Oblivious Transfer and Linear Functions

Ivan B. Damgård[1], Serge Fehr[2*], Louis Salvail[1], and Christian Schaffner[1**]

[1] BRICS, FICS, Aarhus University, Denmark
{ivan|salvail|chris}@brics.dk
[2] CWI Amsterdam, The Netherlands
fehr@cwi.nl

Abstract. We study unconditionally secure 1-out-of-2 Oblivious Transfer (*1-2 OT*). We first point out that a standard security requirement for *1-2 OT* of bits, namely that the receiver only learns one of the bits sent, holds if and only if the receiver has no information on the XOR of the two bits. We then generalize this to *1-2 OT* of strings and show that the security can be characterized in terms of binary linear functions. More precisely, we show that the receiver learns only one of the two strings sent if and only if he has no information on the result of applying any binary linear function (which non-trivially depends on both inputs) to the two strings.

We then argue that this result not only gives new insight into the nature of *1-2 OT*, but it in particular provides a very powerful tool for analyzing *1-2 OT* protocols. We demonstrate this by showing that with our characterization at hand, the reducibility of *1-2 OT* (of strings) to a wide range of weaker primitives follows by a very simple argument. This is in sharp contrast to previous literature, where reductions of *1-2 OT* to weaker flavors have rather complicated and sometimes even incorrect proofs.

1 Introduction

1-2 Oblivious-Transfer, *1-2 OT* for short, is a two-party primitive which allows a sender to send two bits (or, more generally, strings) B_0 and B_1 to a receiver, who is allowed to learn one of the two according his choice C. Informally, it is required that the receiver only learns B_C but not B_{1-C} (*obliviousness*), while at the same time the sender does not learn C (*privacy*). *1-2 OT* was introduced in [28] (under the name of "multiplexing") in the context of quantum cryptography, and, inspired by [25] where a different flavor was introduced, later re-discovered in [19].

1-2 OT turned out to be very powerful in that it was shown to be sufficient for secure general two-party computation [22]. On the other hand, it is quite easy to see that unconditionally secure *1-2 OT* is not possible without any assumption. Even with the help of quantum communication and computation, unconditionally secure *1-2 OT* remains impossible [23, 24]. As a consequence, much effort

* Supported by the Dutch Organization for Scientific Research (NWO).
** Supported by the EC-Integrated Project SECOQC, No: FP6-2002-IST-1-506813.

has been put into constructing unconditionally secure protocols for *1-2 OT* using physical assumptions like (various models for) noisy channels [8, 16, 12, 9], or a memory bounded adversary [6, 17, 18]. Similarly, much effort has been put into reducing *1-2 OT* to (seemingly) weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, etc. [7, 3, 5, 29, 4, 10].

In this work, we focus on a slightly modified notion of *1-2 OT*, which we call *Randomized 1-2 OT*, *Rand 1-2 OT* for short, where the bits (or strings) B_0 and B_1 are not *in*put by the sender, but generated uniformly at random during the *Rand 1-2 OT* and then *out*put to the sender. It is still required that the receiver only learns the bit (or string) of his choice, B_C, whereas the sender does not learn any information on C. It is obvious that a *Rand 1-2 OT* can easily be turned into an ordinary *1-2 OT* simply by using the generated B_0 and B_1 to mask the actual input bits (or strings). Furthermore, all known constructions of unconditionally secure *1-2 OT* protocols make (implicitly) the detour via a *Rand 1-2 OT*.

In a first step, we observe that the obliviousness condition of a *Rand 1-2 OT* of *bits* is equivalent to requiring the XOR $B_0 \oplus B_1$ to be (close to) uniformly distributed from the receiver's point of view. The proof is very simple, and it is kind of surprising that (to the best of our knowledge) this has not been realized before. We then ask and answer the question whether there is a natural generalization of this result to *Rand 1-2 OT* of *strings*. Note that requiring the bitwise XOR of the two strings to be uniformly distributed is obviously not sufficient. We show that the obliviousness condition for *Rand 1-2 OT* of strings can be characterized in terms of *non-degenerate linear functions* (bivariate binary linear functions which non-trivially depend on both arguments, as defined in Definition 2): obliviousness holds if and only if the result of applying any non-degenerate linear function to the two strings is (close to) uniformly distributed from the receiver's point of view.

We then show the usefulness of this new understanding of *1-2 OT*. We demonstrate this on the problem of reducing *1-2 OT* to weaker primitives. Concretely, we show that the reducibility of an (ordinary) *1-2 OT* to weaker flavors via a non-interactive reduction follows by a trivial argument from our characterization of the obliviousness condition. This is in sharp contrast to the current literature: The proofs given in [3, 29, 4] for reducing *1-2 OT* to *1-2 XOT*, *1-2 GOT* and *1-2 UOT* (we refer to Section 5 for a description of these flavors of *OT*) are rather complicated and tailored to a particular class of privacy-amplifying hash functions; whether the reductions also work for a less restricted class is left as an open problem [4, page 222]. And, the proof given in [5] for reducing *1-2 OT* to one execution of a general *UOT* is not only complicated, but also incorrect, as we will point out. Thus, our characterization of the obliviousness condition allows to simplify existing reducibility proofs (and, along the way, to solve the open problem posed in [4], as well as to improve the reduction parameters in most cases), but it also allows for new (respectively until now only incorrectly proven) reductions. Furthermore, our techniques are useful for the construction and analysis of *1-2 OT* protocols in other settings, for instance in the bounded quantum-storage model [13].

2 Notation

Let P and Q be two probability distributions over the same domain $\mathcal{X}$. The *variational distance* $\delta\big(P,Q\big)$ is defined as $\delta\big(P,Q\big) := \frac{1}{2}\sum_{x\in\mathcal{X}} \big|P(x) - Q(x)\big|$. Note that this definition makes sense also for *non-normalized* distributions, and indeed we define and use $\delta\big(P,Q\big)$ for arbitrary positive-valued functions P and Q with common domain. In case $\mathcal{X}$ is of the form $\mathcal{X} = \mathcal{U} \times \mathcal{V}$, we can expand $\delta\big(P,Q\big)$ to $\delta\big(P,Q\big) = \sum_u \delta\big(P(u,\cdot),Q(u,\cdot)\big) = \sum_v \delta\big(P(\cdot,v),Q(\cdot,v)\big)$. We write $P \approx_\varepsilon Q$ to denote that P and Q are ε-close, i.e., that $\delta\big(P,Q\big) \leq \varepsilon$.

For a random variable X it is common to denote its distribution by P_X. We adopt this notation. Alternatively, we also write $[X]$ for the distribution P_X of X. For two random variables X and Y, whereas $[XY]$ naturally denotes the joint distribution P_{XY}, we write $[X][Y]$ to denote the independent distribution $P_{XY} : (x,y) \mapsto P_X(x)P_Y(y)$. Using this notation, X and Y are (close to) *independent* if and only if $[XY] = [X][Y]$ (respectively $[XY] \approx_\varepsilon [X][Y]$). We feel that this notation is sometimes easier to read as it refrains from putting the crucial information into the subscript.

By $\textsc{unif}$ we denote a uniformly distributed binary random variable (independent of anything else), such that $P_{\textsc{unif}}(b) = \frac{1}{2}$ for both $b \in \{0,1\}$, and $\textsc{unif}^\ell$ stands for ℓ independent copies of $\textsc{unif}$.

3 Defining *1-2 OT*

3.1 (Randomized) *1-2 OT* of Bits

Formally capturing the intuitive understanding of the security of *1-2 OT* is a non-trivial task. We adopt the security definition of [11], where it is argued that this definition is the "right" way to define unconditionally secure *1-2 OT*. In their model, a secure *1-2 OT* protocol is as good as an ideal *1-2 OT* functionality.

In this paper, we will mainly focus on a slight modification of *1-2 OT*, which we call *Randomized 1-2 OT* (although *Sender*-randomized *1-2 OT* would be a more appropriate, but also rather lengthy name). A Randomized *1-2 OT*, or *Rand 1-2 OT* for short, essentially coincides with an (ordinary) *1-2 OT*, except that the two bits B_0 and B_1 are not *input* by the sender but generated uniformly at random during the protocol and *output* to the sender. This is formalized in Definition 1 below.

There are two main justifications for focusing on *Rand 1-2 OT*. First, an ordinary *1-2 OT* can easily be constructed from a *Rand 1-2 OT*: the sender can use the randomly generated B_0 and B_1 to one-time-pad encrypt his input bits for the *1-2 OT*, and send the masked bits to the receiver (as first realized in [1]). For a formal proof of this we refer to the full version of [11].[1] And second, all information-theoretically secure constructions of *1-2 OT* protocols we are aware

[1] The definition of *Rand 1-2 OT* in [11] differs syntactically slightly from our Definition 1, in particular in that it involves an auxiliary input Z, but it is not too hard to see that the two definitions are equivalent. We discuss this in more detail in [15].

of in fact do implicitly build a *Rand 1-2 OT* and use the above reduction to achieve *1-2 OT*.

We formalize *Rand 1-2 OT* in such a way that it minimizes and simplifies as much as possible the security restraints, while at the same time remaining sufficient for *1-2 OT*.

Definition 1 (*Rand 1-2 OT*). *An ε-secure Rand 1-2 OT is a protocol between sender S and receiver R, with R having input $C \in \{0,1\}$ (while S has no input), such that for any distribution of C, the following properties hold:*

- *ε-Correctness: For honest S and R, S has output $B_0, B_1 \in \{0,1\}$ and R has output B_C, except with probability ε.*
- *ε-Privacy: For honest R and any (dishonest) $\tilde{\mathsf{S}}$ with output[2] V, $[CV] \approx_\varepsilon [C][V]$.*
- *ε-Obliviousness: For honest S and any (dishonest) $\tilde{\mathsf{R}}$ with output W, there exists a binary random variable D such that $[B_{1-D}\, W\, B_D\, D] \approx_\varepsilon [\textsc{unif}][W\, B_D\, D]$.*

The privacy condition simply says that $\tilde{\mathsf{S}}$ learns no information on C, and obliviousness requires that there exists a choice bit D (supposed to be C) such that when given the choice bit D and the corresponding bit B_D, then the other bit B_{1-D} is independent and random from $\tilde{\mathsf{R}}$'s point of view.

3.2 (Randomized) *1-2 OT* of Strings

In a *1-2 String OT* the sender inputs two *strings* (of the same length), and the receiver is allowed to learn one of the two and only one of the two. Formally, for any positive integer ℓ, *1-2 OT*$^\ell$ and *Rand 1-2 OT*$^\ell$ can be defined along the same lines as *1-2 OT* and *Rand 1-2 OT* of *bits*; for instance for *Rand 1-2 OT*$^\ell$ the binary random variables B_0 and B_1 (as well as $\textsc{unif}$) in Definition 1 are simply replaced by random variables S_0 and S_1 (and $\textsc{unif}^\ell$) with range $\{0,1\}^\ell$.

4 Characterizing Obliviousness

4.1 The Case of Bit *OT*

It is well known (and it follows from the obliviousness condition) that in a (*Rand*) *1-2 OT* the receiver R should in particular learn (essentially) no information on the XOR $B_0 \oplus B_1$ of the two bits. The following proposition shows that this is not only necessary for the obliviousness condition but also *sufficient*.

Theorem 1. *The ε-obliviousness condition for a Rand 1-2 OT is satisfied for a particular (possibly dishonest) receiver $\tilde{\mathsf{R}}$ with output W if and only if*

$$[(B_0 \oplus B_1)W] \approx_\varepsilon [\textsc{unif}][W]\,.$$

[2] Note that $\tilde{\mathsf{S}}$'s output V may consist of $\tilde{\mathsf{S}}$'s complete view on the protocol.

Before going into the proof (which is surprisingly simple), consider the following example. Assume a candidate protocol for *Rand 1-2 OT* and a dishonest receiver $\tilde{\mathsf{R}}$ which is able to output $W = 0$ if $B_0 = 0 = B_1$, $W = 1$ if $B_0 = 1 = B_1$ and $W = 0$ or 1 with probability 1/2 each in case $B_0 \neq B_1$. Then, it is easy to see that conditioned on, say, $W = 0$, (B_0, B_1) is $(0,0)$ with probability $\frac{1}{2}$, and $(0,1)$ and $(1,0)$ each with probability $\frac{1}{4}$, such that the condition on the XOR from Theorem 1 is satisfied. On the other hand, neither B_0 nor B_1 is uniformly distributed (conditioned on $W = 0$), and it appears as if the receiver has some joint information on B_0 and B_1 which is forbidden by a (*Rand*) *1-2 OT*. But that is not so. Indeed, the same view can be obtained when attacking an *ideal Rand 1-2 OT*: submit a random bit C to obtain B_C and output $W = B_C$. And in the light of Definition 1, if $W = 0$ we can split the event $(B_0, B_1) = (0,0)$ into two disjoint subsets (subevents) $\mathcal{E}_0$ and $\mathcal{E}_1$ such that each has probability $\frac{1}{4}$, and we define D by setting $D = 0$ if $\mathcal{E}_0$ or $(B_0, B_1) = (0,1)$, and $D = 1$ if $\mathcal{E}_1$ or $(B_0, B_1) = (1,0)$. Then, obviously, conditioned on $D = d$, the bit B_{1-d} is uniformly distributed, even when given B_d. The corresponding holds if $W = 1$.

Proof. The "only if" implication is well known and straightforward. For the "if" implication, we first argue the perfect case where $[(B_0 \oplus B_1) W] = [\text{UNIF}][W]$. For any value w with $P_W(w) > 0$, the non-normalized distribution $P_{B_0 B_1 W}(\cdot,\cdot,w)$ can be expressed as depicted in the left table of Figure 1, where we write a for $P_{B_0 B_1 W}(0,0,w)$, b for $P_{B_0 B_1 W}(0,1,w)$, c for $P_{B_0 B_1 W}(1,0,w)$ and d for $P_{B_0 B_1 W}(1,1,w)$. Note that $a+b+c+d = P_W(w)$ and, by assumption, $a+d = b+c$. Due to symmetry, we may assume that $a \leq b$. We can then define D by extending $P_{B_0 B_1 W}(\cdot,\cdot,w)$ to $P_{B_0 B_1 D W}(\cdot,\cdot,\cdot,w)$ as depicted in the right two tables in Figure 1: $P_{B_0 B_1 D W}(0,0,0,w) = P_{B_0 B_1 D W}(0,1,0,w) = a$, $P_{B_0 B_1 D W}(1,0,0,w) = P_{B_0 B_1 D W}(1,1,0,w) = c$ etc. Important to realize is that $P_{B_0 B_1 D W}(\cdot,\cdot,\cdot,w)$ is indeed a valid extension since by assumption $c + (b-a) = d$.

a	b
c	d

$P_{B_0 B_1 W}(\cdot,\cdot,w)$

a	a
c	c

$P_{B_0 B_1 D W}(\cdot,\cdot,0,w)$

0	$b-a$
0	$b-a$

$P_{B_0 B_1 D W}(\cdot,\cdot,1,w)$

Fig. 1. Distributions $P_{B_0 B_1 W}(\cdot,\cdot,w)$ and $P_{B_0 B_1 D W}(\cdot,\cdot,\cdot,w)$

It is now obvious that $P_{B_0 B_1 D W}(\cdot,\cdot,0,w) = \frac{1}{2} P_{B_0 D W}(\cdot,0,w)$ as well as $P_{B_0 B_1 D W}(\cdot,\cdot,1,w) = \frac{1}{2} P_{B_1 D W}(\cdot,1,w)$. This finishes the perfect case.

Concerning the general case, the idea is the same as above, except that one has to take some care regarding the error parameter $\varepsilon \geq 0$. As this does not give any new insight, and we anyway state and fully prove a more general result in Theorem 2, we skip this part of the proof.[3] $\square$

[3] Although the special case $\ell = 1$ in Theorem 2 is quantitatively slightly weaker than Theorem 1.

4.2 The Case of String *OT*

The obvious question after the previous section is whether there is a natural generalization of Theorem 1 to *1-2* OT^ℓ for $\ell \geq 2$. Note that the straightforward generalization of the XOR-condition in Theorem 1, requiring that any receiver has no information on the bit-wise XOR of the two strings, is clearly too weak, and does not imply the obliviousness condition for *Rand 1-2* OT^ℓ: for instance the receiver could know the first half of the first string and the second half of the second string.

The Characterization. Let ℓ be an arbitrary positive integer.

Definition 2. *A function* $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ *is called a* non-degenerate linear function *(NDLF) if it is of the form* $\beta : (s_0, s_1) \mapsto \langle a_0, s_0\rangle \oplus \langle a_1, s_1\rangle$ *for two non-zero* $a_0, a_1 \in \{0,1\}^\ell$*, i.e., if it is linear and non-trivially depends on both input strings.*

In case $\ell = 1$, the XOR is a NDLF, and it is the *only* NDLF. Based on this notion, the obliviousness condition of *Rand 1-2* OT^ℓ can be characterized as follows.

Theorem 2. *The* ε*-obliviousness condition for a Rand 1-2* OT^ℓ *is satisfied for a particular (possibly dishonest) receiver* $\tilde{\mathsf{R}}$ *with output* W *if*

$$[\beta(S_0, S_1)W] \approx_{\varepsilon/2^{2\ell+1}} [\text{UNIF}][W]$$

for every NDLF β*, and, on the other hand, the* ε*-obliviousness condition may be satisfied only if* $[\beta(S_0, S_1)W] \approx_\varepsilon [\text{UNIF}][W]$ *for every NDLF* β*.*

Note that the number of NDLFs is exponential in ℓ, namely $(2^\ell - 1)^2$. Nevertheless, we show in Section 5 that this characterization turns out to be very useful. There, we will also argue that an exponential overhead (in ℓ) in the sufficient condition is unavoidable. The proof of Theorem 2 also shows that the set of NDLFs forms a minimal set of functions among all sets that imply obliviousness. In this sense, our characterization is tight.

We would like to point out that Theorem 4 in [4] also provides a tool to analyze the obliviousness condition of *1-2 OT* protocols in terms of linear functions; however, the condition that needs to be satisfied is much stronger than for our Theorem 2: it additionally requires that one of the two strings is *a priori* uniformly distributed (from the receiver's point of view).[4] This difference is crucial, because showing that one of the two strings is uniform (conditioned on the receiver's view) is usually technically involved and sometimes not even possible, as the example given after Theorem 1 shows. This is also demonstrated by the fact that the analysis in [4] of the considered *1-2 OT* protocol is tailored to one particular class of privacy-amplifying hash functions, and it is stated as

[4] Concretely, it is additionally required that every non-trivial parity of that string is uniform, but by the XOR-Lemma this is equivalent to the whole string being uniform.

an open problem how to prove their construction secure when a different class of hash functions is used. The condition for Theorem 2, on the other hand, is naturally satisfied for typical constructions of *1-2 OT* protocols, as we shall see in Section 5. As a result, Theorem 2 allows for much simpler and more elegant security proofs for *1-2 OT* protocols, and, as a by-product, allows to solve the open problem from [4]. We explain this in detail in Section 5, and the interested reader may well jump ahead and save the proof of Theorem 2 for later.

The proof for the "only if" part of Theorem 2 is given in the full version of this paper [15]; in fact, a slightly stronger statement is shown, namely that the ε-obliviousness condition implies $[\beta(S_0, S_1)W] \approx_\varepsilon [\text{UNIF}][W]$ for any *2-balanced* function (as defined in [15]). The "if" part, which is the interesting direction, is proven below.

Proof of Theorem 2 ("if" part). First, we consider the perfect case: if $[\beta(S_0, S_1)W]$ *equals* $[\text{UNIF}][W]$ for every NDLF β, then the obliviousness condition for *Rand 1-2 OT*$^\ell$ holds (perfectly).

THE PERFECT CASE: As the case $\ell = 1$ is already settled, we assume that $\ell \geq 2$.

Fix an arbitrary output w of the receiver, and consider the non-normalized probability distribution $P_{S_0S_1W}(\cdot, \cdot, w)$. We use the variable p_{s_0,s_1} to refer to $P_{S_0S_1W}(s_0, s_1, w)$, and we write $\mathbf{o}$ for the all-zero string $(0, \ldots, 0) \in \{0,1\}^\ell$. We assume that $p_{\mathbf{o},\mathbf{o}} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^\ell$; we show later that we may do so. We extend this distribution to $P_{S_0S_1DW}(\cdot, \cdot, \cdot, w)$ by setting

$$P_{S_0S_1DW}(s_0, s_1, 0, w) = p_{s_0,\mathbf{o}} \quad \text{and} \quad P_{S_0S_1DW}(s_0, s_1, 1, w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}} \tag{1}$$

for any strings $s_0, s_1 \in \{0,1\}^\ell$, and we collect the equations resulting from the condition that $P_{S_0S_1W}(\cdot, \cdot, w) = P_{S_0S_1DW}(\cdot, \cdot, 0, w) + P_{S_0S_1DW}(\cdot, \cdot, 1, w)$ needs to be satisfied: for any two $s_0, s_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$

$$p_{s_0,\mathbf{o}} + p_{\mathbf{o},s_1} = p_{\mathbf{o},\mathbf{o}} + p_{s_0,s_1} \, . \tag{2}$$

If all these equations do hold (for any w) then as in the case of $\ell = 1$, the random variable D is well defined and $[S_{1-D}\, S_D\, W\, D] = [\text{UNIF}^\ell][S_D\, W\, D]$ holds, since $P_{S_0S_1DW}(s_0, s_1, 0, w)$ does not depend on s_1 and $P_{S_0S_1DW}(s_0, s_1, 1, w)$ not on s_0.

Before moving on, we first justify the assumption that $p_{\mathbf{o},\mathbf{o}} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^\ell$. In general, we choose $t \in \{0,1\}^\ell$ such that $p_{\mathbf{o},t} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^\ell$, and we set $P_{S_0S_1DW}(s_0, s_1, 0, w) = p_{s_0,t}$ and $P_{S_0S_1DW}(s_0, s_1, 1, w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},t}$, resulting in the equations $p_{s_0,t} + p_{\mathbf{o},s_1} = p_{\mathbf{o},t} + p_{s_0,s_1}$ for $s_0 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$ and $s_1 \in \{0,1\}^\ell \setminus \{t\}$. However, these equations follow from the equations given by (2): subtract equation (2) with s_1 replaced by t from equation (2). Therefore, it suffices to focus on the equations given by (2).

We proceed by showing that the equations provided by the assumed uniformity of $\beta(S_0, S_1)$ for any β imply the equations given by (2). Consider an arbitrary pair $a_0, a_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$ and let β be the associated NDLF, i.e., such that $\beta(s_0, s_1) = \langle a_0, s_0\rangle \oplus \langle a_1, s_1\rangle$. By assumption, $\beta(S_0, S_1)$ is uniformly distributed, independent of W. Thus, for any fixed w, and writing p_{s_0,s_1} for $P_{S_0S_1W}(s_0, s_1, w)$, this can be expressed as

$$\sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle = \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} = \sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle \neq \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} , \tag{3}$$

where both summations are over all $\sigma_0, \sigma_1 \in \{0,1\}^\ell$ subject to the indicated respective properties. Recall, that this equality holds for any pair $a_0, a_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$. Thus, for fixed $s_0, s_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$, if we add up over all such pairs a_0, a_1 subject to $\langle a_0, s_0\rangle = \langle a_1, s_1\rangle = 1$, we get the equation

$$\sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1}} \sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle = \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} = \sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1}} \sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle \neq \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} ,$$

which, after re-arranging the terms of the summations, leads to

$$\sum_{\sigma_0,\sigma_1} \sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1 \\ \langle a_0,\sigma_0\rangle = \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} = \sum_{\sigma_0,\sigma_1} \sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1 \\ \langle a_0,\sigma_0\rangle \neq \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} . \tag{4}$$

We are now going to argue that, up to a constant multiplicative factor, equation (4) coincides with equation (2).

First, it is straightforward to verify that the variables $p_{\mathbf{o},\mathbf{o}}$ and p_{s_0,s_1} occur only on the left hand side, both with multiplicity $2^{2(\ell-1)}$ (the number of pairs a_0, a_1 such that $\langle a_0, s_0\rangle = \langle a_1, s_1\rangle = 1$), whereas $p_{s_0,\mathbf{o}}$ and $p_{\mathbf{o},s_1}$ only occur on the right hand side, with the same multiplicity $2^{2(\ell-1)}$.

Now, we argue that any other p_{σ_0,σ_1} equally often appears on the right and on the left hand side, and thus vanishes from the equation. Note that the set of pairs a_0, a_1, over which the summation runs on the left respectively the right hand side, can be understood as the set of solutions to a binary (non-homogeneous) linear equations system:

$$\begin{pmatrix} s_0 & 0 \\ 0 & s_1 \\ \sigma_0 & \sigma_1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \text{ respectively } \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} .$$

Also note that the two linear equation systems consist of three equations and involve at least 4 variables (as $a_0, a_1 \in \{0,1\}^\ell$ and $\ell \geq 2$). Therefore, using basic linear algebra, one is tempted to conclude that they both have solutions, and, because they have the same homogeneous part, they have the same number of solutions (equal to the number of homogeneous solutions). However, this is only guaranteed if the matrix defining the homogeneous part has full rank. But here this is precisely the case if and only if $(\sigma_0, \sigma_1) \notin \{(\mathbf{o},\mathbf{o}), (s_0,\mathbf{o}), (\mathbf{o}, s_1), (s_0, s_1)\}$, where those four exceptions have already been treated above.

It follows that the equations (3), which are guaranteed by assumption, imply the equations (2). This concludes the proof for the perfect case.

THE GENERAL CASE: Now, we consider the general case where there exists some $\varepsilon > 0$ such that $\delta\big([\beta(S_0,S_1)W],[\text{UNIF}][W]\big) \le 2^{-2\ell-1}\varepsilon$ for any NDLF β. We use the observations from the perfect case, but additionally we keep track of the "error term".

For any w with $P_W(w) > 0$ and any NDLF β, set

$$\varepsilon_{w,\beta} = \delta\big(P_{\beta(S_0,S_1)W}(\cdot,w), P_{\text{UNIF}}P_W(w)\big)\,.$$

Note that $\sum_w \varepsilon_{w,\beta} = \delta\big([\beta(S_0,S_1)W],[\text{UNIF}][W]\big) \le 2^{-2\ell-1}\varepsilon$, independent of β. Fix now an arbitrary w with $P_W(w) > 0$. Then, (3) only holds up to an error of $2\varepsilon_{w,\beta}$, where β is the NDLF associated to a_0, a_1. As a consequence, equation (4) only holds up to an error of $2\sum_\beta \varepsilon_{w,\beta}$ and thus (2) holds up to an error of $\delta_{s_0,s_1} = \frac{2}{2^{2\ell-2}}\sum_\beta \varepsilon_{w,\beta}$, where the sum is over the $2^{2\ell-2}$ functions associated to the pairs a_0, a_1 with $\langle a_0, s_0\rangle = \langle a_1, s_1\rangle = 1$. Note that δ_{s_0,s_1} depends on w, but the set of β's, over which the summation runs, does not. Adding up over all possible w's gives

$$\sum_w \delta_{s_0,s_1} = \frac{2}{2^{2\ell-2}}\sum_w\sum_\beta \varepsilon_{w,\beta} = \frac{2}{2^{2\ell-2}}\sum_\beta\sum_w \varepsilon_{w,\beta} \le 2^{-2\ell}\varepsilon\,.$$

Since (2) only holds approximately, $P_{S_0S_1DW}$ as in (1) is not necessarily a valid extension, but close. This can obviously be overcome by instead setting

$$P_{S_0S_1DW}(s_0,s_1,0,w) = p_{s_0,\mathbf{o}} \pm \delta'_{s_0,s_1} \text{ and } P_{S_0S_1DW}(s_0,s_1,1,w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}} \pm \delta''_{s_0,s_1}$$

with suitably chosen $\delta'_{s_0,s_1}, \delta''_{s_0,s_1} \ge 0$ with $\delta'_{s_0,s_1} + \delta''_{s_0,s_1} = \delta_{s_0,s_1}$, and with suitably chosen signs "+" or "−".[5] Using that every $P_{S_0S_1DW}(s_0,s_1,0,w)$ differs from $p_{s_0,\mathbf{o}}$ by at most δ'_{s_0,s_1}, it follows from a straightforward computation that $\delta\big(P_{S_{1-D}S_DDW}(\cdot,\cdot,0,w), P_{\text{UNIF}}P_{S_DDW}(\cdot,0,w)\big) \le \sum_{s_0,s_1}\delta'_{s_0,s_1}$. The corresponding holds for $P_{S_0S_1DW}(\cdot,\cdot,1,w)$. It follows that

$$\delta\big(P_{S_{1-D}S_DWD}, P_{\text{UNIF}}P_{S_DWD}\big) \le \sum_w\sum_{s_0,s_1}(\delta'_{s_0,s_1} + \delta''_{s_0,s_1}) = \sum_{s_0,s_1}\sum_w \delta_{s_0,s_1} \le \varepsilon$$

which concludes the proof. □

5 Applications

In this section we will show the usefulness of Theorem 2 for the construction of *1-2 OT*$^\ell$, based on weaker primitives (like a noisy channel, a quantum uncertainty relation or other flavors of OT). In particular, we will show that the reducibility of *1-2 OT* to any weaker flavor of OT follows as a simple argument using Theorem 2.

[5] Most of the time, it probably suffices to correct one of the two, say, choose $\delta'_{s_0,s_1} = \delta_{s_0,s_1}$ and $\delta''_{s_0,s_1} = 0$; however, if for instance $p_{s_0,\mathbf{o}}$ and $p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}}$ are both positive but $P_{S_0S_1W}(s_0,s_1,w) = 0$, then one has to correct both.

5.1 Reducing *1-2* OT^ℓ to Independent Repetitions of Weak *1-2* OT's

Background. A great deal of effort has been put into constructing protocols for *1-2* OT^ℓ based on physical assumptions like (various models for) noisy channels [8, 16, 12, 9] or a memory bounded adversary [6, 17, 18], as well as into reducing *1-2* OT^ℓ to (seemingly) weaker flavors of OT, like *Rabin* OT, *1-2* XOT, *1-2* GOT and *1-2* UOT [7, 3, 5, 29, 4, 10]. Note that the latter three flavors of OT are weaker than *1-2* OT in that the (dishonest) receiver has more freedom in choosing the sort of information he wants to get about the sender's input bits B_0 and B_1: B_0, B_1 or $B_0 \oplus B_1$ in case of *1-2* XOT, $g(B_0, B_1)$ for an arbitrary one-bit-output function g in case of *1-2* GOT, and an arbitrary (probabilistic) Y with mutual information $I(B_0B_1; Y) \leq 1$ in case of *1-2* UOT.[6]

All these reductions of *1-2* OT to weaker versions follow a specific construction design (which is also at the core of the *1-2* OT protocols based on noisy channels or a memory-bounded adversary). By repeated (independent) executions of the underlying primitive, S transfers a randomly chosen bit string $X = (X_0, X_1) \in \{0,1\}^n \times \{0,1\}^n$ to R such that: (1) depending on his choice bit C, the honest R knows either X_0 or X_1, (2) any $\tilde{\mathsf{S}}$ has no information on which part of X R learned, and (3) any $\tilde{\mathsf{R}}$ has some uncertainty in X. Then, this is completed to a *Rand 1-2* OT by means of privacy amplification [2]: S samples two functions f_0 and f_1 from a universal-two class $\mathcal{F}$ of hash functions, sends them to R, and outputs $S_0 = f_0(X_0)$ and $S_1 = f_1(X_1)$, and R outputs $S_C = f_C(X_C)$. Finally, the *Rand 1-2* OT is transformed into an ordinary *1-2* OT in the obvious way.

Correctness and privacy of this construction are clear, they follow immediately from (1) and (2). How easy or hard it is to prove obliviousness depends heavily on the underlying primitive. In case of *Rabin* OT it is rather straightforward. In case of *1-2* XOT and the other weaker versions, this is non-trivial. The problem is that since R might know $X_0 \oplus X_1$, it is not possible to argue that there exists $d \in \{0,1\}$ such that R's uncertainty on X_{1-d} is large when given X_d. This, though, would be necessary in order to finish the proof by simply applying the privacy amplification theorem [2]. This difficulty is overcome in [3, 4] by tailoring the proof to a particular universal-two class of hash functions (namely the class of all *linear* hash functions). Whether the reduction also works for a less restricted class of hash functions is left in [3, 4] as an open problem, which we solve here as a side result. Using a smaller class of hash functions would allow for instance to reduce the communication complexity of the protocol.

In [10], the difficulty is overcome by giving up on the simplicity of the reduction. The cost of two-way communication allowing for interactive hashing

[6] As a matter of fact, reducibility has been proven for any bound on $I(B_0B_1; Y)$ strictly smaller than 2. Note that there is some confusion in the literature in what a *universal* OT, UOT, should be: In [3, 29, 4], a UOT takes as input two *bits* and the receiver is doomed to have at least one bit (or any other non-trivial amount) of *Shannon* entropy on them; we denote this by *1-2* UOT. Whereas in [5], a UOT takes as input two *strings* and the receiver is doomed to have some *Renyi* entropy on them. We address this latter notion in more detail in Section 5.2.

is traded for better reduction parameters. We would like to emphasize that these parameters are incomparable to ours, because a different reduction is used, whereas our approach provides a *better analysis* of the non-interactive reductions.

The New Approach. We argue that, independent of the underlying primitive, obliviousness follows as a simple consequence of Theorem 2, in combination with a straightforward observation regarding the composition of NDLFs with strongly universal-two hash functions (Proposition 1 below). Recall that a class $\mathcal{F}$ of hash functions from, say, $\{0,1\}^n$ to $\{0,1\}^\ell$ is *strongly universal-two* [27] if for any distinct $x, x' \in \{0,1\}^n$ the two random variables $F(x)$ and $F(x')$ are independent and uniformly distributed (over $\{0,1\}^\ell$), where the random variable F represents the random choice of a function in $\mathcal{F}$.

Proposition 1. *Let $\mathcal{F}_0$ and $\mathcal{F}_1$ be two classes of strongly universal-two hash functions from $\{0,1\}^{n_0}$ respectively $\{0,1\}^{n_1}$ to $\{0,1\}^\ell$, and let β be a fixed NDLF $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$. Consider the class $\mathcal{F}$ of all composed functions $f : \{0,1\}^{n_0} \times \{0,1\}^{n_1} \to \{0,1\}$ with $f(x_0, x_1) = \beta(f_0(x_0), f_1(x_1))$ where $f_0 \in \mathcal{F}_0$ and $f_1 \in \mathcal{F}_1$. Then, $\mathcal{F}$ is strongly universal-two.*

The proof is straightforward; for completeness, it is given in the full version [15].[7]

Now, briefly, obliviousness for a construction as sketched above can be argued as follows. The only restriction is that $\mathcal{F}$ needs to be *strongly* universal-two. From the independent repetitions of the underlying weak *OT* (*Rabin OT*, *1-2 XOT*, *1-2 GOT* or *1-2 UOT*) it follows that $\tilde{\mathsf{R}}$ has "high" collision entropy in X. Hence, for any NDLF β, we can apply the privacy amplification theorem [2] (respectively the version given in Appendix A) to the (strongly) universal-two hash function $\beta(f_0(\cdot), f_1(\cdot))$ and argue that $\beta(f_0(X_0), f_1(X_1))$ is close to uniform for randomly chosen f_0 and f_1. Obliviousness then follows immediately from Theorem 2.

We save the quantitative analysis (Theorem 3) for next section, where we consider a reduction of *1-2 OT* to the weakest kind of *OT*: to *one* execution of a *UOT*. Based on this, we compare in Appendix B the quality of the analysis of the above reductions based on Theorem 2 with the results in [4]. It turns out that our analysis is tighter for *1-2 GOT* and *1-2 UOT*, whereas the analysis in [4] is tighter for *1-2 XOT*; but in all cases, our analysis is much simpler and, we believe, more elegant.

5.2 Reducing *1-2* OT^ℓ to One Execution of *UOT*

We assume the reader to be somewhat familiar with the notion of *Renyi entropy* H_α of order α. Definition and some elementary properties needed in this section are given in Appendix A. We also refer to Appendix A for the slightly non-standard notion of *average conditional* Renyi entropy $H_\alpha(X|Y)$ we are using.

[7] The claim does not hold in general for ordinary (as opposed to strongly) universal-two classes: if $n_0 = n_1 = \ell$ and $\mathcal{F}_0$ and $\mathcal{F}_1$ both only contain the identity function $id : \{0,1\}^\ell \to \{0,1\}^\ell$ (and thus are universal-two), then $\mathcal{F}$ consisting of the function $f(x_0, x_1) = \beta(id(x_0), id(x_1)) = \beta(x_0, x_1)$ is not universal-two.

Universal Oblivious Transfer. Probably the weakest flavor of OT is the *Universal* OT (UOT) as it was introduced in [5], in that it gives the receiver the most freedom in getting information on the string X. Formally, for a finite set $\mathcal{X}$ and parameters $\alpha \geq 0$ (allowing $\alpha = \infty$) and $r > 0$, an (α, r)-$UOT(\mathcal{X})$ works as follows. The sender inputs $x \in \mathcal{X}$, and the receiver may choose an arbitrary conditional probability distribution $P_{Y|X}$ with the only restriction that for a uniformly distributed X it must satisfy $H_\alpha(X|Y) \geq r$.[8] The receiver then gets as output y, sampled according to the distribution $P_{Y|X}(\cdot|x)$, whereas the sender gets no information on the receiver's choice for $P_{Y|X}$. Note that a *1-2 UOT* is a special case of this kind of UOT since "*1-2 UOT* $= (1,1)$-$UOT(\{0,1\}^2)$".

The crucial property of such an UOT is that the input is not restricted to two bits, but may be two bit-*strings*; this potentially allows to reduce *1-2 OT* to *one* execution of a UOT, rather than to many independent executions of the same primitive as for the 1-2 flavors of OT mentioned above. Indeed, following the design principle discussed in Section 5.1, it is straightforward to come up with a candidate protocol for *1-2* OT^ℓ which uses *one* execution of a (α, r)-$UOT(\mathcal{X})$ with $\mathcal{X} = \{0,1\}^n \times \{0,1\}^n$. The protocol is given in Figure 2, where $\mathcal{F}$ is a (strongly) universal-two class of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$.

OT2UOT(c):
1. S and R run (α, r)-$UOT(\mathcal{X})$: S inputs a random $x = (x_0, x_1) \in \mathcal{X} = \{0,1\}^n \times \{0,1\}^n$, R inputs $P_{Y|X}$ with $P_{Y|X}(x'_c|(x'_0, x'_1)) = 1$ for any (x'_0, x'_1), and as a result R obtains $y = x_c$.
2. S samples independent random $f_0, f_1 \in \mathcal{F}$, sends f_0 and f_1 to R, and outputs $s_0 = f_0(x_0)$ and $s_1 = f_1(x_1)$.
3. R computes and outputs $s_c = f_c(y)$.

Fig. 2. Protocol *OT2UOT* for *Rand1-2* OT^ℓ.

In [5] it is claimed that, for appropriate parameters, protocol *OT2UOT* is a secure *Rand 1-2* OT^ℓ (respectively, the resulting protocol for *1-2 OT* is secure). However, we argue below that the proof given is not correct (and it is not obvious how to fix it). In Theorem 3 we then show that its security follows easily from Theorem 2.

A Flaw in the Security Proof. In [5] the security of protocol *OT2UOT* is argued as follows. Using (rather complicated) *spoiling-knowledge techniques*, it is shown that, conditioned on the receiver's output (which we suppress to simplify the notation) at least one out of $H_\infty(X_0)$ and $H_\infty(X_1|X_0 = x_0)$ is "large" (for any x_0), and, similarly, at least one out of $H_\infty(X_1)$ and $H_\infty(X_0|X_1 = x_1)$. Since collision entropy is lower bounded by min-entropy, it then follows from the privacy amplification theorem that at least one out of $H(F_0(X_0)|F_0)$ and

[8] This notion of UOT is even slightly weaker than what is considered in [5], where $H_\alpha(X|Y = y) \geq r$ for all y is required.

$H(F_1(X_1)|F_1, X_0{=}x_0)$ is close to ℓ, and similarly, one out of $H(F_1(X_1)|F_1)$ and $H(F_0(X_0)|F_0, X_1{=}x_1)$. It is then claimed that this proves *OT2UOT* secure.

We argue that this very last implication is not correct. Indeed, what is proven about the entropy of $F_0(X_0)$ and $F_1(X_1)$ does not exclude the possibility that both entropies $H(F_0(X_0)|F_0)$ and $H(F_1(X_1)|F_1)$ are maximal, but that $H(F_0(X_0) \oplus F_1(X_1)|F_0, F_1) = 0$. This would allow the receiver to learn the (bitwise) XOR $S_0 \oplus S_1$, which is clearly forbidden by the obliviousness condition.

Also note that the proof does not use the fact that the two functions F_0 and F_1 are chosen *independently*. However, if they are chosen to be the same, then the protocol is clearly insecure: if the receiver asks for $Y = X_0 \oplus X_1$, and if $\mathcal{F}$ is a class of *linear* universal-two hash functions, then $\tilde{\mathsf{R}}$ obviously learns $S_0 \oplus S_1$.

Reducing *1-2 OT*$^\ell$ to *UOT*. The following theorem guarantees the security of *OT2UOT* (for an appropriate choice of the parameters). The only restriction we have to make is that $\mathcal{F}$ needs to be a *strongly* universal-two class of hash function.

Theorem 3. *Let $\mathcal{F}$ be a* strongly *universal-two class of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$. Then OT2UOT reduces a $2^{-\kappa}$-secure Rand 1-2 OT$^\ell$ to a (perfect) $(2, r)$-UOT$(\{0,1\}^{2n})$ with $n \geq r \geq 4\ell + 3\kappa + 4$.*

Using the bounds from Lemma 2 (in Appendix A) on the different orders of Renyi entropy, the reducibility of *1-2 OT*$^\ell$ to (α, r)-*UOT*$(\mathcal{X})$ follows immediately for *any* $\alpha > 1$.

Informally, obliviousness for protocol *OT2UOT* is argued as for the reduction of *1-2 OT* to *Rabin OT*, *1-2 XOT* etc., discussed in Section 5.1, simply by using Proposition 1 in combination with the privacy amplification theorem, and applying Theorem 2. The formal proof given in Appendix C additionally keeps track of the "error term". From this proof it also becomes clear that the exponential (in ℓ) overhead in Theorem 2 is unavoidable. Indeed, a sub-exponential overhead would allow ℓ in Theorem 3 to be super-linear (in n), which of course is nonsense.

6 Generalizations and Further Applications

The general technique described in this section also comes in handy in a quantum setting. The fact that we do not need to know *how* the entropy is distributed over X is fundamental to prove secure a protocol for *1-2 OT*$^\ell$ in the bounded quantum-storage model as introduced in [14]. In upcoming work [13], we present a protocol for *Rand 1-2 OT* for which we can use a quantum uncertainty relation to show a lower bound on the min-entropy of the $2n$-bit string X transmitted by the sender using a quantum encoding. We prove a quantum version of Theorem 2 which enables us to use the result about privacy amplification against quantum adversaries [26] to conclude that our protocol is oblivious against adversaries with bounded quantum memory. This application motivates further the use of (strongly) universal-two hashing, because up to date, no other means of privacy amplification have been shown secure against quantum adversaries.

In [15], we show that it is also possible to generalize Theorem 2 to *1-n OT*: it then states that the condition for *Rand 1-n OT* is satisfied if for any NDLF β and for any $0 \leq i < j \leq n-1$ it holds that $\beta(S_i, S_i)$ is (essentially) uniform, conditioned on the receiver's output W and on all S_k with $k \neq i, j$. This comes in handy for the construction and analysis of *1-n OT* schemes, as demonstrated in [13], where also *1-n OT* schemes in the bounded quantum-storage model are considered.

7 Conclusion

We have established a characterization of the obliviousness condition for (a slightly modified version of) *1-2* OT^ℓ (Theorem 2). Using this characterization in combination with a composition result about strongly universal-two hash functions (Proposition 1), it follows by a very simple argument that when starting with a $2n$-bit string X with enough (collision) entropy, arbitrarily splitting up X into two n-bit strings X_0, X_1 followed by strongly universal-two hashing yields obliviousness as required by a *1-2 OT*. This allows for easy analyses whenever this design principle is used or can be applied, like reductions of *1-2* OT^ℓ to weaker flavors, or *1-2* OT^ℓ in the bounded (quantum) storage model, but possibly also in other contexts like in a computational setting when unconditional obliviousness is required.

Acknowledgments

We would like to thank Renato Renner for bringing up the idea of characterizing obliviousness in terms of the XOR, and Jürg Wullschleger for observing that our earlier results, which were expressed in terms of balanced functions, can also be expressed in terms of NDLFs. We are also grateful to Claude Crépeau and George Savvides for enlightening discussions regarding the formal definition of *1-2 OT*.

References

1. D. Beaver. Precomputing oblivious transfer. In *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*. Springer, 1995.
2. C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6), 1995.
3. G. Brassard and C. Crépeau. Oblivious transfers and privacy amplification. In *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*. Springer, 1997.
4. G. Brassard, C. Crépeau, and S. Wolf. Oblivious transfer and privacy amplification. *Journal of Cryptology*, 16(4), 2003.

5. C. Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology—EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*. Springer, 1998.
6. C. Cachin, C. Crépeau, and J. Marcil. Oblivious transfer with a memory-bounded receiver. In *39th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 493–502, 1998.
7. C. Crépeau. Equivalence between two flavours of oblivious transfers. In *Advances in Cryptology—CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*. Springer, 1987.
8. C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 1988.
9. C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In *International Conference on Security in Communication Networks (SCN)*, volume 4 of *Lecture Notes in Computer Science*, 2004.
10. C. Crépeau and G. Savvides. Optimal reductions between oblivious transfers using interactive hashing. In *Advances in Cryptology—EUROCRYPT '06*, Lecture Notes in Computer Science. Springer, 2006.
11. C. Crépeau, G. Savvides, C. Schaffner, and J. Wullschleger. Information-theoretic conditions for two-party secure function evaluation. In *Advances in Cryptology—EUROCRYPT '06*, Lecture Notes in Computer Science. Springer, 2006. Full version: `http://eprint.iacr.org`.
12. I. B. Damgård, S. Fehr, K. Morozov, and L. Salvail. Unfair noisy channels and oblivious transfer. In *Theory of Cryptography Conference (TCC)*, volume 2951 of *Lecture Notes in Computer Science*. Springer, 2004.
13. I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic uncertainty relation with applications in the bounded quantum-storage model. In preparation, 2006.
14. I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2005.
15. I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Oblivious transfer and linear functions (full version). Available at `http://eprint.iacr.org/2005/349`, 2006.
16. I. B. 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*. Springer, 1999.
17. Y. Z. Ding. Oblivious transfer in the bounded storage model. In *Advances in Cryptology—CRYPTO '01*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.
18. Y. Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel. Constant-round oblivious transfer in the bounded storage model. In *Theory of Cryptography Conference (TCC)*, volume 2951 of *Lecture Notes in Computer Science*, pages 446–472. Springer, 2004.
19. S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*. Plenum Press, 1982.
20. J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4), 1999.
21. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *21st Annual ACM Symposium on Theory of Computing (STOC)*, 1989.

22. J. Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, 1988.
23. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997.
24. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997.
25. M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
26. R. Renner and R. Koenig. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005. Also available at `http://arxiv.org/abs/quant-ph/0403133`.
27. M. N. Wegman and J. L. Carter. New classes and applications of hash functions. In *20th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 1979.
28. S. Wiesner. Conjugate coding. *ACM Special Interest Group on Automata and Computability Theory (SIGACT News)*, 15, 1983. Original manuscript written circa 1970.
29. S. Wolf. Reducing oblivious string transfer to universal oblivious transfer. In *IEEE International Symposium on Information Theory (ISIT)*, 2000.

A (Conditional) Renyi Entropy

Let $\alpha \geq 0$, $\alpha \neq 1$. The *Renyi entropy of order* α of a random variable X with distribution P_X is defined as

$$H_\alpha(X) = \frac{1}{1-\alpha} \log\Big(\sum_x P_X(x)^\alpha\Big) = -\log\Big(\big(\sum_x P_X(x)^\alpha\big)^{\frac{1}{\alpha-1}}\Big).$$

The limit for $\alpha \to 1$ is the *Shannon entropy* $H(X) = -\log\big(\sum_x P_X(x)\, \log P_X(x)\big)$ and the limit for $\alpha \to \infty$ the *min-entropy* $H_\infty(X) = -\log\big(\max_x P_X(x)\big)$. Another important special case is the case $\alpha = 2$, also known as *collision entropy* $H_2(X) = -\log\big(\sum_x P_X(x)^2\big)$.

The *conditional* Renyi entropy $H_\alpha(X|Y = y)$ for two random variables X and Y is naturally defined as $H_\alpha(X|Y=y) = \frac{1}{1-\alpha} \log\big(\sum_x P_{X|Y}(x|y)^\alpha\big)$. Furthermore, in the literature $H_\alpha(X|Y)$ is often defined as $\sum_y P_Y(y)\, H_\alpha(X|Y=y)$, like for Shannon entropy. However, for our purpose, a slightly different definition will be useful. For $1 < \alpha < \infty$, we define the *average conditional* Renyi entropy $H_\alpha(X|Y)$ as

$$H_\alpha(X|Y) = -\log\Big(\sum_y P_Y(y)\big(\sum_x P_{X|Y}(x|y)^\alpha\big)^{\frac{1}{\alpha-1}}\Big),$$

and as $H_\infty(X|Y) = -\log\big(\sum_y P_Y(y) \max_x P_{X|Y}(x|y)\big)$ for $\alpha = \infty$. This notion is useful in particular because it has the property that if the *average* conditional Renyi entropy is large, then the conditional Renyi entropy is large with high probability:

Lemma 1. *Let $\alpha > 1$ (allowing $\alpha = \infty$) and $t \geq 0$. Then with probability at least $1 - 2^{-t}$ (over the choice of y) $H_\alpha(X|Y{=}y) \geq H_\alpha(X|Y) - t$.*

The proof is straightforward and thus omitted. The following lemma follows from well known properties of the Renyi entropy which are easily seen to translate to the average conditional Renyi entropy.

Lemma 2. *For any $1 < \alpha < \infty$: $H_2(X|Y) \geq H_\infty(X|Y) \geq \frac{\alpha-1}{\alpha} H_\alpha(X|Y)$.*

Finally, our notion of average conditional Renyi entropy is such that the privacy amplification theorem of [2] still provides a lower bound on the average conditional collision entropy as we define it (as can easily be seen from the proof given in [2]). However, for us it is convenient to express the smoothness in terms of variational distance rather than entropy, as in [21, 20]:

Theorem 4 ([20]). *Let X be a random variable over $\mathcal{X}$, and let F be the random variable corresponding to the random choice of a member of a universal-two class $\mathcal{F}$ of hash functions from $\mathcal{X}$ to $\{0,1\}^\ell$. Then*

$$\delta\big([F(X)F], [\text{UNIF}^\ell][F]\big) \leq 2^{-\frac{1}{2}(H_2(X)-\ell)-1}\,.$$

B Quantitative Comparison

We compare the simple reduction of *1-2* OT^ℓ to n executions of *1-2* XOT, *1-2* GOT and *1-2* UOT, respectively, using our analysis based on Theorem 2 as discussed in Section 5.1 (together with the quantitative statement given in Theorem 3), with the results achieved in [4].[9] The quality of (the analysis of) a reduction is given by the *reduction parameters* c_{len}, c_{sec} and c_{const} such that the *1-2* OT^ℓ is guaranteed to be $2^{-\kappa}$-secure as long as $n \geq c_{\text{len}} \cdot \ell + c_{\text{sec}} \cdot \kappa + c_{\text{const}}$. The smaller these constants are, the better is the (analysis of the) reduction. The comparison of these parameters is given in Figure 3 (we focus on c_{len} and c_{sec} since c_{const} is not really relevant, unless very large).

	1-2 XOT		*1-2* GOT		*1-2* UOT	
	c_{len}	c_{sec}	c_{len}	c_{sec}	c_{len}	c_{sec}
BCW [4]	2	2	4.8	4.8	14.6	14.6
this work	4	3	4	3	13.2	10.0

Fig. 3. Comparison of the reduction parameters.

The parameters in the first line can easily be extracted from Theorems 5, 7 and 9 of [4] (where in Theorem 9 $p_e \approx 0.19$). The parameters in the second line

[9] As mentioned earlier, these results are incomparable to the parameters achieved in [10], where *interactive* reductions are used.

corresponding to the reductions to *1-2 XOT* and *1-2 GOT* follow immediately from Theorem 3, using the fact that in *one* execution of a *1-2 XOT* or a *1-2 GOT* the receivers average conditional collision entropy (as defined in Appendix A) on the sender's two input bits is at least 1 (in case of *1-2 XOT* this is trivial, and in case of *1-2 GOT* this can easily be computed). The parameters for *1-2 UOT* follow from Theorem 3 and the following observation. If for one execution of the *1-2 UOT* the receiver's average (Shannon) entropy is at least 1, then it follows from Fano's Inequality that his average guessing probability is at most $1 - p_e$ (with p_e as above), and thus his average conditional min-entropy, which lower bounds the collision entropy, is at least $-\log(1-p_e) \approx 0.3$. c_{len} and c_{sec} are then computed as $c_{\text{len}} \approx 4/0.3$ and $c_{\text{sec}} \approx 3/0.3$.

C Proof of Theorem 3

Define the event $\mathcal{E} = \{y : H_2(X|Y=y) \geq H_2(X|Y) - \kappa - 1\}$. By Lemma 1 $P[\mathcal{E}] \geq 1 - 2^{-\kappa-1}$. We will show below that conditioned on $\mathcal{E}$, the obliviousness condition of Definition 1 holds with "error term" $2^{-\kappa-1}$. It then follows that

$$\begin{aligned}
&\delta\big([B_{1-D}\, B_D\, W\, D], [\text{UNIF}]\,[B_D\, W\, D]\big) \\
&\quad \leq \delta\big(P_{B_{1-D}B_D W D \mathcal{E}}, P_{\text{UNIF}} P_{B_D W D \mathcal{E}}\big) + \delta\big(P_{B_{1-D}B_D W D \bar{\mathcal{E}}}, P_{\text{UNIF}} P_{B_D W D \bar{\mathcal{E}}}\big) \\
&\quad = \delta\big(P_{B_{1-D}B_D W D|\mathcal{E}}, P_{\text{UNIF}} P_{B_D W D|\mathcal{E}}\big) P[\mathcal{E}] + \delta\big(P_{B_{1-D}B_D W D|\bar{\mathcal{E}}}, P_{\text{UNIF}} P_{B_D W D|\bar{\mathcal{E}}}\big) P[\bar{\mathcal{E}}] \\
&\quad \leq 2^{-\kappa-1} + 2^{-\kappa-1} \;=\; 2^{-\kappa}.
\end{aligned}$$

It remains to prove the claimed obliviousness when conditioning on $\mathcal{E}$. To simplify notation, instead of conditioning on $\mathcal{E}$ we consider a distribution $P_{Y|X}$ with $H_2(X|Y{=}y) \geq H_2(X|Y){-}\kappa{-}1$ for *all* y. Note that $H_2(X|Y){-}\kappa{-}1 \geq 4\ell{+}2\kappa{+}3$. Fix an arbitrary y. Consider an arbitrary NDLF $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$. Let F_0 and F_1 be the random variables that represent the random choices of f_0 and f_1, and set $B = \beta(F_0(X_0), F_1(X_1))$. In combination with Proposition 1, privacy amplification (Theorem 4) guarantees that

$$\delta\big(P_{BF_0F_1|Y=y}, P_{\text{UNIF}} P_{F_0F_1|Y=y}\big) \leq 2^{-\frac{1}{2}(H_2(X|Y=y)+1)} \leq 2^{-\frac{1}{2}(4\ell+2\kappa+4)} = 2^{-2\ell-\kappa-2}.$$

It now follows that

$$\begin{aligned}
\delta\big([\beta(S_0,S_1)\, W], [\text{UNIF}]\,[W]\big) &= \delta\big(P_{BF_0F_1Y}, P_{\text{UNIF}} P_{F_0F_1Y}\big) \\
&= \sum_y \delta\big(P_{BF_0F_1|Y=y}, P_{\text{UNIF}} P_{F_0F_1|Y=y}\big) P_Y(y) \leq 2^{-2\ell-\kappa-2}\,.
\end{aligned}$$

Obliviousness as claimed now follows from Theorem 2. □