Oblivious-Transfer Amplification

Jürg Wullschleger

ETH Zürich, Switzerland
wjuerg@inf.ethz.ch

Abstract. Oblivious transfer (OT) is a primitive of paramount importance in cryptography or, more precisely, two- and multi-party computation due to its universality. Unfortunately, OT cannot be achieved in an unconditionally secure way for both parties from scratch. Therefore, it is a natural question what information-theoretic primitives or computational assumptions OT *can* be based on.

The results in our paper are threefold. First, we give an optimal proof for the standard protocol to realize unconditionally secure OT from a weak variant of OT called *universal OT*, for which a malicious receiver can virtually obtain any possible information he wants, as long as he does not get all the information. This result is based on a novel distributed leftover hash lemma which is of independent interest.

Second, we give conditions for when OT can be obtained from a faulty variant of OT called *weak OT*, for which it can occur that any of the parties obtains too much information, or the result is incorrect. These bounds and protocols, which correct on previous results by Damgård *et. al.*, are of central interest since in most known realizations of OT from weak primitives, such as noisy channels, a weak OT is constructed first.

Finally, we carry over our results to the computational setting and show how a weak OT that is sometimes incorrect and is only mildly secure against computationally bounded adversaries can be strengthened.

Keywords: oblivious-transfer amplification, universal oblivious transfer, weak oblivious transfer, computational weak oblivious transfer, distributed leftover hash lemma, hard-core lemma.

1 Introduction

The goal of *multi-party computation*, introduced in [42], is to allow two parties to carry out a computation in such a way that no party has to reveal unnecessary information about her input. A primitive of particular importance in this context is *oblivious transfer* (OT) [39, 36, 18]. *Chosen one-out-of-two string oblivious transfer*, $\binom{2}{1}\text{-}\mathsf{OT}^n$ for short, is a primitive where the sender sends two strings x_0 and x_1 of length n and the receiver's input is a choice bit c; the latter then learns x_c but gets no information about the other string x_{1-c}. One reason for the importance of OT is its *universality*, i.e., it allows for carrying out *any* two-party computation [32]. Unfortunately, OT is impossible to achieve in an unconditionally secure way from scratch, i.e., between parties connected by a noiseless channel. However, if some additional weak primitives are available such as noisy channels or noisy correlations, then unconditional security can often be achieved [12, 11, 17, 15, 13, 40, 16, 35]. Most of these protocols first implement a weak version of OT, and then strengthen it to achieve OT. In [20, 23] it was shown that such a strengthening is sometimes also needed in the computational setting.

In this paper we study how weak versions of OT can be *amplified* to OT.

1.1 Previous Work

Various weak versions of OT have been proposed. In most of them, only the receiver's side is weak, such as α-1-2 *slightly OT* from [12], or only the sender's side is weak, such as *XOT*, *GOT* or *UOT with repetitions* from [6, 7]. All of these primitives were shown to be strong enough to imply OT. In [8], a more general primitive called *Universal OT*, (α)-$\binom{2}{1}$-UOT^n for short, has been proposed, where α specifies a lower bound on the amount of uncertainty a (possibly malicious) receiver has over *both* inputs, measured in collision- or min-entropy. Unfortunately, the security proof contained an error that was corrected in [16]. It was shown that $\binom{2}{1}$-OT^ℓ can be implemented from one instance of (α)-$\binom{2}{1}$-UOT^n with an error of at most ε if $\ell \leq \frac{1}{4}\alpha - \frac{3}{4}\log(1/\varepsilon) - 1$.

Weak OT, introduced in [17], is a weak version of $\binom{2}{1}$-OT^1 where *both* players may obtain additional information about the other player's input, and where the output may have some errors. It is used as a tool to construct OT out of *unfair primitives*, i.e., primitives where the adversary is more powerful than the honest participant, such as the *unfair noisy channel*. Weak OT is denoted as (p, q, ε)-WOT, where p is the maximal probability that the sender gets side information about the receiver's input, q the maximal probability that the receiver gets side information about the sender's input, and ε is the maximal probability that an error occurs. Using a simple simulation argument, it was shown in [17] that there cannot exist a protocol that implements $\binom{2}{1}$-OT^1 from (p, q, ε)-WOT if $p+q+2\varepsilon \geq 1$. For $\varepsilon = 0$, they give a protocol secure against active adversaries that implements $\binom{2}{1}$-OT^1 from $(p, q, 0)$-WOT for $p + q < 1$, which is optimal. Furthermore, for the case where p, q, and ε are bigger than 0, a protocol is presented that is secure against passive adversaries for $p + q + 2\varepsilon < 0.45$. Weak OT was later generalized in [15] to *(special) generalized weak OT*, in order to improve the reduction of $\binom{2}{1}$-OT^1 to unfair noisy channels.

In [20], a reduction of $\binom{2}{1}$-OT^1 to (p, q, ε)-WOT in the computational setting was presented. These results were used to show that OT can be based on *collections of dense trapdoor permutations*.

1.2 Problems with the Definition of Weak OT in [17]

While [17] does not give a formal definition of (p, q, ε)-WOT, [15] formally defines (p, q, ε)-WOT by giving an ideal functionality. Their definition implicitly makes two assumptions. It requires that, firstly, the players do not get information about whether an error occurred, and secondly, that the event that an error occurs is independent from the events that the players get side information. These assumptions are rather unnatural and in most of the cases where (p,q,ε)-WOT is used, they cannot be satisfied. For example, neither the simulation of (p,q,ε)-WOT for $p+q+2\varepsilon=1$, nor the application to the unfair noisy channel satisfy these assumptions.

Unfortunately, if we remove these two assumptions from the definition of (p,q,ε)-WOT, the $\mathsf{E\text{-}Reduce}$ protocol from [17] gets insecure, because it depends on the fact that the two events are independent. The following example illustrates the problem: Even though $(0,1/2,1/4)$-WOT can be simulated, by applying $\mathsf{R\text{-}Reduce}(3000, \mathsf{E\text{-}Reduce}(10,(0,1/2,1/4)\text{-}\mathsf{WOT}))$ (using the reductions $\mathsf{R\text{-}Reduce}$ and $\mathsf{E\text{-}Reduce}$ as defined in [17]) we get a $(0,0.06,0.06)$-WOT, which implies $\binom{2}{1}$-OT^1. We would get an information-theoretic secure $\binom{2}{1}$-OT^1 from scratch, which is impossible.

Directly affected by this problem are Lemma 5 and Theorem 2 in [17] and Lemma 6 in [15]. Indirectly affected are Lemma 11 and Theorem 3 in [17], and Lemma 1, 4, 5 and 7 in [15], as they rely on Lemma 5 in [17].

1.3 Contribution

In the first part, we show how to implement $\binom{2}{1}$-OT^ℓ from one instance of (α)-$\binom{2}{1}$-UOT^n for $\ell \leq \frac{\alpha}{2} - 3\log\frac{1}{\varepsilon}$ with an error of at most 2ε. This improves the bound of [16] by a factor of two, at the cost of a slightly bigger error term, and is asymptotically optimal for the standard protocol using 2-universal hashing. The proof makes use of a new *distributed leftover hash lemma*, which is a generalization of the leftover hash lemma and of independent interest.

In the second part, we will look at reductions of $\binom{2}{1}$-OT^1 to (p,q,ε)-WOT, for new, weaker definitions of (p,q,ε)-WOT. Using a different $\mathsf{E\text{-}Reduce}$ protocol that also works for our definitions, we show for the special case where $p=0$ ($q=0$), that $\binom{2}{1}$-OT^1 can efficiently be implemented from (p,q,ε)-WOT if $\sqrt{q}+2\varepsilon<1$ ($\sqrt{p}+2\varepsilon<1$), secure against passive adversaries. For the general case, we show that if $p+q+2\varepsilon \leq 0.24$ or $\max(p+22q+44\varepsilon, 22p+q+44\varepsilon, 7\sqrt{p+q}+2\varepsilon)<1$, $\binom{2}{1}$-OT^1 can efficiently be implemented from (p,q,ε)-WOT secure against passive adversaries. This fixes Lemma 5 and Theorem 2 in [17] and gives some new bounds, but does not reach the bound of $p+q+2\varepsilon<0.45$ from [17].

Finally, we apply these results to the computational case, and show, using the uniform hard-core lemma from [26], how an OT which may contain errors and which is only mildly *computationally* secure against the two players can be amplified to a computationally-secure OT. In particular, we show that if (p,q,ε)-WOT can be amplified to $\binom{2}{1}$-OT^1 in the information-theoretic setting, then also the computational version of (p,q,ε)-WOT which we call (p,q,ε)-$\mathsf{compWOT}$ can be amplified to a computationally-secure $\binom{2}{1}$-OT^1, *using the same protocol.* In combination with our information-theoretic results, we get a way to amplify (p,q,ε)-$\mathsf{compWOT}$. Our results generalize the results presented in [20], as we cover a much bigger region for the values p, q and ε, and in our case the security for both players may only be computational.

A more detailed analysis of all these results can be found in [41].

2 Preliminaries

Let X and X' be two random variables distributed over the same domain $\mathcal{X}$. The *advantage* of an algorithm $A : \mathcal{X} \to \{0,1\}$ to distinguish X from X' is defined as $\mathrm{Adv}^A(X, X') := \left|\Pr[A(X) = 1] - \Pr[A(X') = 1]\right|$. The *statistical distance* between X and X' is defined as $\Delta(X, X') = \frac{1}{2}\sum_{x \in \mathcal{X}} \left|\Pr[X = x] - \Pr[X = x]\right|$. It is easy to see that $\Delta(X, X') = \max_A \mathrm{Adv}^A(X, X')$. We say that a random variable X *over* $\mathcal{X}$ *is* ε*-close to uniform with respect to* Y, if $\Delta(P_{XY}, P_U P_Y) \leq \varepsilon$, where P_U is the uniform distribution over $\mathcal{X}$.

Definition 1. *Let P_{XY} be a distribution over $\{0,1\} \times \mathcal{Y}$. The* maximal bit-prediction advantage *of X from Y is* $\mathrm{PredAdv}(X \mid Y) := 2 \cdot \max_f \Pr[f(Y) = X] - 1$.

In other words, if $\mathrm{PredAdv}(X \mid Y) = \delta$, then we have for all functions $f : \mathcal{Y} \to \{0,1\}$ that $\Pr[f(Y) = X] \leq (1+\delta)/2$. It is easy to see that there exists an event $\mathcal{E}$ with $\Pr[\mathcal{E}] = \mathrm{PredAdv}(X \mid Y)$, such that if $\mathcal{E}$ occurs, then X is a function of Y and if $\mathcal{E}$ does not occur, then X is uniform conditioned on Y. Furthermore, we have $\mathrm{PredAdv}(X \mid Y) = 2 \cdot \Delta(P_{XY}, P_U P_Y)$, where P_U is the uniform distribution over $\{0,1\}$. Let $H_\infty(X \mid Y) = \min_{xy:P_{XY}(x,y)>0} - \log P_{X|Y}(x \mid y)$ be the *conditional min-entropy* of X given Y. A function $h : \mathcal{R} \times \mathcal{X} \to \{0,1\}^m$ is called a 2*-universal hash function* [10], if for all $x_0 \neq x_1 \in \mathcal{X}$, we have $\Pr[h(R, x_0) = h(R, x_1)] \leq 2^{-m}$, if R is uniform over $\mathcal{R}$.

We say that a function $f : \mathbb{N} \to \mathbb{N}$ is *polynomial in* k, denoted by $\mathrm{poly}(k)$, if there exists a constant $c > 0$ such that $f(k) \in O(k^c)$. A function $f : \mathbb{N} \to [0,1]$ is *negligible in* k, denoted by $\mathrm{negl}(k)$, if for all $c > 0$, $f(k) \in o(k^{-c})$.

2.1 Definition of Security

A $\mathcal{W}$*-hybrid protocol* is a sequence of interactions between two players. In each step, the players may apply a randomized function on their data, and send the result to the other player. They may also use the functionality $\mathcal{W}$ by sending input to $\mathcal{W}$ which gives them an output back according to the specification of $\mathcal{W}$. In the last stage the players output a randomized function of their data. A protocol is *efficient* if it can be executed using two polynomial time turing machines.

In the *semi-honest model*, the adversary is *passive*, which means that she follows the protocol, but outputs her entire view, i.e., all the information she has obtained during the execution of the protocol. In the *malicious model* the adversary is *active*, which means that he may change his behavior in an arbitrary way. Our definitions for the security of a protocol are based on the standard *real vs. ideal* paradigm of [34] and [1] (see also [9]). The idea behind the definition is that anything an adversary can achieve in the *real life protocol*, he could also achieve by another attack in an *ideal world*, i.e., where the players only have black-box access to the functionality they try to achieve. If the executions in the real and the ideal settings are *statistically indistinguishable* (the statistical distance is smaller than ε), we call the protocol *secure with an error of at most* ε, if they are only *computationally indistinguishable* (any efficient algorithm has negligible advantage in distinguishing them), we call the protocol *computationally secure*.

We will only look at a *fully randomized* version of $\binom{2}{1}$-OT^n denoted by $\binom{2}{1}$-ROT^n. $\binom{2}{1}$-ROT^n is equivalent to $\binom{2}{1}$-OT^n, which was shown in [4] and formally proved in [2]. Our definition of $\binom{2}{1}$-ROT^n is similar to the definitions in [16] and [14].

Definition 2 (Randomized oblivious transfer, malicious model). *A protocol Π between a sender and a receiver where the sender outputs $(X_0, X_1) \in \{0,1\}^n \times \{0,1\}^n$ and the receiver outputs $(C, Y) \in \{0,1\} \times \{0,1\}^n$ securely implements $\binom{2}{1}$-ROT^n in the malicious model with an error of at most ε, if the following conditions are satisfied:*

- (Correctness) *If both players are honest, then* $\Pr[Y \neq X_C] \leq \varepsilon$.
- (Security for the sender) *For an honest sender and any (malicious) receiver with output $\overline{V}$, there exists a random variable $\overline{C} \in \{0,1\}$, such that $X_{1-\overline{C}}$ is ε-close to uniform with respect to $(\overline{C}, X_{\overline{C}}, \overline{V})$.*
- (Security for the receiver) *For an honest receiver and any (malicious) sender with output $\overline{U}$, C is ε-close to uniform with respect to $\overline{U}$.*

In the semi-honest model, we additionally require that $\overline{C} = C$, because we also require the adversary in the ideal world to be semi-honest.

3 Distributed Randomness Extraction

In order to get an optimal bound for the reduction from $\binom{2}{1}$-OT^1 to (α)-$\binom{2}{1}$-UOT^n, we will need a generalization of Lemma 1, the *leftover hash lemma*. Since this is of independent interest, we present it in a separate section.

Lemma 1 tells us how many almost-random bits can be extracted from an imperfect source of randomness X, if some additional uniform randomness is present. It is also known as *privacy amplification*. See also [3, 25].

Lemma 1 (Leftover hash lemma [5, 30]). *Let X be a random variable over $\mathcal{X}$ and let $m > 0$. Let $h : \mathcal{S} \times \mathcal{X} \to \{0,1\}^m$ be a 2-universal hash function. If $m \leq H_\infty(X) - 2\log(1/\varepsilon) + 2$, then for S uniform over $\mathcal{S}$, $h(S, X)$ is ε-close to uniform with respect to S.*

We now generalize the setting and let two players independently extract randomness from two *dependent* random variables. Lemma 1 tells us that if the length of the extracted strings are smaller than the min-entropy of these random variables, then each of the extracted strings is close to uniform. However, the two strings might still be dependent on each other. Lemma 2 now says that if the total length of the extracted strings is smaller than the overall min-entropy, then the two strings are also almost independent. The obtained bound is optimal. The proof is very similar to a standard proof of the leftover hash lemma.

Lemma 2 (Distributed leftover hash lemma). *Let X and Y be random variables over $\mathcal{X}$ and $\mathcal{Y}$, and let $m, n > 0$. Let $g : \mathcal{S} \times \mathcal{X} \to \{0,1\}^m$ and $h : \mathcal{R} \times \mathcal{Y} \to \{0,1\}^n$ be 2-universal hash functions. If*

$$\min\left(H_\infty(X) - m, H_\infty(Y) - n, H_\infty(XY) - m - n\right) \geq 2\log(1/\varepsilon) \ ,$$

then, for (S, R) uniform over $\mathcal{S} \times \mathcal{R}$, $(g(S,X), h(R,Y))$ is ε-close to uniform with respect to (S,R).

Proof. For any W having distribution P_W over $\mathcal{W}$, and W' being uniformly distributed over $\mathcal{W}$, we have

$$\begin{aligned}\Delta(W,W') =& \frac{1}{2}\sum_w \left| P_W(w) - \frac{1}{|\mathcal{W}|}\right| = \frac{1}{2}\sqrt{\left(\sum_w \left| P_W(w) - \frac{1}{|\mathcal{W}|}\right|\right)^2} \\ \leq& \frac{1}{2}\sqrt{|\mathcal{W}|}\sqrt{\sum_w \left(P_W(w) - \frac{1}{|\mathcal{W}|}\right)^2} = \frac{1}{2}\sqrt{|\mathcal{W}|}\sqrt{\sum_w P_W^2(w) - \frac{1}{|\mathcal{W}|}} \ .\end{aligned}$$

Here we used that $(\sum_{i=1}^n a_i)^2 \leq n \sum_{i=1}^n a_i^2$, which follows from Cauchy-Schwarz. Let $V = g(S,X)$, $V' = h(R,Y)$ and U, U' be two uniform random variables over $\{0,1\}^m$ and $\{0,1\}^n$. Choosing $W := (V, V', S, R)$ and $W' := (U, U', S, R)$ in the above inequality, we get

$$\begin{aligned}&\Delta((V,V',S,R),(U,U',S,R)) \\ &\quad \leq \frac{1}{2}\sqrt{|\mathcal{S}||\mathcal{R}|2^{m+n}}\sqrt{\sum_{vv'sr} P^2_{VV'SR}(v,v',s,r) - \frac{1}{|\mathcal{S}||\mathcal{R}|2^{m+n}}} \ .\end{aligned}$$

Since $\sum_x P_X^2(x)$ is the *collision probability*[1] of a random variable X, we have for (X_0, Y_0) and (X_1, Y_1) independently distributed according to P_{XY} and for uniformly random S_0, S_1, R_0, and R_1 that

$$\begin{aligned}&\sum_{vv'sr} P^2_{VV'SR}(v,v',s,r) \\ &\quad = \Pr[g(X_0,S_0) = g(X_1,S_1) \wedge h(Y_0,R_0) = h(Y_1,R_1) \wedge S_0 = S_1 \wedge R_0 = R_1] \\ &\quad = \Pr[S_0 = S_1 \wedge R_0 = R_1]\Pr[g(X_0,S_0) = g(X_1,S_0) \wedge h(Y_0,R_0) = h(Y_1,R_0)] \ .\end{aligned}$$

Because g and h are 2-universal hash functions, we have

$$\begin{aligned}&\Pr[g(X_0,S_0) = g(X_1,S_0) \wedge h(Y_0,R_0) = h(Y_1,R_0)] \\ &\quad \leq \Pr[X_0 = X_1 \wedge Y_0 = Y_1] + 2^{-m}\Pr[X_0 \neq X_1 \wedge Y_0 = Y_1] \\ &\qquad + 2^{-n}\Pr[X_0 = X_1 \wedge Y_0 \neq Y_1] + 2^{-m-n} \\ &\quad = (1 + 3\varepsilon^2)2^{-m-n} \ ,\end{aligned}$$

from which follows that $\Delta((V,V',S,R),(U,U',S,R)) \leq \frac{\sqrt{3}}{2}\varepsilon$. $\square$

[1] Let X_0 and X_1 be distributed according to P_X. The collision probability is $\Pr[X_0 = X_1] = \sum P_X(x)^2$.

4 Universal Oblivious Transfer

In this section, we give an implementation of $\binom{2}{1}$-ROT^ℓ that uses one instance of *universal oblivious transfer (UOT)*, that allows ℓ to be roughly twice as large as in [16], at the cost of a slightly larger error term.

UOT is a weak version of ROT that allows a malicious receiver to obtain more information than what he would be allowed in ROT. For simplicity, we only define a perfect version of UOT. The definition (and also the proof of Theorem 1) can easily be adapted to the statistical case.

Definition 3 (Universal oblivious transfer, malicious model). *A protocol Π between a sender and a receiver where the sender outputs $(X_0, X_1) \in \{0,1\}^n \times \{0,1\}^n$ and the receiver outputs $(C, Y) \in \{0,1\} \times \{0,1\}^n$ securely implements (α)-$\binom{2}{1}$-UOT^n in the malicious model, if the following conditions are satisfied:*

- (Correctness) *If both players are honest, then $Y = X_C$.*
- (Security for the sender) *For an honest sender and any (malicious) receiver with output $\overline{V}$, we have $H_\infty(X_0, X_1 \mid \overline{V}) \geq \alpha$.*
- (Security for the receiver) *For an honest receiver and any (malicious) sender with output $\overline{U}$, C is uniform with respect to $\overline{U}$.*

We will use the same protocol as [6, 8, 7, 16]. Note that this protocol is only secure in the the malicious, but not to the semi-honest model.

Protocol $\mathsf{ROTfromUOT}(\alpha, n, \ell)$
Let $(U_0, U_1) \in \{0,1\}^\ell \times \{0,1\}^\ell$ be the senders output and $(C, Y) \in \{0,1\} \times \{0,1\}^\ell$ the receivers output. Let $h : \mathcal{R} \times \{0,1\}^n \to \{0,1\}^\ell$ be a 2-universal hash function.

1. Both players execute (α)-$\binom{2}{1}$-UOT^n. The sender receives (X_0, X_1), and the receiver receives (C, W).
2. The sender chooses $R_0, R_1 \in \mathcal{R}$ at random and sends (R_0, R_1) to the receiver.
3. The sender outputs $(U_0, U_1) := (h(R_0, X_0), h(R_1, X_1))$, and the receiver outputs $(C, Y) := (C, h(R_C, W))$.

To prove that the protocol is secure for the sender, we will define an additional random variable $A \in \{0, 1, 2\}$ that distinguishes between three cases. (We assume that the receiver gets to know A, which may only help him.) We will show that the protocol is secure in all three cases. It is easy to see that for this protocol the bound we obtain in Theorem 1 is asymptotically optimal.

Theorem 1. *Let $\varepsilon > 0$. Protocol $\mathsf{ROTfromUOT}(\alpha, n, \ell)$ securely implements $\binom{2}{1}$-ROT^ℓ with an error of at most 2ε out of one instance of (α)-$\binom{2}{1}$-UOT^n in the malicious model, if $\ell \leq \alpha/2 - 3\log(1/\varepsilon)$.*

Proof. Obviously the protocol satisfies correctness. Let the sender be honest. Let $\overline{V}'$ be the output of (α)-$\binom{2}{1}$-UOT^n to the (malicious) receiver. We will implicitly condition on $\overline{V}' = v'$. After the execution of (α)-$\binom{2}{1}$-UOT^n, we have $H_\infty(X_0 X_1) \geq \alpha$. Let $S_i := \left\{x_i \in \mathcal{X}_i : \Pr[X_i = x_i] \leq 2^{-\alpha/2}\right\}$, for $i \in \{0,1\}$. We define the random variable A as follows. Let $A = 2$ if $(X_0 \in S_0) \wedge (X_1 \in S_1)$, let $A = 0$ if $(X_0 \notin S_0) \wedge (X_1 \in S_1)$, let $A = 1$ if $(X_1 \notin S_1) \wedge (X_0 \in S_0)$, and let A be chosen uniformly at random in $\{0, 1\}$ if $(X_0 \notin S_0) \wedge (X_1 \notin S_1)$. If $\Pr[A = 2] \le \varepsilon$, we will ignore the event $A = 2$. Therefore, we redefine A for this event to take on the value 3. We end up with a random variable A that takes on the value 2 with probability 0 or at least ε, and which takes on the value 3 with probability at most ε. Let $\overline{C} = \min(A, 1)$.

– If the event $A = i$ occurs for $i \in \{0, 1\}$, we have $\overline{C} = i$. All $x_i \in S_i$ have $\Pr[X_i = x_i \wedge A = i] = 0$. For all $x_i \notin S_i$ we have $\Pr[X_i = x_i \wedge A = i] \ge \Pr[X_i = x_i]/2 \ge 2^{-\alpha/2-1}$. It follows that

$$\Pr[X_{1-i} = x_{1-i} \mid X_i = x_i \wedge A = i] = \frac{\Pr[X_{1-i} = x_{1-i} \wedge X_i = x_i \wedge A = i]}{\Pr[X_i = x_i \wedge A = i]} \le 2^{-\alpha}/2^{-\alpha/2-1} = 2^{-\alpha/2+1} ,$$

  and hence, $H_\infty(X_{1-\overline{C}} \mid X_{\overline{C}}, A = i) \ge \alpha/2 - 1$. Since $R_{1-\overline{C}}$ is chosen independently of the rest, it follows from Lemma 1 that, given $A = i$, the distribution of $U_{1-\overline{C}}$ is ε-close to uniform with respect to $(R_0, R_1, U_{\overline{C}})$.
– If the event $A = 2$ occurs, we have $\overline{C} = 1$, $\Pr[A = 2] \ge \varepsilon$, $\Pr[X_0 = x_0 \wedge X_1 = x_1 \mid A = 2] \le 2^{-\alpha}/\varepsilon$, and $\Pr[X_i = x_i \mid A = 2] \le 2^{-\alpha/2}/\varepsilon$, for $i \in \{0, 1\}$. It follows that $H_\infty(X_0 \mid A = 2) \ge \alpha/2 - \log(1/\varepsilon)$, $H_\infty(X_1 \mid A = 2) \ge \alpha/2 - \log(1/\varepsilon)$, and $H_\infty(X_0 X_1 \mid A = 2) \ge \alpha - \log(1/\varepsilon)$. Since R_0 and R_1 are chosen independently of the rest, it follows from Lemma 2 that given $A = 2$, (U_0, U_1) is ε-close to uniform with respect to (R_0, R_1), from which follows that $U_{1-\overline{C}}$ is ε-close to uniform with respect to $(R_0, R_1, U_{\overline{C}})$.

Therefore, for all $a \in \{0, 1, 2\}$, given $A = a$, there exists a $\overline{C}$ such that the distribution of $U_{1-\overline{C}}$ is ε-close to uniform with respect to $(R_0, R_1, \overline{C}, U_{\overline{C}})$. It follows that $U_{1-\overline{C}}$ is also ε-close to uniform with respect to $(R_0, R_1, \overline{C}, U_{\overline{C}})$ given $A < 3$, and since $\Pr[A = 3] \le \varepsilon$, $U_{1-\overline{C}}$ is 2ε-close to uniform with respect to $(R_0, R_1, \overline{C}, U_{\overline{C}})$. Because this holds for all $v' \in \mathcal{V}'$, and because $\overline{V}$ is a randomized function of $(R_0, R_1, \overline{V}')$, $U_{1-\overline{C}}$ is also 2ε-close to uniform with respect to $(\overline{C}, U_{\overline{C}}, \overline{V})$.

Let the receiver be honest, and let $\overline{U}'$ be the output of (α)-$\binom{2}{1}$-UOT^n to a (malicious) sender. From the security of (α)-$\binom{2}{1}$-UOT^n follows that C is uniform with respect to $\overline{U}'$. Since the receiver does not send any messages to the sender, C is also uniform with respect to $\overline{U}$. □

5 Weak Oblivious Transfer

In this section we show how ROT can be implemented using many instances of *weak oblivious transfer (WOT)*, which is a weak version of ROT where *both* players may get additional information, and where the output may be incorrect. We start by giving two new, weaker definitions of WOT for both models.

Definition 4 (Weak oblivious transfer, semi-honest model). *Let Π be a protocol between a sender and a receiver that outputs $(X_0, X_1) \in \{0,1\} \times \{0,1\}$ to the sender and $(C, Y) \in \{0,1\} \times \{0,1\}$ to the receiver. Let U be the view of the semi-honest sender, and let V be the view of the semi-honest receiver. Let $E := X_C \oplus Y$. Π implements (p,q,ε)-WOT in the semi-honest model, if*

- *(Correctness)* $\Pr[Y \neq X_C] \leq \varepsilon$.
- *(Security for the sender)* $\mathrm{PredAdv}(X_{1-C} \mid V, E) \leq q$.
- *(Security for the receiver)* $\mathrm{PredAdv}(C \mid U, E) \leq p$.

Since C and Y are part of V, (C, X_C, V) is a function of (V, E). Note that for the protocols we present here, it would be sufficient to require $\mathrm{PredAdv}(C \mid U) \leq p$ for the security for the receiver. We do not use this definition in order to get a stronger Theorem 6 that is easier to proof.

Definition 5 (Weak oblivious transfer, malicious model). *Let Π be a protocol between a sender and a receiver that outputs (X_0, X_1) to the sender and (C, Y) to the receiver. Π implements (p,q,ε)-WOT in the malicious model, if*

- *(Correctness)* $\Pr[Y \neq X_C] \leq \varepsilon$.
- (Security for the sender) *For an honest sender and any (malicious) receiver with output $\overline{V}$, there exists a $\overline{C}$, such that* $\mathrm{PredAdv}(X_{1-C} \mid \overline{C}, X_{\overline{C}}, \overline{V}) \leq q$.
- (Security for the receiver) *For an honest receiver and any (malicious) sender with output $\overline{U}$, we have* $\mathrm{PredAdv}(C \mid \overline{U}) \leq p$.

It is easy to see that in both models $(\varepsilon,\varepsilon,\varepsilon)$-WOT implies $\binom{2}{1}$-ROT^1 with an error of at most ε.

Besides the fact that we only consider a randomized version of WOT, our definitions of (p,q,ε)-WOT differ from the definitions used in [17] and [15] in the fact that we do not specify exactly what a malicious player may receive, but we only require that his output should not give too much information about X_{1-C} and C. This means that a malicious player may, for example, always receive whether an error occurred in the transmission or not, if that information is independent of the inputs. The most important difference is, however, that our definitions do not require that the error must occur independently of the event that a player gets side information, which is very important when we want to apply it. Note that our definitions still are quite close to the definitions from [17, 15], because there exist events with probability $1-p$ and $1-q$, such that if they occur, then the adversary does not get any side information.

In order to improve the achievable range of the reductions, *Generalized WOT* (GWOT) was introduced in [15]. Our weaker definitions of WOT imply that, at least for the moment, the usage of GWOT does not give any advantage over WOT.

Notice that the impossibility result, Lemma 1 in [17], only works for our weaker definitions of WOT.

5.1 Basic Protocols for WOT Amplification

To achieve $\binom{2}{1}$-OT^1 from (p, q, ε)-WOT, we will use the reductions R-Reduce, S-Reduce and E-Reduce. Protocol R-Reduce is used to reduce the parameter p, and Protocol S-Reduce is used to reduce the parameter q. Both protocols where already used in [12, 17, 15, 20], as well as in [22, 33] to build OT-combiners. It is easy to verify that these protocols are also secure when our definitions of (p, q, ε)-WOT is used. (Notice that R-Reduce and S-Reduce, as well as E-Reduce below, use a non-randomized WOT as input. Therefore, we have to apply first the protocol presented in [4, 2] that converts ROT into OT.)

Lemma 3 ([17]). *Protocol R-$\mathsf{Reduce}(n, \mathcal{W})$ implements a (p', q', ε')-WOT in the semi-honest and the malicious model out of n instances of (p, q, ε)-WOT, where $p' = 1 - (1 - p)^n \leq np$, $q' = q^n \leq e^{-n(1-q)}$, and $\varepsilon' = (1 - (1 - 2\varepsilon)^n)/2 \leq n\varepsilon$.*

Protocol S-$\mathsf{Reduce}(n, \mathcal{W})$ implements a (p', q', ε')-WOT in the semi-honest and the malicious model out of n instances of (p, q, ε)-WOT, where $p' = p^n \leq e^{-n(1-p)}$, $q' = 1 - (1 - q)^n \leq np$, and $\varepsilon' = (1 - (1 - 2\varepsilon)^n)/2 \leq n\varepsilon$.

Protocol E-Reduce was also used in [20] and is an one-way variant of Protocol E-Reduce presented in [17]. It is only secure in the semi-honest model.

Protocol E-$\mathsf{Reduce}(n, \mathcal{W})$
The sender has input $(x_0, x_1) \in \{0, 1\} \times \{0, 1\}$, and the receiver $c \in \{0, 1\}$.

1. They execute $\mathcal{W}$ n times, using x_0, x_1 and c as input in the ith execution. The receiver receives y_i.
2. The receiver outputs $y := \text{majority}(y_1, \ldots, y_n)$.

Lemma 4. *Protocol E-$\mathsf{Reduce}(n, \mathcal{W})$ implements (p', q', ε')-WOT in the semi-honest model out of n instances of (p, q, ε)-WOT, where $p' = 1 - (1 - p)^n \leq np$, $q' = 1 - (1 - q)^n \leq nq$ and $\varepsilon' = \sum_{i=\lceil n/2 \rceil}^{n} \binom{n}{i} \varepsilon^i (1 - \varepsilon)^{n-i} \leq e^{-2n(1/2-\varepsilon)^2}$.*

The proof of Lemma 4 is straightforward. The last inequality follows from the Chernoff-Hoeffding bound.

5.2 WOT Amplification for $\varepsilon = 0$

If $p, q > 0$, but $\varepsilon = 0$, we only need Protocols R-Reduce and S-Reduce. As they are the same as in [17], their result for this case also holds for our definitions. The bound is optimal. For a more detailed analysis, see [41].

Theorem 2 ([17]). *If $p + q \leq 1 - 1/\operatorname{poly}(k)$, then $(2^{-k}, 2^{-k}, 0)$-WOT can be efficiently implemented using $(p, q, 0)$-WOT secure in the semi-honest and the malicious model.*

5.3 WOT Amplification for $p = 0$ or $q = 0$

The special case where $\varepsilon > 0$, but either $p = 0$ or $q = 0$ has not been considered in [17]. There is a strong connection of this problem to the *one-way key-agreement problem* studied in [28], as well as to the *statistical distance polarization problem* studied in [37, 38]. We use the same protocol as Lemma 3.1.12 in [38].

Theorem 3. *For constant p, q, and ε with $p = 0 \;\wedge\; \sqrt{q} + 2\varepsilon < 1$ or $q = 0 \;\wedge\; \sqrt{p} + 2\varepsilon < 1$, $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently be implemented using (p, q, ε)-WOT secure in the semi-honest model.*

Proof. We will only show the theorem for $q = 0$. For $p = 0$ it is symmetric.

Let $\beta = p$, and $\alpha = 1 - 2\varepsilon$. Let $\lambda = \min(\alpha^2/\beta, 2)$, $\ell = \lceil \log_\lambda 4k \rceil$ and $m = \lambda^\ell/(2\alpha^{2\ell}) \le (\alpha^{2\ell}/\beta^\ell)/(2\alpha^{2\ell}) = 1/(2\beta^\ell)$. From $\sqrt{p} + 2\varepsilon < 1$ follows that $\beta < \alpha^2$ and hence, $1 < \lambda \le 2$. Notice that m is polynomial in k, since $\ell = O(\log k)$. We use the reductions $\mathcal{W}' = \mathsf{S\text{-}Reduce}(\ell, \mathcal{W})$, $\mathcal{W}'' = \mathsf{E\text{-}Reduce}(m, \mathcal{W}')$, and $\mathcal{W}''' = \mathsf{S\text{-}Reduce}(k, \mathcal{W}'')$. Since $\mathcal{W}$ is a $(\beta, 0, (1-\alpha)/2)$-WOT, $\mathcal{W}'$ is a $(\beta', 0, (1-\alpha')/2)$-$\mathsf{WOT}$, where $\beta' = \beta^\ell$ and $\alpha' = \alpha^\ell$. $\mathcal{W}''$ is a $(\beta'', 0, (1-\alpha'')/2)$-$\mathsf{WOT}$ with $\beta'' \le m\beta' \le 1/2$ and

$$\alpha'' \ge 1 - 2\exp\left(-\frac{\lambda^\ell}{2\alpha^{2\ell}} \cdot \frac{(\alpha^\ell)^2}{2}\right) = 1 - 2\exp\left(-\frac{\lambda^\ell}{4}\right) \ge 1 - 2e^{-k} \;.$$

Finally, $\mathcal{W}'''$ is a $(\beta''', 0, (1-\alpha''')/2)$-$\mathsf{WOT}$ with $\alpha''' \ge (1-2e^{-k})^k \ge 1 - 2ke^{-k} \ge 1 - 2^{-k}$ and $\beta''' \le 2^{-k}$, as long as k is sufficiently large, which can be achieved by artificially increasing k at the start. □

5.4 WOT Amplification for $p, q, \varepsilon > 0$

To find a good protocol for the general case is much harder. We start with the case where all values are smaller than 1/50.

Lemma 5. *In the semi-honest model, $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently and securely be implemented using $O(k^{2+\log(3)})$ instances of $(1/50, 1/50, 1/50)$-WOT.*

Proof. We iterate the reduction $\mathcal{W}' := \mathsf{S\text{-}Reduce}(2, \mathsf{R\text{-}Reduce}(2, \mathsf{E\text{-}Reduce}(3, \mathcal{W})))$ t times. In every iteration, we have $p' \le (2\cdot(3p))^2 = 36p^2$, $q' \le 2\cdot((3q)^2) = 18q^2$, and $\varepsilon' \le 2\cdot 2\cdot(3\varepsilon^2 - 2\varepsilon^3) \le 12\varepsilon^2$, from which follows that after t iterations, we have $\max(p', q', \varepsilon') \le (36/50)^{2^t}$. To achieve $\max(p', q', \varepsilon') \le 2^{-k}$, we choose $t := \lceil \log k/\log(50/36) \rceil \le \log(3\cdot k) + 1 = \log(6\cdot k)$. We need at most $12^t \le (6\cdot k)^{\log(12)} = O(k^{2+\log(3)})$ instances of $\mathcal{W}$. □

The following Lemma 6 is a corrected version of Lemma 5 in [17]. Since our Protocol $\mathsf{E\text{-}Reduce}$ is different, we are only able to achieve a smaller bound. As in [17], we obtain our bound using a simulation.

Let $l_i(p, q)$ be a function such that for all p, q and $\varepsilon < l_i(p, q)$, $\binom{2}{1}$-ROT^1 can be implemented using (p, q, ε)-WOT. Using $l_i(p, q)$, we define $l_{i+1}(p, q) := \max(S_\varepsilon^{-1}(l_i(S_p(p), S_q(q))), R_\varepsilon^{-1}(l_i(R_p(p), R_q(q))), E_\varepsilon^{-1}(l_i(E_p(p), E_q(q))))$, where

$S_p(p) := p^2$, $S_q(q) := 1-(1-q)^2$, $S_\varepsilon^{-1}(\varepsilon) := (1-\sqrt{1-2\varepsilon})/2$, $R_p(p) := 1-(1-p)^2$, $R_q(q) := q^2$, $R_\varepsilon^{-1}(\varepsilon) := (1-\sqrt{1-2\varepsilon})/2$, $E_p(p) := 1-(1-p)^3$, $E_q(q) := 1-(1-q)^3$, and $E_\varepsilon^{-1}(\varepsilon)$ is the inverse of $E_\varepsilon(\varepsilon) := 3\varepsilon - 2\varepsilon^3$.

Now for all p, q and $\varepsilon < l_{i+1}(p,q)$, $\binom{2}{1}$-ROT^1 can be implemented using (p,q,ε)-WOT, since one of the protocols $\mathsf{S\text{-}Reduce}(2,\mathcal{W})$, $\mathsf{R\text{-}Reduce}(2,\mathcal{W})$, or $\mathsf{E\text{-}Reduce}(3,\mathcal{W})$ achieves $\varepsilon' < l_i(p',q')$, from which we can achieve $\binom{2}{1}$-ROT^1.

From Lemma 5 follows that $l_0(p,q) := 0.02 - p - q$ satisfies our condition. Iterating 8 times, we get that for all p,q, $l_8(p,q) \geq (0.15 - p - q)/2$. Using $l'_0(p,q) := (0.15-p-q)/2$ and iterating 11 times, we get $l'_{11}(p,q)$. Since for all p,q we have $l'_{11}(p,q) \geq (0.24 - p - q)/2$, we get

Lemma 6. *If $p + q + 2\varepsilon \leq 0.24$, then $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently be implemented using (p,q,ε)-WOT secure in the semi-honest model.*

Often (p,q,ε)-WOT will be applied when one of the three values is big, while the others are small. We will now give bounds for these three cases.

Lemma 7. *If $p + 22q + 44\varepsilon < 1 - 1/\operatorname{poly}(k)$, then $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently be implemented using (p,q,ε)-WOT secure in the semi-honest model.*

Proof. We apply $\mathcal{W}' = \mathsf{S\text{-}Reduce}(n,\mathcal{W})$ for $n = \lceil \ln(20)/(1-p) \rceil$. From Lemmas 3 follows directly that we obtain a (p',q',ε')-WOT with $p' + q' + 2\varepsilon' \leq 0.24$. The lemma follows now from Lemma 6. $\square$

Lemma 8. *If $22p + q + 44\varepsilon < 1 - 1/\operatorname{poly}(k)$, then $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently be implemented using (p,q,ε)-WOT secure in the semi-honest model.*

Lemma 9. *If $7\sqrt{p+q} + 2\varepsilon < 1 - 1/\operatorname{poly}(k)$, then $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently be implemented using (p,q,ε)-WOT secure in the semi-honest model.*

Proof. We apply $\mathcal{W}' = \mathsf{E\text{-}Reduce}(n,\mathcal{W})$ for $n = \left\lceil \ln(50)/(2(\frac{1}{2}-\varepsilon)^2) \right\rceil$. From Lemma 4 follows directly that we obtain a (p',q',ε')-WOT with $p' + q' + 2\varepsilon' \leq 0.24$. The lemma follows now from Lemma 6. $\square$

Theorem 4. *If $p + q + 2\varepsilon \leq 0.24$, or $\min(p + 22q + 44\varepsilon, 22p + q + 44\varepsilon, 7\sqrt{p+q} + 2\varepsilon) \leq 1 - 1/\operatorname{poly}(k)$, then $(2^{-k}, 2^{-k}, 2^{-k})$-WOT can efficiently be implemented using (p,q,ε)-WOT secure in the semi-honest model.*

6 Computationally Secure Weak Oblivious Transfer

Even though the protocols from the last section are purely information-theoretic, we can also use them in the computational semi-honest model, as we will see in this section. The main tool to show this will be a *pseudo-randomness extraction theorem* (Theorem 5), that is a modified version of Theorem 7.3 from [27]. It is based on the *uniform hard-core lemma* from [26], which is a uniform variant of the hard-core lemma from [29].

6.1 Pseudo-Randomness Extraction

The main difference of Theorem 5 compared to the (implicit) extraction lemma in [24, 25] and the extraction lemma in [21] is that it allows the adversary to gain some additional knowledge during the extraction (expressed by the function Leak), which is needed for our application.

Besides a simplification, the main difference of our Theorem 5 to Theorem 7.3 from [27] is that we allow the functions Ext and Leak also to depend on the values Z_i. Intuitively, Theorem 5 says the following: if we have an information-theoretic protocol (modeled by the two functions Ext and Leak), that converts many instances of X over which an adversary having Z has only partial knowledge, into an X' over which the adversary has almost no knowledge, and if we have a computational protocol (modeled by the function $f(W)$ and the predicate $P(W)$), where an adversary having $f(W)$ has only partial *computational* knowledge about $P(W)$, then the modified information-theoretic protocol, where every instance of X is replaced with $P(W)$ and every instance of Z with $f(W)$, will produce a value over which the adversary has almost no computation knowledge.

Theorem 5 (Pseudo-Randomness Extraction Theorem, Modified Theorem 7.3 in [27]). *Let the functions $f : \{0,1\}^k \to \{0,1\}^\ell$, $P : \{0,1\}^k \to \{0,1\}$, and $\beta : \mathbb{N} \to [0,1]$ computable in time $\mathrm{poly}(k)$ be given. Assume that every polynomial time algorithm B satisfies*

$$\Pr[B(f(W)) = P(W)] \leq (1 + \beta(k))/2$$

for all but finitely many k, for a uniform random $W \in \{0,1\}^k$. Further, let also functions $n(k)$, $s(k)$,

$$\mathrm{Ext} : \{0,1\}^{\ell \cdot n} \times \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^t \;,$$
$$\mathrm{Leak} : \{0,1\}^{\ell \cdot n} \times \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^{t'} \;,$$

be given which are computable in time $\mathrm{poly}(k)$, and satisfy the following: for any distribution P_{XZ} over $\{0,1\} \times \{0,1\}^\ell$ where $\mathrm{PredAdv}(X \mid Z) \leq \beta(k)$, the output of $\mathrm{Ext}(Z^n, X^n, R)$ is $\varepsilon(k)$-close to uniform with respect to $\mathrm{Leak}(Z^n, X^n, R)$ (where $R \in \{0,1\}^s$ is chosen uniformly at random). Then, no polynomial time algorithm A, which gets as input

$$\mathrm{Leak}((f(w_1), \ldots, f(w_n)), (P(w_1), \ldots, P(w_n)), R) \;,$$

(where $(w_1, \ldots, w_n)$ are chosen uniformly at random) distinguishes

$$\mathrm{Ext}((f(w_1), \ldots, f(w_n)), (P(w_1), \ldots, P(w_n)), R)$$

from a uniform random string of length t with advantage $\varepsilon(k) + \gamma(k)$, for any non-negligible function $\gamma(k)$.

The proof of Theorem 5 is very similar to the proof of Theorem 7.3 in [27] and can be found in the appendix. Note that our proof makes an additional step that has been missing in the proof of Theorem 7.3 in [27].

6.2 Computational-WOT Amplification

We will denote the computational version of (p, q, ε)-WOT by (p, q, ε)-$\mathsf{compWOT}$. The difference to the information-theoretic definition is that now we require the algorithms that guess X_{1-C} or C to be efficient, i.e., to run in polynomial time.

Definition 6 (Computationally secure weak oblivious transfer, semi-honest model). *Let functions $\varepsilon : \mathbb{N} \to [0, 1/2]$, $p : \mathbb{N} \to [0, 1]$, and $q : \mathbb{N} \to [0, 1]$ computable in time* $\text{poly}(k)$ *be given. Let Π be a protocol between a sender and a receiver. On input 1^k, Π outputs $(X_0, X_1) \in \{0, 1\} \times \{0, 1\}$ to the sender and $(C, Y) \in \{0, 1\} \times \{0, 1\}$ to the receiver. Let U be the view of a semi-honest sender, and let V be the view of a semi-honest receiver. Let $E := X_C \oplus Y$. Π implements $(p(k), q(k), \varepsilon(k))$-compWOT in the semi-honest model, if*

- (Efficiency) *Π can be executed in time* $\text{poly}(k)$.
- (Correctness) $\Pr[Y \neq X_C] \leq \varepsilon(k)$ *for all k.*
- (Security for the sender) *All polynomial time algorithms A satisfy*

$$\Pr[A(V, E) = X_{1-C}] \leq (1 + q(k))/2$$

  for all but finitely many k.
- (Security for the receiver) *All polynomial time algorithms A satisfy*

$$\Pr[A(U, E) = C] \leq (1 + p(k))/2$$

  for all but finitely many k.

We apply Theorem 5 twice to get Theorem 6, which says that if we have a protocol that implements (p, q, ε)-$\mathsf{compWOT}$, and an efficient information-theoretic protocol that implements $\binom{2}{1}$-ROT^1 from (p, q, ε)-WOT secure in the semi-honest model, then we can construct a protocol that implements $\binom{2}{1}$-ROT^1 computationally secure in the semi-honest model.

Theorem 6. *Let the functions $\varepsilon(k)$, $p(k)$, and $q(k)$ computable in time* $\text{poly}(k)$ *be given. Let a protocol Π achieve (p, q, ε)-compWOT and let an efficient information-theoretic protocol Π' be given which takes 1^k as input and implements $(2^{-k}, 2^{-k}, 2^{-k})$-WOT from (p, q, ε)-WOT secure in the semi-honest model. Then, protocol Π', where every instance of (p, q, ε)-WOT is replaced by an independent outcome of Π, implements $\binom{2}{1}$-ROT^1 computationally secure in the semi-honest model.*

Proof. Let $W = (W_\mathsf{S}, W_\mathsf{R})$ be the randomness used in Π by the sender and the receiver, and let Z be the communication. (X_0, X_1) and (C, Y) are the output to the honest sender and receiver, respectively. $U = (X_0, X_1, Z, W_\mathsf{S})$ and $V = (C, Y, Z, W_\mathsf{R})$ are the views of the semi-honest sender and receiver, respectively. Let $E := Y \oplus X_C$. Note that all these values are functions of W.

In the protocol Π', the sender receives $(X_0, X_1)^n$, which are her output from the n independent instances of Π, and the receiver receives $(C, Y)^n$. The sender outputs (X_0^*, X_1^*) and the receiver (C^*, Y^*). Let $R = (R_{\mathsf{S}}, R_{\mathsf{R}})$ be the randomness used in Π' by both players, and let Z' be the communication produced by Π'. $V^* = (E^*, C^*, Y^*, V^n, Z', R_{\mathsf{R}})$ is the view of the semi-honest receiver after the execution of Π', and $U^* = (E^*, X_0^*, X_1^*, U^n, Z', R_{\mathsf{S}})$ the view of the semi-honest sender. Let $E^* := Y^* \oplus X_{C^*}^*$. Note that the values E^*, X_0^*, X_1^*, C^*, Y^*, V^*, U^* and Z' are functions of $((X_0, X_1, C, Y)^n, R)$.

First of all, the resulting protocol will be correct and efficient, as every outcome of Π satisfies $\Pr[Y \neq X_C] \leq \varepsilon$.

For the security of the sender, we define the following functions: let $f(W) := (V, E)$ and $P(W) := X_{1-C}$. Since $X_C = E \oplus Y$, it is possible to simulate the protocol Π' using the values $(V,E)^n$, $(X_{1-C})^n$, and R. Therefore, we can define $\mathrm{Ext}((V,E)^n, (X_{1-C})^n, R) := X_{1-C^*}^*$ and $\mathrm{Leak}((V,E)^n, (X_{1-C})^n, R) := V^*$. Since Π' implements $(\mathrm{negl}(k), \mathrm{negl}(k), \mathrm{negl}(k))$-$\mathsf{WOT}$, the functions Ext and Leak satisfy the extraction requirements from Theorem 5 with $\varepsilon(k) = \mathrm{negl}(k)$. Furthermore, Ext and Leak can be computed efficiently, since the protocol Π' is efficient. From the security condition of $\mathsf{compWOT}$ follows that every polynomial-time algorithm B satisfies $\Pr[B(f(W)) = P(W)] \leq (1 + q(k))/2$ for all but finitely many k, for W chosen uniformly at random. Theorem 5 tells us that no polynomial time algorithm A, which gets as input $\mathrm{Leak}((V,E)^n, (X_{1-C})^n, R)$, distinguishes $\mathrm{Ext}((V,E)^n, (X_{1-C})^n, R)$ from a uniform random bit with advantage $\mathrm{negl}(k) + \gamma(k)$, for any non-negligible function $\gamma(k)$, from which follows that the protocol is computationally secure for the sender.

For the security of the receiver, we define the following functions: let $f(W) := (U, E)$ and $P(W) := C$. Since $X_C = E \oplus Y$, it is possible to simulate the protocol Π' using the values $(U,E)^n$, C^n, and R. Therefore, we can define $\mathrm{Ext}((U,E)^n, C^n, R) := C^*$, and $\mathrm{Leak}((U,E)^n, C^n, R) := U^*$. Since Π' implements $(\mathrm{negl}(k), \mathrm{negl}(k), \mathrm{negl}(k))$-$\mathsf{WOT}$, the functions Ext and Leak satisfy the extraction requirements from Theorem 5 with $\varepsilon(k) = \mathrm{negl}(k)$. Furthermore, Ext and Leak can be computed efficiently, since the protocol Π' is efficient. From the security condition of $\mathsf{compWOT}$ follows that every polynomial time algorithm A satisfies $\Pr[A(f(W)) = P(W)] \leq (1 + p(k))/2$ for all but finitely many k, for W chosen uniformly at random. Theorem 5 tells us that no polynomial time algorithm B, which gets as input $\mathrm{Leak}((U,E)^n, C^n, R)$, distinguishes $\mathrm{Ext}((U,E)^n, C^n, R)$ from a uniform random bit with advantage $\mathrm{negl}(k) + \gamma(k)$, for any non-negligible function $\gamma(k)$, from which follows that the protocol is computationally secure for the receiver. □

Together with the information-theoretic protocols presented in Section 5, (Theorems 2, 3 and 4) we get a way to implement ROT based on compWOT, computationally secure in the semi-honest model. From [31] follows that such a protocol implies one-way functions. Using the compiler from [19], we get an implementation of OT computationally secure in the malicious model. The following corollary follows.

Corollary 1. *Let the functions $\varepsilon(k)$, $p(k)$, and $q(k)$ computable in time* $\mathrm{poly}(k)$ *be given, such that either for all k $\varepsilon = 0 \wedge p + q < 1 - 1/\mathrm{poly}(k)$ or $p + q + 2\varepsilon \leq$*

0.24 *or* $\min(p + 22q + 44\varepsilon, 22p + q + 44\varepsilon, 7\sqrt{p+q} + 2\varepsilon) < 1 - 1/\operatorname{poly}(k)$*, or, for constant functions* $p(k)$*,* $q(k)$ *and* $\varepsilon(k)$*,* $(p = 0) \wedge (\sqrt{q} + 2\varepsilon < 1)$ *or* $(q = 0) \wedge (\sqrt{p} + 2\varepsilon < 1)$*. If there exists a protocol* Π *that achieve* (p, q, ε)*-compWOT computationally secure in the semi-honest model, then there exists a protocol that implements* $\binom{2}{1}$*-OT*^{1} *computationally secure in the malicious model.*

Corollary 1 generalizes results from [20], because it covers a much wider range of values for p, q, and ε, and it allows the security for both players to be only computational.

Acknowledgments

I would like to thank Thomas Holenstein and Stefan Wolf for helpful discussions, and Ivan Damgård and Louis Salvail for answering my questions about their work. I also thank Serge Fehr, Iftach Haitner, Melanie Raemy, Christian Schaffner and anonymous referees for giving helpful comments on this work.

I was supported by the Swiss National Science Foundation (SNF).

References

1. D. Beaver. Foundations of secure interactive computing. In *Advances in Cryptology — CRYPTO '91*, volume 1233 of *LNCS*, pages 377–391. Springer-Verlag, 1992.
2. D. Beaver. Precomputing oblivious transfer. In *Advances in Cryptology — EUROCRYPT '95*, volume 963 of *LNCS*, pages 97–109. Springer-Verlag, 1995.
3. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41, 1995.
4. C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology — CRYPTO '91*, volume 576 of *LNCS*, pages 351–366. Springer, 1992.
5. C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.
6. G. Brassard and C. Crépeau. Oblivious transfers and privacy amplification. In *Advances in Cryptology — EUROCRYPT '97*, volume 1233 of *LNCS*, pages 334–347. Springer-Verlag, 1997.
7. G. Brassard, C. Crépeau, and S. Wolf. Oblivious transfers and privacy amplification. *Journal of Cryptology*, 16(4):219–237, 2003.
8. C. Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology — EUROCRYPT '98*, volume 1403 of *LNCS*, pages 361–374. Springer-Verlag, 1998.
9. R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.
10. J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.
11. C. Crépeau. Efficient cryptographic protocols based on noisy channels. In *Advances in Cryptology — CRYPTO '97*, volume 1233 of *LNCS*, pages 306–317. Springer-Verlag, 1997.
12. 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.

13. 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 *LNCS*, pages 47–59. Springer-Verlag, 2004.
14. C. Crépeau, G. Savvides, C. Schaffner, and J. Wullschleger. Information-theoretic conditions for two-party secure function evaluation. In *Advances in Cryptology — EUROCRYPT '06*, volume 4004 of *LNCS*, pages 538–554. Springer-Verlag, 2006. Full version available at http://eprint.iacr.org/2006/183.
15. 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 *LNCS*, pages 355–373. Springer-Verlag, 2004.
16. I. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS '05)*, pages 449–458. IEEE Computer Society, 2005.
17. 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 *LNCS*, pages 56–73. Springer-Verlag, 1999.
18. S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.
19. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '87)*, pages 218–229. ACM Press, 1987.
20. I. Haitner. Implementing oblivious transfer using collection of dense trapdoor permutations. In *Theory of Cryptography Conference — TCC '04*, volume 2951 of *LNCS*, pages 394–409. Springer-Verlag, 2004.
21. I. Haitner, D. Harnik, and O. Reingold. On the power of the randomized iterate. In *Advances in Cryptology — CRYPTO '06*, volume 4117 of *LNCS*, pages 21–40. Springer-Verlag, 2006.
22. D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen. On robust combiners for oblivious transfer and other primitives. In *Advances in Cryptology — EUROCRYPT '05*, volume 3494 of *LNCS*, pages 96–113, 2005.
23. D. Harnik, M. Naor, O. Reingold, and A. Rosen. Completeness in two-party secure computation: a computational view. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC '04)*, pages 252–261. ACM Press, 2004.
24. J. Håstad. Pseudo-random generators under uniform assumptions. In *Proceedings of the 22st Annual ACM Symposium on Theory of Computing (STOC '90)*, pages 395–404. ACM Press, 1990.
25. J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.
26. T. Holenstein. Key agreement from weak bit agreement. In *Proceedings of the 37th ACM Symposium on Theory of Computing (STOC '05)*, pages 664–673. ACM Press, 2005.
27. T. Holenstein. *Strengthening key agreement using hard-core sets*. PhD thesis, ETH Zurich, Switzerland, 2006. Reprint as vol. 7 of *ETH Series in Information Security and Cryptography*, Hartung-Gorre Verlag.
28. T. Holenstein and R. Renner. One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption. In *Advances*

in Cryptology — CRYPTO '05, volume 3621 of *LNCS*, pages 478–493. Springer-Verlag, 2005.
29. R. Impagliazzo. Hard-core distributions for somewhat hard problems. In *Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science (FOCS '95)*, pages 538–545. IEEE Computer Society, 1995.
30. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89)*, pages 12–24. ACM Press, 1989.
31. R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science (FOCS '89)*, pages 230–235, 1989.
32. 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.
33. R. Meier, B. Przydatek, and J. Wullschleger. Robuster combiners for oblivious transfer. In *Theory of Cryptography Conference — TCC '07*, LNCS. Springer-Verlag, 2007.
34. S. Micali and P. Rogaway. Secure computation (abstract). In *Advances in Cryptology — CRYPTO '91*, volume 576 of *LNCS*, pages 392–404. Springer-Verlag, 1992.
35. 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.
36. M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
37. A. Sahai and S. Vadhan. Manipulating statistical difference. In *Randomization Methods in Algorithm Design (DIMACS Workshop '97)*, volume 43 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 251–270. American Mathematical Society, 1999.
38. S. Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, Massachusets Institute of Technology, USA, 1999.
39. S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.
40. S. Wolf and J. Wullschleger. Zero-error information and applications in cryptography. In *Proceedings of 2004 IEEE Information Theory Workshop (ITW '04)*, 2004.
41. J. Wullschleger. *Oblivious-Transfer Amplification*. PhD thesis, ETH Zurich, Switzerland, 2007.
42. 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 Appendix

Proof (Theorem 5). Let us assume there exists an algorithm A that contradicts our assumption. To be able to apply the uniform hard-core lemma, Theorem 6.8 in [27], we will use A to construct an oracle algorithm $\overline{A}^{\chi_{\mathcal{S}}}$[2] for which the fol-

[2] $A^{(\cdot)}$ has oracle access to the *characteristic function* $\chi_{\mathcal{S}}$ of the set $\mathcal{S}$, which is defined as $\chi_{\mathcal{S}}(w) := 1$ if $w \in \mathcal{S}$ and $\chi_{\mathcal{S}}(w) := 0$ otherwise.

lowing holds. For any set $\mathcal{S} \subseteq \{0,1\}^k$ with $|\mathcal{S}| \geq (1-\beta(k))2^k$, we have

$$\Pr[\overline{A}^{\chi_{\mathcal{S}}}(f(W)) = P(W)] \geq (1+\gamma')/2$$

for a non-negligible function γ', where the expectation is over the randomness of $\overline{A}^{\chi_{\mathcal{S}}}$, W is chosen uniformly at random from $\{0,1\}^k$, and $\overline{A}^{\chi_{\mathcal{S}}}$ calls $\chi_{\mathcal{S}}$ only with queries which are computed independently of the input. For any fixed $j \in \{0,\ldots,n\}$ and any fixed set $\mathcal{S} \subseteq \{0,1\}^k$ with $|\mathcal{S}| \geq (1-\beta)2^k$, we define the following values. For all $i \in \{0,\ldots,n-1\}$, we choose $w_i \in \{0,1\}^k$ and $u_i \in \{0,1\}$ uniformly at random. Then we compute

$$y_i := \begin{cases} P(w_i) & \text{if } i \geq j \text{ or } w_i \notin \mathcal{S} \ , \\ u_i & \text{otherwise} \ , \end{cases} \tag{A.1}$$

$$e_j := \mathrm{Ext}((f(w_1),\ldots,f(w_n)), y^n, r) \ , \quad \text{and} \tag{A.2}$$

$$\ell_j := \mathrm{Leak}((f(w_1),\ldots,f(w_n)), y^n, r) \ , \tag{A.3}$$

where $r \in \{0,1\}^s$ is chosen uniformly at random.

Let $P_{E_j L_j}$ be the distribution of (e_j, ℓ_j). From our assumption follows that

$$\mathrm{Adv}^A((E_0, L_0), (U, L_0)) \geq \varepsilon + \gamma \ ,$$

where $U \in \{0,1\}^t$ is chosen uniformly at random. On the other hand, for $j = n$, with probability $1-\beta$ (over the choice of w_i) we have $y_i = u_i$, and therefore, by Lemma 2.2 in [27], $\mathrm{PredAdv}(Y_i \mid f(W_i)) \leq \beta$. The information-theoretic requirement on the functions Ext and Leak imply that E_n is ε-close to uniform with respect to L_n and therefore

$$\mathrm{Adv}^A((E_n, L_n), (U, L_n)) \leq \varepsilon \ .$$

The triangle inequality implies

$$\mathrm{Adv}^A((E_0, L_0), (E_n, L_n)) + \mathrm{Adv}^A((U, L_0), (U, L_n)) \geq \gamma \ .$$

It follows that at least one of the four inequalities $\Pr[A(E_0, L_0) = 1] - \Pr[A(E_n, L_n) = 1] \geq \gamma/2$, $\Pr[A(E_n, L_n) = 1] - \Pr[A(E_0, L_0) = 1] \geq \gamma/2$, $\Pr[A(U, L_0) = 1] - \Pr[A(U, L_n) = 1] \geq \gamma/2$, or $\Pr[A(U, L_n) = 1] - \Pr[A(U, L_0) = 1] \geq \gamma/2$ holds for infinitely many k, from which follows that there exists an algorithm A' such that

$$\Pr[A'(E_0, L_0) = 1] - \Pr[A'(E_n, L_n) = 1] \geq \gamma/2$$

for infinitely many k. For $J \in \{0,\ldots,n-1\}$ chosen uniformly at random, we have

$$\Pr[A'(E_J, L_J) = 1] - \Pr[A'(E_{J+1}, L_{J+1}) = 1] \geq \gamma/(2n)$$

for infinitely many k. We can now give an implementation of a distinguisher which distinguishes $(f(W), P(W))$ from $(f(W), U)$ with advantage $\gamma/(2n)$ for infinitely many k, if W is chosen uniformly from $\mathcal{S}$ and U is a uniform random bit, as long as oracle access to $\chi_{\mathcal{S}}$ is given. Let $(f(w), b)$ be the input to the distinguisher. It chooses $j \in \{0, \ldots, n-1\}$, and for all $i \in \{0, \ldots, n-1\}$ the values $w_i \in \{0,1\}^k$ and $u_i \in \{0,1\}$ uniformly at random. Then, for all $i \in \{0, \ldots, n-1\}$, it computes the values $f(w_i)$, $P(w_i)$ and y_i as in (A.1). If $w_j \in \mathcal{S}$, it replaces $f(w_j)$ with $f(w)$ and y_i with b. Then, it computes e_j and ℓ_j as in (A.2) and (A.3). If b is a uniform bit, then this process gives random variables (E_j, L_j) distributed according to $P_{E_{j+1}L_{j+1}}$, otherwise it gives random variables distributed according to $P_{E_j L_j}$. Therefore, A' distinguishes $(f(W), P(W))$ from $(f(W), U)$ with advantage $\gamma/(2n)$ for infinitely many k, if W is chosen uniformly at random from $\mathcal{S}$. From Lemma 7.2 in [27] follows that there exists a polynomial time algorithm that predicts $P(W)$ from $f(W)$, where W is chosen uniformly at random from $\{0,1\}^k$, with probability at least $1/2+\gamma/(2n)$ for infinitely many k. We can now apply the uniform hard-core lemma, Theorem 6.8 in [27], to obtain the statement. □