea96,IKNP03,Nie07].

[4] Bounds on OT in the semi-honest model imply similar bounds in the malicious model, see Section 2.3.

Corollary 2 is strictly stronger than the impossibility bounds from [AC07]. The following corollary is implied by Corollary 1, and gives an explicit error bound on how good $\binom{2}{1}$-OT^1 can be implemented from scratch, i.e., using noiseless communication only.

Corollary 3. *There does not exist a protocol that implements $\binom{2}{1}$-OT^1 in the semi-honest model with an error smaller than* 0.026*.*

We derive new bounds in the statistical case for protocols implementing (p)-$\mathsf{RabinOT}^k$ (Theorems 4 - 5). Finally, we show that our bounds imply bounds for implementations of oblivious linear function evaluation (OLFE, Corollary 5).

Our results show that the upper bounds implied by the protocols presented in [DM99] and [WW05] are tight in many cases, and that the protocol presented in [CS06] is asymptotically optimal. Our bounds also imply that the statistical reduction of the product-sharing functionality $\mathcal{F}_{\texttt{pdt-shr}}$ (which is equivalent to OLFE) to OT presented in [IPS09] is close to optimal.

2 Preliminaries

We denote the distribution of a random variable X over $\mathcal{X}$ by $P_X(x)$. 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

$$\delta(P_X, P_{X'}) = \frac{1}{2} \sum_{x \in \mathcal{X}} \left| P_X(x) - P_{X'}(x) \right|.$$

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

2.1 Entropies and Information

We will use the following tools from information theory[5] in our proofs. The *conditional Shannon entropy* of X given Y is defined as[6]

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

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

$$h(c \cdot \varepsilon) \geq c \cdot h(\varepsilon) . \tag{2.1}$$

[5] See [CT91] for a good introduction into information theory.

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

We will need the chain-rule

$$\mathrm{H}(XY \mid Z) = \mathrm{H}(X \mid Z) + \mathrm{H}(Y \mid XZ)\ , \tag{2.2}$$

and the following monotonicity inequalities

$$\mathrm{H}(XY \mid Z) \geq \mathrm{H}(X \mid Z) \geq \mathrm{H}(X \mid YZ)\ , \tag{2.3}$$
$$\mathrm{I}(WX; Y \mid Z) \geq \mathrm{I}(X; Y \mid Z)\ . \tag{2.4}$$

We will also need

$$\mathrm{H}(X \mid YZ) = \sum_z P_Z(z) \cdot H(X \mid Y, Z = z)\ . \tag{2.5}$$

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 $P_{X|Y} = P_{X|YZ}$, or $P_{Z|Y} = P_{Z|XZ}$, since the condition is symmetric in X and Z. $X \leftrightarrow Y \leftrightarrow Z$ implies that

$$H(X \mid Z) \geq H(X \mid YZ) = H(X \mid Y)\ . \tag{2.6}$$

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

$$I(X; Y \mid ZW) \leq I(X; Y \mid Z) \text{ and} \tag{2.7}$$
$$I(W; Y \mid Z) \leq I(X; Y \mid Z)\ . \tag{2.8}$$

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 (as we prove in Appendix B)

$$\mathrm{H}(\hat{X}|\hat{Y}) \geq \mathrm{H}(X|Y) - \epsilon \log(|\mathcal{X}|) - \mathrm{h}(\epsilon)\ . \tag{2.9}$$

Inequality (2.9) implies Fano's inequality: For all $X, \hat{X} \in \mathcal{X}$ with $\Pr[X \neq \hat{X}] \leq \varepsilon$, we have

$$H(X \mid \hat{X}) \leq \varepsilon \cdot \log |\mathcal{X}| + h(\varepsilon)\ . \tag{2.10}$$

2.2 Protocols and Security in the Semi-Honest Model

In the following we consider two-party primitives that take inputs (x, y) and output $(\bar{x}, \bar{y})$ 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 (x, y) distributed according to $P_{\bar{X}\bar{Y}}$, we may simply write $P_{\bar{X}\bar{Y}}$.

We define a *protocol with black-box access to a primitive* P_{UV} as a pair of functions (f, g). The protocol is then executed between the two players, Alice and Bob, as follows. The players receive their inputs x and y, choose uniformly at random $r_A, r_B \in \{0,1\}^*$, and receive the outputs u and v from P_{UV}. Then they repeat for $i = 1, 2 \ldots$: If i is odd, then Alice sends a message $m_i = f(x, u, m_1, \ldots, m_{i-1}, r_A)$ to Bob; if i is even, Bob sends a message $m_i = g(y, v, m_1, \ldots, m_{i-1}, r_B)$ to Alice. If any m_i is equal to halt, i.e., if one of the two players aborts the computation, then the loop is exited. Finally, Alice outputs $\tilde{x} = f(x, u, m_1, \ldots, m_i, r_A)$, and Bob outputs $\tilde{y} = g(y, v, m_1, \ldots, m_i, r_A)$.

We will only 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. Therefore, a dishonest Alice will output her whole view $(\tilde{x}, (x, u, m_1, \ldots, m_i, r_A))$.

A protocol securely implements $P_{\bar{X}\bar{Y}|XY}$, if the entire view of each player can be simulated 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 the input nor the output from the ideal primitive. Our definition of security follows Definition 7.2.1 from [Gol04], but is adapted to the case of computationally unbounded adversaries and statistical indistinguishability.

Definition 1. *A protocol (f, g) with black-box access to a primitive P_{UV} implements a primitive $P_{\bar{X}\bar{Y}|XY}$* ε-secure in the semi-honest model*, if there exist two randomized functions $S_A(x, \bar{x})$ and $S_B(y, \bar{y})$, called the simulators*[7]*, such that for all x and y, the distribution of $((\bar{x}, S_A(x, \bar{x})), \bar{y})$ is ε-close to the distribution of $((\tilde{x}, (x, u, m_1, \ldots, m_i, r_A)), \tilde{y})$ and the distribution of $(\bar{x}, (\bar{y}, S_B(y, \bar{y})))$ is ε-close to the distribution of $(\tilde{x}, (\tilde{y}, (y, v, m_1, \ldots, m_i, r_B)))$, where $\bar{x}, \bar{y}$ are distributed according to $P_{\bar{X}\bar{Y}|X=x,Y=y}$.*

2.3 Semi-Honest vs. Malicious Model

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, however, this implication *does* hold, because if the adversary is semi-honest, a simulator can only change the input with small probability. Otherwise, it 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. The proof is given in Appendix A.

2.4 Primitives and Randomized Primitives

In this work we will mainly focus on implementations of the primitives $\binom{n}{1}\text{-}\mathsf{OT}^k$ and $(p)\text{-}\mathsf{RabinOT}^k$.

- $\binom{n}{1}\text{-}\mathsf{OT}^k$ 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 $c \in \{0, \ldots, n-1\}$. Bob receives $y = x_c \in \{0,1\}^k$.
- $(p)\text{-}\mathsf{RabinOT}^k$ 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.

We only allow a protocol to use a primitive P_{UV} that does not have any input. This is enough for all reductions we look at in this work, since $\binom{n}{1}\text{-}\mathsf{OT}^k$ and $(p)\text{-}\mathsf{RabinOT}^k$ are all equivalent to such primitives 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 the primitive using the distributed randomness as input to the two parties. The fact that $\binom{2}{1}\text{-}\mathsf{OT}^1$ is equivalent to distributed randomness has been presented in [BBCS92,Bea95]. The generalization to $\binom{2}{1}\text{-}\mathsf{OT}^k$ is straightforward. The randomized primitives are obtained by simply choosing all inputs uniformly at random. For $(p)\text{-}\mathsf{RabinOT}^k$, the implementation is straightforward. Hence, any protocol that uses some instances of $\binom{n}{1}\text{-}\mathsf{OT}^k$ or $(p)\text{-}\mathsf{RabinOT}^k$ can be converted into a protocol that only uses a primitive P_{UV} without any input. In our proofs, we will need three properties of

[7] We do not require the simulator to be efficient.

these primitives: $H(U \mid V)$, $H(V \mid U)$ and $I(U;V)$, which are simplified versions of the monotones defined in [WW05,WW08][8]

If (U,V) is distributed according to the randomized primitive equivalent to $\binom{n}{1}\text{-}\mathsf{OT}^k$, we get

$$H(U \mid V) = (n-1)k\ , \quad H(V \mid U) = \log(n)\ , \quad I(U;V) = k\ . \tag{2.11}$$

If (U,V) is distributed according to the randomized primitive equivalent to $(p)\text{-}\mathsf{RabinOT}^k$, we get

$$H(U \mid V) = (1-p)k\ , \quad H(V \mid U) = h(p)\ , \quad I(U;V) = pk\ . \tag{2.12}$$

3 Lower Bounds for Unconditionally Secure Two-Party Computation

We will now give lower bounds for unconditionally secure two-party protocols. We will look at protocols as described in Section 2.2. Let (U,V) be the output of the primitive P_{UV}, and let M be the whole communication during the execution of the protocol. Let $\tilde{X}$ and $\tilde{Y}$ be the outputs of Alice and Bob on inputs X and Y distributed according to P_{XY}. Note that $\tilde{X}$ is generated from (X,U,M) and $\tilde{Y}$ from (Y,V,M), from which follows that $\tilde{X} \leftrightarrow XUM \leftrightarrow YV\tilde{Y}$ and $XU\tilde{X} \leftrightarrow YVM \leftrightarrow \tilde{Y}$. Since this holds for any input distribution P_{XY}, it also holds conditioned on $X = x$ or $Y = y$.

Lemma 1.

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

Proof. Let $M^i := (M_1, \dots, M_i)$, 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 (2.7) that

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

The statement follows by induction over all rounds.

Let the 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., $P_{\bar{X}\bar{Y}} := P_{XY}P_{\bar{X}\bar{Y}|XY}$. Then the security of the protocol implies the following lemma.

Lemma 2.

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

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 (2.9) and (2.6), we get

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

[8] Note that our results could easily be generalized to the monotones from [WW05,WW08]. However, for the distributions of the randomized primitives considered here, they would only complicate the proofs and not give any improvement.

3.1 Lower Bounds for Protocols implementing OT

Let $P_{\bar{Y}|XC}$ be the conditional distribution of $\binom{n}{1}$-OT^k. Let Alice and Bob choose their inputs $X = (X_0, X_1, \ldots, X_{n-1}) \in \{0,1\}^{kn}$ and $C \in \{0, \ldots, n-1\}$ uniformly at random. We have $\bar{Y} = X_C$. Let Y be the output of Bob at the end of the protocol.

Lemma 3.

$$\mathrm{H}(X \mid UM) \leq (3n-2)(\varepsilon k + h(\varepsilon)).$$

Proof. There exists a randomized function $S_A(x)$ such that $\delta(P_{XMU|C=c}, P_{XS_A(X)}) \leq \varepsilon$ for all $c \in \{0, \ldots, n-1\}$. Using the triangle inequality it follows that for any c, c'

$$\delta(P_{XMU|C=c}, P_{XMU|C=c'}) \leq 2\varepsilon \; . \tag{3.1}$$

It holds that $X \leftrightarrow UM \leftrightarrow YC$. Furthermore, we have $\Pr[Y \neq X_C \mid C = c] \leq \varepsilon$. Thus, it follows from (2.10) that

$$\mathrm{H}(X_c \mid UM, C = c) \leq \mathrm{H}(X_c \mid Y, C = c) \leq \varepsilon k + h(\varepsilon) \; . \tag{3.2}$$

Together with (3.1) and (2.9), this implies that for any c, c'

$$\begin{aligned} \mathrm{H}(X_{c'} \mid UM, C = c) &\leq 3\varepsilon k + h(\varepsilon) + h(2\varepsilon) \\ &\leq 3\varepsilon k + 3h(\varepsilon) \; , \end{aligned}$$

where the second inequality follows from (2.1). Using (2.2) and (2.3) we get

$$\mathrm{H}(X \mid UM, C = c) \leq \sum_{c' \in \{0,\ldots,n-1\}} \mathrm{H}(X_{c'} \mid UM, C = c) \leq (3n-2)(\varepsilon k + h(\varepsilon)) \; .$$

Using (2.5), this implies that

$$\mathrm{H}(X \mid UMC) \leq (3n-2)(\varepsilon k + h(\varepsilon))$$

Since $X \leftrightarrow UM \leftrightarrow YC$, (2.6) implies that

$$\begin{aligned} \mathrm{H}(X \mid UM) &= \mathrm{H}(X \mid UMC) \\ &\leq (3n-2)(\varepsilon k + h(\varepsilon)) \; . \end{aligned}$$

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

$$\mathrm{H}(U \mid V) \geq (n-1)k - (3n-1)(\varepsilon k + h(\varepsilon)).$$

Proof. From Lemma 3 and (2.3) follows that

$$\mathrm{H}(X \mid UVM) \leq \mathrm{H}(X \mid UM) \leq (3n-2)(\varepsilon k + h(\varepsilon)) \; .$$

Using (2.3), (2.2), (2.9) and Lemma 2, we get

$$\begin{aligned} (n-1)k - \varepsilon k - h(\varepsilon) &= \mathrm{H}(X \mid CX_C) - \varepsilon k - h(\varepsilon) \\ &\leq \mathrm{H}(X \mid VM) \\ &= \mathrm{H}(U \mid VM) + \mathrm{H}(X \mid UVM) - \mathrm{H}(U \mid XVM) \\ &\leq \mathrm{H}(U \mid VM) + (3n-2)(\varepsilon k + h(\varepsilon)) \\ &\leq \mathrm{H}(U \mid V) + (3n-2)(\varepsilon k + h(\varepsilon)) \; . \end{aligned}$$

Lemma 4. *For all $c \in \{0, \ldots, n-1\}$, we have*

$$H(X_C \mid M, C = c) \geq k - h(6\varepsilon) - 6\varepsilon k \geq k - 6(\varepsilon + h(\varepsilon))k.$$

Proof. Let P_R be the uniform distribution over the k-bit strings. As in the proof of Lemma 3 we get for all $c \neq c' \in \{0, \ldots, n-1\}$ that

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

which implies that

$$\delta(P_{X_cM|C=c}, P_{X_cM|C=c'}) \leq 2\varepsilon \ . \tag{3.3}$$

and

$$\delta(P_R P_{M|C=c}, P_R P_{M|C=c'}) \leq 2\varepsilon \ . \tag{3.4}$$

Because the protocol is secure, there exists a simulator $S_B(c, \bar{y})$ such that

$$\delta(P_{XM|C=c'}, P_{XS_B(c', X_{c'})}) \leq \varepsilon \ ,$$

which implies that $\delta(P_{X_cM|C=c'}, P_R P_{S_B(c',X_{c'})}) \leq \varepsilon$. Therefore, using the triangle inequality we get that

$$\begin{aligned} \delta(P_{X_cM|C=c'}, P_R P_{M|C=c'}) &\leq \delta(P_{X_cM|C=c'}, P_R P_{S_B(c',X_{c'})}) \\ &\quad + \delta(P_R P_{S_B(c',X_{c'})}, P_R P_{M|C=c'}) \\ &\leq 2\varepsilon. \end{aligned} \tag{3.5}$$

Using the triangle inequality again it follows from (3.3), (3.4) and (3.5) that

$$\begin{aligned} \delta(P_{X_cM|C=c}, P_R P_{M|C=c}) &\leq \delta(P_{X_cM|C=c}, P_{X_cM|C=c'}) \\ &\quad + \delta(P_{X_cM|C=c'}, P_R P_{M|C=c'}) \\ &\quad + \delta(P_R P_{M|C=c'}, P_R P_{M|C=c}) \\ &\leq 6\varepsilon \ . \end{aligned}$$

Using (2.9) and (2.1), we get for all $c \in \{0, \ldots, n-1\}$

$$H(X_C \mid M, C = c) \geq k - h(6\varepsilon) - 6\varepsilon k \geq k - 6h(\varepsilon) - 6\varepsilon k \ .$$

Using Lemma 4 we can prove the following lower bound for reductions of $\binom{n}{1}$-OT^k in the semi-honest model.

Theorem 2. *Let a protocol having access to P_{UV} be an ε-secure implementation of $\binom{n}{1}$-OT^k in the semi-honest model. Then*

$$\mathrm{I}(U; V) \geq k - 7\varepsilon k - 7h(\varepsilon) \ .$$

Proof. Let Alice's input X be uniformly distributed and Bob's input be $C = 0$. Let Y be Bob's output and M be the whole communication. Then Lemma 4 implies that

$$H(X_0 \mid M) \geq k - 6(h(\varepsilon) + \varepsilon k)\ . \tag{3.6}$$

Since $\Pr[Y \neq X_0] \leq \varepsilon$ and $X_0 \leftrightarrow VM \leftrightarrow Y$, it follows from (2.6) and (2.10) that

$$H(X_0 \mid VM) \leq H(X_0 \mid Y) \leq \varepsilon k + h(\varepsilon)\ . \tag{3.7}$$

(3.6) and (3.7) imply, using $X \leftrightarrow UM \leftrightarrow CYV$, (2.8) and (2.4), that

$$\begin{aligned}\mathrm{I}(U; V \mid M) &\geq \mathrm{I}(X; V \mid M)\\ &\geq \mathrm{I}(X_0; V \mid M)\\ &= H(X_0 \mid M) - H(X_0 \mid VM)\\ &\geq k - 7\varepsilon k - 7h(\varepsilon)\end{aligned}$$

The statement follows using Lemma 1.

In [WW06], it has been shown that $\binom{2}{1}$-OT^1 can be implemented from one instance of $\binom{2}{1}$-OT^1 in the opposite direction. Therefore, it follows immediately from Theorem 1 that

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

since any violation of this bound could be used to construct a violation of the bound from Theorem 1. We will now show that a generalization of this bound also holds for $n > 2$. In the following, we will assume that $k = 1$. The resulting bound then also implies a bound for $k > 1$ since one instance of $\binom{n}{1}$-OT^1 can be implemented from one instance of $\binom{n}{1}$-OT^k.

Lemma 5.

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

Proof. Let $A_i := X_0 \oplus X_i$, for $i \in \{1, \dots, n-1\}$. From the security of the protocol follows that there exist a randomized function $S_B(c, \bar{y})$ such that for all $a = (a_1, \dots, a_{n-1}) \in \{0,1\}^{n-1}$,

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

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

$$\delta(P_{YCVM \mid A=a}, P_{YCVM \mid A=a'}) \leq 2\varepsilon\ . \tag{3.8}$$

We have $\Pr[Y \neq X_C \mid A = a] \leq \varepsilon$ for all a. If $A = (0, \dots, 0)$, we have $X_C = X_0$. Since $X \leftrightarrow VM \leftrightarrow Y$, it follows from (2.3) and (2.10) that

$$\begin{aligned}H(Y \mid VM, A = (0, \dots, 0)) &\leq H(Y \mid X, A = (0, \dots, 0))\\ &\leq H(Y \mid X_0, A = (0, \dots, 0)) \leq \varepsilon + h(\varepsilon)\ .\end{aligned} \tag{3.9}$$

Now, let us map C to a bit-string of size $\lceil \log n \rceil$, and let C_b be the bth bit of that bit-string, where $b \in \{0, \dots, \lceil \log n \rceil - 1\}$. Let $a^b = (a^b_1, \dots, a^b_{n-1})$, where $a^b_i = 1$ if and only if the bth bit of i is 1. Conditioned on $A = a^b$, we have $X_C = X_0 \oplus C_b$. It follows from $X \leftrightarrow VM \leftrightarrow YC$, (2.3) and (2.10) that

$$H(Y \oplus C_b \mid VM, A = a^b) \leq H(Y \oplus C_b \mid X_0, A = a^b) \leq \varepsilon + h(\varepsilon)\ . \tag{3.10}$$

From (3.8) and (3.9), we get

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

It follows from (3.8) and (3.10) that for all b

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

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

$$H(CY \mid VMA) \leq 3(\lceil \log n \rceil + 1)(\varepsilon + h(\varepsilon))\ .$$

The statement follows from $A \leftrightarrow VM \leftrightarrow CY$, (2.3) and $\lceil \log n \rceil \leq \log n + 1$.

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

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

Proof. From Lemma 5 and (2.3) follows that

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

Using (2.3), (2.2), (2.9) and Lemma 2, we get

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

Theorems 1, 2 and 3 can now be used to show various lower bounds. First of all, 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 $\mathrm{H}(V \mid U) = m \log n$. For any protocol that implements one instance of $\binom{N}{1}$-OT^K, with an error of ε, it follows from Theorem 1 that

$$m(n-1)k \geq (N-1)K - (3N-1)(\varepsilon K + h(\varepsilon))\ ,$$

from Theorem 2 that

$$mk \geq K - 7\varepsilon K - 7h(\varepsilon)\ ,$$

and from Theorem 3 that

$$m \log n \geq \log N - (4 \log N + 7)(\varepsilon + h(\varepsilon))\ .$$

Hence, we get

$$\begin{aligned}
m &\geq \max\left(\frac{(N-1)K}{(n-1)k}, \frac{K}{k}, \frac{\log N}{\log n}\right) \\
&\qquad - \max\left(\frac{(3N-1)K}{(n-1)k}, \frac{7K}{k}, \frac{4\log N + 7}{\log n}\right)(\varepsilon + h(\varepsilon)) \\
&\geq \max\left(\frac{(N-1)K}{(n-1)k}, \frac{K}{k}, \frac{\log N}{\log n}\right) - 7NK \cdot (\varepsilon + h(\varepsilon))\ ,
\end{aligned}$$

which is the statement of Corollary 2.
In the same way we can prove the following corollary that generalizes a bound on reductions of OT to the binary symmetric noisy channel with error p ((p)-BNC), given in [WW08] to the statistical case. (p)-BNC has an input $x \in \{0,1\}$ and outputs a value $y \in \{0,1\}$ that is equal to x with probability p, where $0 \leq p < \frac{1}{2}$.

Corollary 4. *If a protocol implements $\binom{n}{1}$-OT^k from t instances of a (p)-BNC secure in the semi-honest model with an error ε, then*

$$t \geq \max\left(\frac{(n-1)k}{h(p)}, \frac{k}{1-h(p)}, \frac{\log n}{h(p)}\right) - \frac{7nk}{h(p)} \cdot (\varepsilon + h(\varepsilon)) \ .$$

There exists a trivial protocol that implements $\binom{n}{1}$-OT^{km} from m instances of $\binom{n}{1}$-OT^k: The receiver simply chooses always the same value. This allows us to generalize Theorems 1 and 2, because from any protocol for which the bounds of Corollary 5 does not hold, we could construct a protocol that violates the bounds of Theorems 1 or 2.

Corollary 5. *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*

$$\begin{aligned} \mathrm{H}(U \mid V) &\geq m(n-1)k - (3n-1)(\varepsilon mk + h(\varepsilon)) \ , \\ \mathrm{I}(U;V) &\geq mk - 7\varepsilon mk - 7h(\varepsilon) \ . \end{aligned}$$

If P_{UV} is equivalent to m instances of $\binom{n}{1}$-OT^k, we get $\mathrm{H}(U \mid V) = m(n-1)k$. Hence, for any protocol that implements $m+1$ instances with an error ε, we have

$$m(n-1)k \geq (m+1)(n-1)k - (3n-1)(\varepsilon mk + h(\varepsilon)) \ .$$

This implies the following corollary.

Corollary 6. *Let a protocol P having access to m instances of $\binom{n}{1}$-OT^k be an ε-secure implementation of $m+1$ instances of $\binom{n}{1}$-OT^k in the semi-honest model. Then*

$$\varepsilon mk + h(\varepsilon) \geq \frac{(n-1)k}{3n-1} \ .$$

The statement of Corollary 1 follows for $k = 1$ and $n = 2$.

3.2 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 6.

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

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 12 follows that

$$\delta(P_{XMU|D=0}, P_{XMU|D=1}) \leq \frac{2\varepsilon}{\min(p, 1-p) - \varepsilon} \; . \tag{3.11}$$

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 (2.6) and (2.10) that

$$\begin{aligned} \mathrm{H}(X \mid UM, Y \neq \Delta) &\leq \mathrm{H}(X \mid Y, Y \neq \Delta) \\ &\leq \frac{\varepsilon k}{p - \varepsilon} + h\left(\frac{\varepsilon}{p - \varepsilon}\right) \leq \frac{\varepsilon k + h(\varepsilon)}{p - \varepsilon} \; . \end{aligned} \tag{3.12}$$

Together (3.11) and (3.12) imply that

$$\begin{aligned} \mathrm{H}(X \mid UM, Y = \Delta) &\leq \frac{\varepsilon k + h(\varepsilon)}{p - \varepsilon} + \frac{2(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \\ &\leq \frac{3(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - \varepsilon} \; , \end{aligned} \tag{3.13}$$

and (2.5), (3.12) and (3.13) 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 (2.6) we get that $\mathrm{H}(X \mid UM) = \mathrm{H}(X \mid UMD)$. The statement follows.

Lemma 7.

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

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 (2.6) and (2.9) that

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

Let a protocol P having access to P_{UV} be an ε-secure implementation of (p)-$\mathsf{RabinOT}^k$ over k-bit strings in the semi-honest model. Let X be the uniformly distributed input of Alice and Y 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 m ideal instances of RabinOT and $P_{\bar{Y}X} := P_X P_{\bar{Y}|X}$.

Theorem 4. *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 6 and (2.3)

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

Using (2.3), (2.2), (2.9) and Lemma 2 we get

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

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

Lemma 8.

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

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

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

since $\delta(P_{X\bar{Y}M_A}, P_{XYM}) \leq \varepsilon$ and $\delta(P_{X\bar{Y}M_B}, P_{XYM}) \leq \varepsilon$. Together with Lemma 12 it follows that

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

Since $H(X \mid M_B, \bar{Y} = \mathit{\Delta}) = k$, together with (2.9) this implies

$$H(X \mid M_B, \bar{Y} \neq \mathit{\Delta}) \geq k - \frac{4(\varepsilon k + h(\varepsilon))}{\min(p, 1-p) - 2\varepsilon} .$$

From (2.5) follows

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

Therefore, using again (2.9),

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

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

Theorem 5. *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 8 implies that

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

and from Lemma 7 we have

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

Together this implies

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

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

Note that as in Corollary 5 for $\binom{n}{1}$-OT^k, the statement of these theorems can be generalized to m independent instances. We leave this to the full version of this work.

3.3 Lower Bounds for Protocols implementing OLFE

We will now show that Theorems 1 and 2 also imply 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 7. *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*

$$\mathrm{H}(U \mid V) \geq m \log q - 5(\varepsilon m \log q + h(\varepsilon)) \ , \tag{3.14}$$

$$\mathrm{H}(V \mid U) \geq m \log q - 5(\varepsilon m \log q + h(\varepsilon)) \ , \tag{3.15}$$

$$\mathrm{I}(U; V) \geq m \log q - 7(\varepsilon m \log q + h(\varepsilon)) \ . \tag{3.16}$$

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 (3.14) or (3.16) would imply a violation of Theorem 1 or Theorem 2. Furthermore, it has been shown in [WW06] that (q)-OLFE is symmetric. Hence, a violation of (3.15) would imply a violation of (3.14).

From Corollary 7 follows immediately that

Corollary 8. *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*

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

Acknowledgement

This work was funded by the Swiss National Science Foundation (SNSF) and the U.K. EPSRC, grant EP/E04297X/1.

References

[AC07] R. Ahlswede and I. Csiszar. On oblivious transfer capacity. Proceedings of the IEEE International Symposium on Information Theory (ISIT '07), 2007.

[BBCS92] C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology — CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 1992.

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[BCR86] G. Brassard, C. Crépeau, and J.-M. Robert. Information theoretic reductions among disclosure problems. In *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science (FOCS '86)*, pages 168–173, 1986.

[BCS96] G. Brassard, C. Crépeau, and M. Sántha. Oblivious transfers and intersecting codes. *IEEE Transactions on Information Theory, special issue on coding and complexity*, 42(6):1769–1780, 1996.

[BCW03] G. Brassard, C. Crépeau, and S. Wolf. Oblivious transfers and privacy amplification. *Journal of Cryptology*, 16(4):219–237, 2003.

[Bea95] D. Beaver. Precomputing oblivious transfer. In *Advances in Cryptology — EUROCRYPT '95*, volume 963 of *Lecture Notes in Computer Science*, pages 97–109. Springer-Verlag, 1995.

[Bea96] D. Beaver. Correlated pseudorandomness and the complexity of private computations. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 479–488. ACM Press, 1996.

[BM04] Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In *Theory of Cryptography Conference — TCC '04*, pages 238–257, 2004.

[Cac98] C. Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology — EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 361–374. Springer-Verlag, 1998.

[CK88] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS '88)*, pages 42–52, 1988.

[CMW04] C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In *Proceedings of Fourth Conference on Security in Communication Networks (SCN)*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59. Springer-Verlag, 2004.

[Cré88] C. Crépeau. Equivalence between two flavours of oblivious transfers (abstract). In *Advances in Cryptology — CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 350–354. Springer-Verlag, 1988.

[CS91] C. Crépeau and M. Sántha. On the reversibility of oblivious transfer. In *Advances in Cryptology — EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 106–113. Springer, 1991.

[CS06] C. Crépeau and G. Savvides. Optimal reductions between oblivious transfers using interactive hashing. In *Advances in Cryptology — EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 201–221. Springer-Verlag, 2006.

[CT91] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* Wiley-Interscience, New York, USA, 1991.

[DFMS04] I. Damgård, S. Fehr, K. Morozov, and L. Salvail. Unfair noisy channels and oblivious transfer. In *Theory of Cryptography Conference — TCC '04*, volume 2951 of *Lecture Notes in Computer Science*, pages 355–373. Springer-Verlag, 2004.

[DFSS06] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Oblivious transfer and linear functions. In *Advances in Cryptology — CRYPTO '06*, volume 4117 of *Lecture Notes in Computer Science*. Springer-Verlag, 2006.

[DKS99] I. Damgård, J. Kilian, and L. Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *Advances in Cryptology — EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 56–73. Springer-Verlag, 1999.

[DM99] Y. Dodis and S. Micali. Lower bounds for oblivious transfer reductions. In *Advances in Cryptology — EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 42–55. Springer-Verlag, 1999.

[EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.

[Gol04] O. Goldreich. *Foundations of Cryptography*, volume II: Basic Applications. Cambridge University Press, 2004.

[GV88] O. Goldreich and R. Vainish. How to solve any protocol problem - an efficiency improvement. In *Advances in Cryptology — CRYPTO '87*, Lecture Notes in Computer Science, pages 73–86. Springer-Verlag, 1988.

[IKNP03] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank. Extending oblivious transfers efficiently. In *Advances in Cryptology — CRYPTO '03*, pages 145–161. SpringerVerlag, 2003.

[IPS09] Y. Ishai, M. Prabhakaran, and A. Sahai. Secure arithmetic computation with no honest majority. In *Theory of Cryptography Conference — TCC '09*. Springer-Verlag, 2009.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 20–31. ACM Press, 1988.

[KK07] K. Kurosawa and W. Kishimoto. How to derive lower bound on oblivious transfer reduction. Cryptology ePrint Archive, Report 2007/065, 2007.

[Mau99] U. Maurer. Information-theoretic cryptography. In *Advances in Cryptology — CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 47–64. Springer-Verlag, 1999.

[Nie07] J. B. Nielsen. Extending oblivious transfers efficiently - how to get robustness almost for free. Cryptology ePrint Archive, Report 2007/215, 2007.

[NW06] A. Nascimento and A. Winter. On the oblivious transfer capacity of noisy correlations. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT '06)*, 2006.

[Rab81] M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[Wul07] J. Wullschleger. Oblivious-transfer amplification. In *Advances in Cryptology — EUROCRYPT '07*, Lecture Notes in Computer Science. Springer-Verlag, 2007.

[WW04] S. Wolf and J. Wullschleger. Zero-error information and applications in cryptography. In *Proceedings of 2004 IEEE Information Theory Workshop (ITW '04)*, 2004.

[WW05] S. Wolf and J. Wullschleger. New monotones and lower bounds in unconditional two-party computation. In *Advances in Cryptology — CRYPTO '05*, volume 3621 of *Lecture Notes in Computer Science*, pages 467–477, 2005.

[WW06] S. Wolf and J. Wullschleger. Oblivious transfer is symmetric. In *Advances in Cryptology — EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer-Verlag, 2006.

[WW08] S. Wolf and J. Wullschleger. New monotones and lower bounds in unconditional two-party computation. *IEEE Transactions on Information Theory*, 54(6):2792–2797, 2008.

[Yao82] A. C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164, 1982.

A Malicious OT implies Semi-honest OT

To prove the impossibility results in the malicious model it is sufficient to allow the simulators (for a semi-honest adversary) in Definition 1 to change the input from the honest players and change the output from the ideal primitive. The following lemmas prove that from such a malicious simulator we can always construct a semi-honest simulator in case of implementations of $\binom{n}{1}$-OT^k and (p)-$\mathsf{RabinOT}^k$.

Lemma 9. *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 10. *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 9 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 9 and 10.

B Some Lemmas

Lemma 11. *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,

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

Lemma 12. *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. $\delta(P_{XY}, P_{X'}P_{Y'}) \leq \varepsilon$ 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 11.

Lemma 13. *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*

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

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

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