Oblivious Transfer and Balanced 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 the notion of *Randomized 1-2 Oblivious-Transfer* (*Rand 1-2 OT*), a minor variation of the notion of an ordinary 1-2 Oblivious-Transfer (*1-2 OT*), which in particular is sufficient for *1-2 OT*. We show that the obliviousness condition for *Rand 1-2 OT* of bits, i.e., the requirement that the receiver only learns one bit but gets (essentially) no information on the other, holds if and only if the receiver learns (essentially) no information on the XOR of the two bits. More generally we show that the obliviousness condition for *Rand 1-2 OT* of *strings* can be characterized in terms of *2-balanced functions* (i.e., bivariate functions which are balanced in both arguments), in that it holds if and only if the receiver learns (essentially) no information on the result of applying any 2-balanced function to the two strings.
We then show the usefulness of this result to the reduceability of (ordinary) *1-2 OT* to weaker primitives. In particular, we show that, based on our characterization of obliviousness (of *Rand 1-2 OT*) in terms of 2-balanced functions, the reduceability of *1-2 OT* to any weaker flavor of *OT* follows by a very simple argument. This is in sharp contrast to the current literature, where the reductions of *1-2 OT* to weaker flavors have rather complicated, often limited, 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 to his choice C, such that, informally, 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 first introduced in [Wie83] (under the name of "multiplexing") in the context of quantum cryptography, and, inspired by [Rab81] where a different flavor was introduced, later re-discovered in [EGL82].

1-2 OT turned out to be very powerful as it was shown to be sufficient for secure general two-party computation [Kil88]. 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, unconditionally secure *1-2 OT* remains impossible [LC96, May96]. As a consequence, much effort has been put into constructing unconditionally secure protocols for *1-2 OT* using physical assumptions like (various models for) noisy channels [CK88, DKS99, DFMS04, CMW04], or a memory bounded adversary [CCM98, Din01, DHRS04]. Similarly, much effort has been put into reducing *1-2 OT* to (seemingly) weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, etc. [Cré87, BC97, Cac98, Wol00, BCW03].

In this work, we first 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 C. It is rather 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 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 *2-balanced functions* (bivariate functions which are balanced, in the usual sense, in both arguments, as defined in Definition 4.2): obliviousness holds if and only if the result of applying any 2-balanced function to the two strings is (close to) uniformly distributed from the receiver's point of view.

We then show the usefulness of the above result to the reduceability of (ordinary) *1-2 OT* to weaker primitives. Concretely, we show that the reduceability of *1-2 OT* to weaker flavors follows by a trivial argument from our characterization of the obliviousness condition. This is in sharp contrast to the current literature: [BC97, Wol00, BCW03] use rather complicated and restrictive proofs 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*), and the proof given in [Cac98] for reducing *1-2 OT* to one execution of a general *UOT* is not only rather complicated, using sophisticated spoiling-knowledge techniques, but as a matter of fact it is incorrect, as we will point out. Thus, our technique allows to drastically simplify existing reduceability proofs (and in most cases to improve the reduction parameters), and it allows for new (respectively until now only incorrectly proven) reduceability results. Furthermore, it is very likely that our characterization of the obliviousness condition turns out to be useful for the construction of unconditionally-secure *1-2 OT* in certain settings, for instance in the bounded quantum-storage model [DFSS05].

2 Preliminaries

2.1 Variational Distance and Conditional Independence

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 "disentangled" distribution $P_X P_Y : (x,y) \mapsto P_X(x)P_Y(y)$. Using this notation, X and Y are (close to) *independent* if and only if $[XY] = [X][Y]$ (respectively $[XY] \approx_\varepsilon [X][Y]$).

We often have to deal with *conditional independence*. Two random variables X and Y are independent conditioned on a third, Z, if $P_{XY|Z} = P_{X|Z}P_{Y|Z}$, respectively, by multiplying both sides with P_Z^2, if $P_{XYZ}P_Z = P_{XZ}P_{YZ}$.[3] More generally, for random variables X, Y, Z and W we have to express, that – conditioned on Z – X and Y are independent and X is distributed like W: $P_{XY|Z} = P_{W|Z}P_{Y|Z}$, respectively $P_{XYZ}P_Z = P_{WZ}P_{YZ}$. We measure closeness to this ideal situation by $\delta\big([XYZ][Z], [WZ][YZ]\big)$, and we write $[XY] \approx_\varepsilon [W][Y] \;\big|Z$ to express that $\delta\big([XYZ][Z], [WZ][YZ]\big) \leq \varepsilon$. Note that "multiplying out" Z, as we do, has the effect that no special care needs to be taken if $P_Z(z)$ vanishes or is small. Also note that if W and Z are independent, then $\delta\big([XYZ][Z], [WZ][YZ]\big) = \delta\big([XYZ], [W][YZ]\big)$.

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

2.2 Tensor Product of Matrices

For matrices $A \in \mathbb{R}^{k\times\ell}$ and $B \in \mathbb{R}^{m\times n}$, the tensor product $A \otimes B \in \mathbb{R}^{km\times\ell n}$ is obtained by replacing each entry a_{ij} of A by the block $a_{ij}B$: $A \otimes B = (a_{ij}B)_{ij}$. In particular, when A and B are two row (or column) vectors, say $\mathbf{v} = (v_1, \ldots, v_\ell) \in \mathbb{R}^\ell$ and $\mathbf{w} \in \mathbb{R}^n$, then $\mathbf{v} \otimes \mathbf{w}$ is given by the vector $\mathbf{v} \otimes \mathbf{w} = (v_1\mathbf{w}, \ldots, v_\ell\mathbf{w}) \in \mathbb{R}^{\ell n}$.

We point out a couple of elementary properties of this tensor product that we will use later; they are both rather well known and straightforward to prove.

Lemma 2.1. *If the dimensions are appropriate then $(A \otimes B)(A' \otimes B') = AA' \otimes BB'$. In particular, if A and B are invertible, then so is $A \otimes B$ and $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.*

Lemma 2.2. *If A consists of the rows $\mathbf{a}_1, \ldots, \mathbf{a}_k$ and B of the rows $\mathbf{b}_1, \ldots, \mathbf{b}_m$, then the tensor product $A \otimes B$ consists of the rows $\mathbf{a}_1 \otimes \mathbf{b}_1, \mathbf{a}_1 \otimes \mathbf{b}_2, \ldots, \mathbf{a}_k \otimes \mathbf{b}_m$.*

2.3 Hadamard Matrices and Designs

A $(n \times n)$-matrix H is a *Hadamard* matrix (of order n), if every entry of H is in $\{-1, +1\}$, and if $HH^T = n\mathbb{I}$, where $\mathbb{I}$ is the $n \times n$-identity matrix. It is known that Hadamard matrices of order n can only exist if n is 1, 2 or a multiple of 4. On the other hand, they are known to exist for all powers of 2 (and believed to exist for all multiples of 4). For example, a Hadamard matrix H of order $n = 2^\ell$ can be constructed as $H = H_\circ \otimes \cdots \otimes H_\circ$ (ℓ times) with $H_\circ = \left(\begin{smallmatrix} +1 & +1 \\ +1 & -1 \end{smallmatrix}\right)$. Obviously, by multiplying a row or a column by -1, a Hadamard matrix remains a Hadamard matrix, and thus any Hadamard matrix can be *normalized* so that the first column and row is made up entirely of $+1$'s, and (as a consequence) all other columns and rows have evenly distributed -1's and $+1$'s. Removing the first row and the first column from a normalized Hadamard matrix (of order $n > 1$) results in a matrix, $\hat{H}$, which is called a *Hadamard design*. Hadamard designs are important objects in combinatorics. For us, the following property will be useful (which can be proven quite easily from above observations).

[3] Yet another way of expressing this is to say that $X \leftrightarrow Z \leftrightarrow Y$ forms a Markow chain.

Lemma 2.3. *Let H be a normalized Hadamard matrix of order $n > 1$ and $\hat{H}$ the corresponding Hadamard design. Then $\hat{H}$ is invertible, and $\hat{H}^{-1}$ is given by removing the first row and first column from $(H^T - \mathbb{1})/n$, where $\mathbb{1}$ denotes the $(n \times n)$-dimensional all-1 matrix. In particular, every row of $\hat{H}^{-1}$ consists of exactly $\frac{n}{2}$ non-zero entries, each $-\frac{2}{n}$.*

3 Defining *1-2 OT*

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

We want to formally capture the intuitive understanding of the security of *1-2 OT*. The privacy condition appears to be rather straightforward: the sender S's view V on the protocol should essentially be independent of the receiver R's choice bit C, where, generally, by the *view* of an entity executing a protocol we understand the entity's input, his choices for the random coins, and all messages received during the execution of the protocol. A subtlety (which is often overlooked) is that privacy should hold for *any* joint distribution $P_{B_0 B_1 C}$, in particular also if S's input bits B_0 and B_1 are *dependent* of C, so asking S to have *no* information on C is too demanding. In this case, one can only ask S to have no information on C *besides* B_0 and B_1; formally, that S's view V and R's choice bit C are independent conditioned on B_0 and B_1.

The obliviousness conditions needs even more care. We want to capture that R is allowed to learn one bit, say B_d, but when given this bit, his view W of the protocol should give essentially no information on the other bit B_{1-d} besides B_d and C. This is formalized by requiring that for every R there exists a random variable D with range $\{0,1\}$ such that conditioned on D, B_D and C, his view W and B_{1-D} are (close to) independent.

Another important subtlety, though often overlooked (see e.g. [BCW03]), is that (conditioned on C) D needs to be (close to) independent of B_0 and B_1. This is for instance to prevent R from receiving B_0 if $B_0 = 0$ and otherwise B_1. This gives the following definition.

Definition 3.1 (*1-2 OT*). *An ε-secure 1-2 OT is a protocol between S and R, with S having input $B_0, B_1 \in \{0,1\}$ and R having input $C \in \{0,1\}$, such that (for any distribution of B_0, B_1 and C) if S and R follow the protocol then R gets B_C as output (except with probability ε), whereas S has no output, and the following two properties hold:*

ε-Privacy: If R is honest then for any (possibly dishonest) S with view V on the protocol,

$$[CV] \approx_\varepsilon [C][V] \ \big| B_0 B_1 \,.$$

ε-Obliviousness: If S is honest then for any (possibly dishonest) R with view W on the protocol, there exists a random variable D (possibly in an extended probability space) with range $\{0,1\}$ such that

$$[D B_0 B_1] \approx_\varepsilon [D][B_0 B_1] \ \big| C \quad \text{and} \quad [B_{1-D} W] \approx_\varepsilon [B_{1-D}][W] \ \big| B_D C D$$

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. Formally, this is captured by Definition 3.2 below.

There are two main reasons for focusing on *Rand 1-2 OT*. First, an (ordinary) *1-2 OT* can obviously 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. We point this out once more in Proposition 3.3 below. And second, all information-theoretically secure constrictions of *1-2 OT* protocols we are aware of in fact do implicitly build a *Rand 1-2 OT* and use the above reduction to achieve a *1-2 OT*.

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

Definition 3.2 (*Rand 1-2 OT*). *An ε-secure Rand 1-2 OT is a protocol between* S *and* R*, with* R *having input $C \in \{0,1\}$ (while* S *has no input), such that (for any distribution of C) if* S *and* R *follow the protocol then* S *gets output $B_0, B_1 \in \{0,1\}$ and* R *gets B_C (except with probability ε) and the following two properties hold:*

ε-Privacy: If R *is honest then for any (possibly dishonest)* S *with view V on the protocol,*

$$[C\,V] \approx_\varepsilon [C]\,[V]$$

ε-Obliviousness: If S *is honest then for any (possibly dishonest)* R *with view W on the protocol, there exists a random variable D (possibly in an extended probability space) with range $\{0,1\}$ such that*

$$[B_{1-D}\,W] \approx_\varepsilon [\text{UNIF}]\,[W] \;\big|\, B_D\,D.$$

Proposition 3.3. *An ε-secure Rand 1-2 OT naturally induces an ε-secure 1-2 OT.*

Proof (sketch). As pointed out earlier, this is intuitively rather obvious. The sender and receiver run the *Rand 1-2 OT* and the sender then uses the generated B_0 and B_1 to one-time-pad encrypt his input bits, say B_0^* and B_1^*, for the *1-2 OT*, and he sends the masked bits to the receiver who can decrypt one of the two. We give some arguments that the formal security conditions of *Rand 1-2 OT* (Definition 3.2) are indeed sufficient for the security of *1-2 OT* (Definition 3.1): Regarding privacy, since the privacy condition of *Rand 1-2 OT* holds for *any* a-priori distribution of C, it in particular also holds for C conditioned on (concrete values for) B_0^* and B_1^*. On the other hand, the obliviousness condition of *Rand 1-2 OT* implies that, when given D and B_D, the mask B_{1-D} is (essentially) uniformly distributed from R's point of view. Hence, R learns (essentially) no information on the masked B_{1-D}^* besides what he knows a-priori through C. And, since the execution of the *Rand 1-2 OT* only depends on C (if at all) but not (directly) on B_0^* and B_1^*, the random variable D is independent of B_0^* and B_1^*, when given C. □

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, we can define a *1-2 ℓ-String OT* and a *Rand 1-2 ℓ-String OT* along the lines of Definition 3.1 respectively Definition 3.2 above, just by replacing the binary random variables B_0 and B_1 (as well as UNIF) by random variables S_0 and S_1 (and UNIF^ℓ) with range $\{0,1\}^\ell$. Proposition 3.3 obviously generalizes to *1-2 String OT*.

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 no information on the XOR $B_0 \oplus B_1$ of the two bits (except maybe a small amount). The following proposition shows that this is not only necessary for the obliviousness condition but also *sufficient*.

Theorem 4.1. *The ε-obliviousness condition for a Rand 1-2 OT is satisfied for a particular (possibly dishonest) receiver R with view W if and only if*

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

Before going into the proof (which is surprisingly simple), consider the following example. Assume a candidate protocol for *Rand 1-2 OT*, such that for a certain dishonest receiver, conditioned on the view of the receiver, (B_0, B_1) is $(0,0)$ with probability $\frac{1}{2}$, and $(0,1)$ and $(1,0)$ each with probability $\frac{1}{4}$. Then obviously the condition on the XOR from Theorem 4.1 is satisfied; on the other hand 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. 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 then 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 from the receiver's point of view, even when given B_d.

Proof. The "only if" implication is well known and straightforward. For the "if" implication, we first give the argument in the perfect case where $[(B_0 \oplus B_1)W] \stackrel{!}{=} [\text{UNIF}][W]$. 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 in Figure 1, with $a + b + c + d = P_W(w)$ and, by assumption, $a + d = b + c$. Due to symmetry, we may assume that $a \leq b$. Then we can 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. $P_{B_0 B_1, D, W}(\cdot,\cdot,\cdot,w)$ is indeed an 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 $P_{B_0 B_1 DW}(\cdot,\cdot,0,w) = \frac{1}{2} P_{B_0 DW}(\cdot,0,w)$ and $P_{B_0 B_1 DW}(\cdot,\cdot,1,w) = \frac{1}{2} P_{B_1 DW}(\cdot,1,w)$. This finishes the proof for 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 4.3, we skip this part of the proof.[4] □

[4] Although the special case $\ell = 1$ in Theorem 4.3 is quantitatively slightly weaker than Theorem 4.1.

4.2 The Case of String *OT*

The obvious question that occurs after the previous section is whether there is a natural generalization of Theorem 4.1 to *1-2 String OT*. Note that the straightforward generalization of the XOR-condition in Theorem 4.1, 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 String OT*: 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 4.2. *A binary function* $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ *is called* 2-balanced *if for any* $s_0, s_1 \in \{0,1\}^\ell$, *the functions* $\beta(s_0,\cdot)$ *and* $\beta(\cdot,s_1)$ *are balanced (in the usual sense), i.e.,*

$$\left|\{\varsigma_1 \in \{0,1\}^\ell : \beta(s_0,\varsigma_1)=0\}\right| = 2^\ell/2 \quad \text{and} \quad \left|\{\varsigma_0 \in \{0,1\}^\ell : \beta(\varsigma_0,s_1)=0\}\right| = 2^\ell/2\,.$$

In case $\ell = 1$, the XOR is a 2-balanced function, and up to addition of a constant the XOR is the *only* 2-balanced function. Based on this notion of 2-balanced functions, the obliviousness condition of *Rand 1-2 String OT* can be characterized as follows.

Theorem 4.3. *The ε-obliviousness condition for a Rand 1-2 ℓ-String OT is satisfied for a particular (possibly dishonest) receiver* R *with view W if*

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

for every 2-balanced function β, and, on the other hand, the ε-obliviousness condition is satisfied only if $[\beta(S_0,S_1)W] \approx_\varepsilon [\text{UNIF}][W]$ for every 2-balanced function β.

We will argue at the end of Section 5.2 that the exponential (in ℓ) overhead in the sufficient condition is unavoidable. The proof for the "only if" part is given in Appendix B. The "if" part, which is the interesting direction, is proven below.

The Case $\ell = 2$. We feel that in order to understand the proof of Theorem 4.3, it is useful to first consider the case $\ell = 2$. Let us focus on trying to develop a condition that is sufficient for *perfect* obliviousness. Fix an arbitrary view w, and consider an arbitrary non-normalized probability distribution $P_{S_0S_1W}(\cdot,\cdot,w)$ of S_0 and S_1 when $W = w$. This is depicted in the left table of Figure 2. We may assume that $a \le b,c,d$. We now extend this distribution to $P_{S_0S_1DW}(\cdot,\cdot,\cdot,w)$ similar as in the proof of Theorem 4.1, this is depicted in the two right tables in Figure 2, and then we verify what condition(s) $P_{S_0S_1W}(\cdot,\cdot,w)$ must satisfy such that $P_{S_0S_1DW}$ is indeed a valid extension, i.e., that $P_{S_0S_1DW}(\cdot,\cdot,0,w)+P_{S_0S_1DW}(\cdot,\cdot,1,w) = P_{S_0S_1W}(\cdot,\cdot,w)$.

For instance looking at the second row and second column we get equation $e+(b-a) = f$. Altogether, we get the following equations system.

$$\begin{array}{lll} b+e=a+f & b+i=a+j & b+m=a+n \\ c+e=a+g & c+i=a+k & c+m=a+o \\ d+e=a+h & d+i=a+l & d+m=a+p \end{array}$$

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

$P_{S_0S_1W}(\cdot,\cdot,w)$

a	a	a	a
e	e	e	e
i	i	i	i
m	m	m	m

$P_{S_0S_1DW}(\cdot,\cdot,0,w)$

0	$b-a$	$c-a$	$d-a$
0	$b-a$	$c-a$	$d-a$
0	$b-a$	$c-a$	$d-a$
0	$b-a$	$c-a$	$d-a$

$P_{S_0S_1DW}(\cdot,\cdot,1,w)$

Fig. 2. Distributions $P_{S_0S_1W}(\cdot,\cdot,w)$ and $P_{S_0S_1DW}(\cdot,\cdot,\cdot,w)$

Note that if all these equations do hold for any w, then $P_{S_0S_1DW}(\cdot,\cdot,\cdot,\cdot)$ is well defined and satisfies $P_{S_0S_1DW}(\cdot,\cdot,0,\cdot) = \frac{1}{4}P_{S_0DW}(\cdot,0,\cdot)$ and $P_{S_0S_1DW}(\cdot,\cdot,1,\cdot) = \frac{1}{4}P_{S_1DW}(\cdot,1,\cdot)$, in other words, perfect obliviousness holds.

The idea is to transform the equation system into a new but equivalent one, such that each equation in the new system expresses that a certain specific function applied to S_0 and S_1 is uniformly distributed (when $W = w$). All these functions will turn out to be 2-balanced functions.

For instance, by adding all the equations in the original system, but taking every second equation with negative sign, one gets the equation

$$b + d + e + g + j + l + m + o = a + c + f + h + i + k + n + p$$

Define the function $\beta : \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$ as follows. Let $\beta(s_0, s_1)$ be 0 if the entry which corresponds to (s_0, s_1) in the left table in Figure 2 appears on the left hand side of the above equation, and else we let $\beta(s_0, s_1)$ be 1. Then the above equation simply says that $\beta(S_0, S_1) = 0$ with the same probability as $\beta(S_0, S_1) = 1$ (when $W = w$). Furthermore, it is easy to verify that this function β is 2-balanced: for every row of the left table in Figure 2, half of the variables in that row appear on the left hand side of the above equation and the other half appear on the right hand side (always with multiplicity 1). The corresponding holds for every column.

One can now show (and we are going to do this below for an arbitrary ℓ) that it is possible to generate enough such equations, corresponding to 2-balanced functions, such that the new equation system has the same solution space as the original system. This implies that if $\beta(S_0, S_1)$ is distributed uniformly and independently of W for every 2-balanced function β, then the original equation system is satisfied (for any w).

Proof of Theorem 4.3 ("if" part). First, we consider the perfect case: if $[\beta(S_0, S_1)W] = [\text{UNIF}][W]$ for every 2-balanced function β, then the obliviousness condition for *Rand 1-2 ℓ-String OT* holds (perfectly).

THE PERFECT CASE: We generalize the idea from the case $\ell = 2$. The main issue will be how to transform the initial equation system.

Fix an arbitrary view w of the receiver. Consider the non-normalized probability distribution $P_{S_0S_1W}(\cdot,\cdot,w)$ (which adds up to $P_W(w)$). We name $P_{S_0S_1W}(s_0, s_1, w)$ by the variable p_{s_0,s_1}. Writing $\mathbf{o}$ 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 $s_1 \in \{0,1\}^l$. We show later that we may do so. We extend this distribution to $P_{S_0 S_1 DW}(\cdot,\cdot,\cdot,w)$ by setting

$$P_{S_0 S_1 DW}(s_0,s_1,0,w) = p_{s_0,\mathbf{o}} \quad \text{and} \quad P_{S_0 S_1 DW}(s_0,s_1,1,w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}} \tag{1}$$

for any strings $s_0, s_1 \in \{0,1\}^\ell$, and we collect the equations resulting from the condition $P_{S_0 S_1 DW}(\cdot,\cdot,0,w) + P_{S_0 S_1 DW}(\cdot,\cdot,1,w) = P_{S_0 S_1 W}(\cdot,\cdot,w)$: 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 $\ell = 1$ or $\ell = 2$, the random variable D is well defined and $[S_{1-D} S_D W D] = [\text{UNIF}][S_D W D]$ holds.

Before moving on, we first justify the assumption that $p_{\mathbf{o},\mathbf{o}} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^l$. In general, we choose $t \in \{0,1\}^\ell$ such that $p_{\mathbf{o},t} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^l$, and we set $P_{S_0 S_1 DW}(s_0,s_1,0,w) = p_{s_0,t}$ and $P_{S_0 S_1 DW}(s_0,s_1,1,w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},t}$, 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). Thus, it suffices to focus on the equations given by (2).

We proceed by transforming this equation system (consisting of $2^{\ell-1} \cdot 2^{\ell-1}$ equations) to a new but equivalent equation system whose equations say something about the distribution of $\beta(S_0, S_1)$ (when $W = w$) for 2-balanced functions β. We introduce some convenient notation first. Let $\mathbf{p}$ be the $2^\ell \cdot 2^\ell$-dimensional (column) vector containing all variables p_{s_0,s_1} in lexicographic order as entries: $\mathbf{p} = (p_{\mathbf{o},\mathbf{o}}, p_{\mathbf{o},0\cdots01}, \ldots, p_{1\cdots1,1\cdots1})^T$. We identify the elements in $\{0,1\}^\ell$ with the numbers $\{1,\ldots,2^\ell\}$ and the elements in $\{0,1\}^\ell \times \{0,1\}^\ell$ with the numbers $\{1,\ldots,2^{2\ell}\}$ by counting them in the lexicographic order. Using this convention, we can say that for any $s_0, s_1 \in \{0,1\}^\ell$ the (s_0,s_1)-th entry of $\mathbf{p}$ is p_{s_0,s_1}. For any $s \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$ let $\mathbf{e}_s$ be the 2^ℓ-dimensional (row) vector with first coordinate $+1$ and s-th coordinate -1 and all remaining coordinates 0. Then, equation (2) can be expressed as $(\mathbf{e}_{s_0} \otimes \mathbf{e}_{s_1}) \cdot \mathbf{p} = 0$. Finally, let E be the matrix with the $\mathbf{e}_s$'s as rows, in lexicographic order. Note that $E = [\,\mathbf{1} | -\mathbb{I}\,]$, where $\mathbf{1}$ is the $(2^\ell - 1)$-dimensional all-one vector, and $\mathbb{I}$ is the $(2^\ell - 1)$-dimensional identity matrix. Then, using Lemma 2.2, the whole equation system can be expressed as

$$(E \otimes E) \cdot \mathbf{p} = \mathbf{0}$$

where $\mathbf{0}$ denotes the $(2^\ell - 1)^2$-dimensional all-zero vector.

Consider now the following matrix T over $\{-1,+1\}$, consisting of $2^\ell - 1$ rows and $2^\ell - 1$ columns. Let H be a normalized Hadamard matrix of order 2^ℓ, and let $\hat{H}$ be the corresponding Hadamard design (obtained by removing first column and row of H). Then, set $T = -\hat{H}$. The crucial properties of T are that all entries are ± 1, each row has weight (i.e., sum of entries) $+1$, and T is invertible (Lemma 2.3). By Lemma 2.1, also $T \otimes T$ is invertible, and thus

$$(TE \otimes TE) \cdot \mathbf{p} = (T \otimes T)(E \otimes E) \cdot \mathbf{p} = \mathbf{0} \tag{3}$$

is an equivalent equation system. We consider now an arbitrary but fixed row of $TE \otimes TE$. This row can be written as $\mathbf{t}E \otimes \mathbf{t}'E$ where $\mathbf{t}$ and $\mathbf{t}'$ are two rows of T. By the shape of E it is clear that $\mathbf{t}E = [\,1 \,|\, -\mathbf{t}\,]$ and $\mathbf{t}'E = [\,1 \,|\, -\mathbf{t}'\,]$. For any strings $s_0, s_1 \in \{0,1\}^\ell$ the multiplicity with which p_{s_0,s_1} occurs in $(\mathbf{t}E \otimes \mathbf{t}'E) \cdot \mathbf{p}$ is given by the s_0-th coordinate of $\mathbf{t}E$ times the s_1-th coordinate of $\mathbf{t}'E$, and hence is either $+1$ or -1. We define $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$

by setting $\beta(s_0, s_1) = 0$ if the multiplicity of p_{s_0,s_1} equals $+1$ and setting $\beta(s_0, s_1) = 1$ if the multiplicity of p_{s_0,s_1} equals -1. Then, the equation $(\mathbf{t}E \otimes \mathbf{t}'E) \cdot \mathbf{p} = 0$ is equivalent to asking $\beta(S_0, S_1)$ to be uniformly distributed, given $W = w$. It remains to argue that β is 2-balanced.

But this is rather obvious, again by the shape of E. For any fixed $s_0 \in \{0,1\}^\ell$, the number of ς_1's with $\beta(s_0, \varsigma_1) = 0$ is given by the number of $+1$'s in $\mathbf{t}'E$, and the number of ς_1's with $\beta(s_0, \varsigma_1) = 1$ is given by the number of -1's in $\mathbf{t}'E$, or the other way round, depending on s_0. But as $\mathbf{t}'E = [\,1 \,|\, -\mathbf{t}'\,]$ they are the same. The same holds for the number of ς_0's with $\beta(\varsigma_0, s_1) = 0$ respectively 1 for any s_1.

THE GENERAL CASE: Now, we consider the general case where there exists some $\varepsilon > 0$ such that $\delta\big([\beta(S_0, S_1)W], [\text{UNIF}][W]\big) \leq 2^{-2\ell-1}\varepsilon$ for any 2-balanced function 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 2-balanced function 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 $\sum_w \varepsilon_{w,\beta} = \delta\big([\beta(S_0, S_1)W], [\text{UNIF}][W]\big) \leq 2^{-2\ell-1}\varepsilon$, independent of β. Fix now an arbitrary w with $P_W(w) > 0$. Then, (3) only holds approximately in that every coordinate in $\mathbf{0}$ needs to be replaced by $\pm 2\varepsilon_{w,\beta}$ for some 2-balanced function β (corresponding to that row). Now, by Lemma 2.3 and the choice of T, every row of T^{-1} has exactly $2^{\ell-1}$ non-zero entries, each $1/2^{\ell-1}$, and thus every row of $(T \otimes T)^{-1}$ has exactly $2^{2\ell-2}$ non-zero entries, each $1/2^{2\ell-2}$. Hence, (2) still holds approximately in that $\big|p_{\mathbf{o},\mathbf{o}} + p_{s_0,s_1} - (p_{\mathbf{o},s_1} + p_{s_0,\mathbf{o}})\big| = \delta_{s_0,s_1}$ with

$$\delta_{s_0,s_1} \leq \frac{2}{2^{2\ell-2}}\big(\varepsilon_{w,\mathcal{B}_1(s_0,s_1)} + \cdots + \varepsilon_{w,\mathcal{B}_{2^{2\ell-2}}(s_0,s_1)}\big)$$

(and $\delta_{s_0,s_1} = 0$ if $s_0 = \mathbf{o}$ or $s_2 = \mathbf{o}$) where for every $i \in \{1, \ldots, 2^{2\ell-2}\}$ and $s_0, s_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$, $\mathcal{B}_i(s_0, s_1)$ represents a particular 2-balanced function $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$. Note that δ_{s_0,s_1} depends on w, but $\mathcal{B}_i(s_0, s_1)$ does not, it is solely determined by the positions of the non-zero entries of $(T \otimes T)^{-1}$.

Since (2) only holds approximately, $P_{S_0 S_1 DW}$ as in (1) is not necessarily a valid extension, but close. This can obviously be overcome by instead setting

$$P_{S_0 S_1 DW}(s_0, s_1, 0, w) = p_{s_0,\mathbf{o}} \pm \delta'_{s_0,s_1} \quad \text{and} \quad P_{S_0 S_1 DW}(s_0, s_1, 1, w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}} \pm \delta''_{s_0,s_1}$$

with suitably chosen $\delta'_{s_0,s_1}, \delta''_{s_0,s_1} \geq 0$ with $\delta'_{s_0,s_1} + \delta''_{s_0,s_1} = \delta_{s_0,s_1}$ and suitably chosen signs "+" or "−".[5] Then, every $P_{S_0 S_1 DW}(s_0, s_1, 0, w)$ differs from $p_{s_0,\mathbf{o}}$ by at most δ'_{s_0,s_1}. A straightforward computation then shows that

$$\delta\big(P_{S_{1-D} S_D DW}(\cdot, \cdot, 0, w), P_{\text{UNIF}} P_{S_D DW}(\cdot, 0, w)\big) \leq \sum_{s_0,s_1} \delta'_{s_0,s_1}\,.$$

The corresponding holds for $P_{S_0 S_1 DW}(\cdot, \cdot, 1, w)$. It follows that

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

[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 $P_{S_0 S_1 W}(s_0, s_1, w) = 0$, then one has to correct both.

$$\leq \frac{2}{2^{2\ell-2}} \sum_{s_0,s_1} \sum_{i} \sum_{w} \varepsilon_{w,\mathcal{B}_i(s_0,s_1)} \leq \frac{2}{2^{2\ell-2}} \sum_{s_0,s_1} 2^{2\ell-2} \cdot 2^{-2\ell-1}\varepsilon = \varepsilon\,.$$

This concludes the proof. □

5 Application

In this section we are going to show the usefulness of Theorem 4.3 for the construction of *1-2 (String) OT*, based on weaker primitives (like a noisy channel or other flavors of *OT*). In particular, we will show that the reduceability of *1-2 OT* to any weaker flavor of *OT* follows as a simple argument using Theorem 4.3.

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

Background. Much effort has been put into constructing protocols for *1-2 (String) OT* based on physical assumptions like (various models for) noisy channels [CK88, DKS99, DFMS04, CMW04] or a memory bounded adversary [CCM98, Din01, DHRS04], as well as into reducing *1-2 (String) OT* to (seemingly) weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, *1-2 GOT* and *1-2 UOT* [Cré87, BC97, Cac98, Wol00, BCW03]. 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 S has no information on which part of X R learned, and (3) any R has some uncertainty in X. Then, this is completed to a *Rand 1-2 OT* by means of privacy amplification [BBCM95]: 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 $S_C = h_C(X_C)$. 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 [BBCM95]. This difficulty is overcome in [BC97, BCW03] 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 has remained an open problem.

[6] As a matter of fact, reduceability has been proven for any bound on $I(B_0B_1; Y)$ strictly smaller than 2.

The New Approach. We argue that, independent of the underlying primitive, obliviousness follows as a simple consequence of Theorem 4.3, in combination with a simple observation regarding the composition of 2-balanced functions with strongly universal-two hash functions (Proposition 5.1 below). Recall that a class $\mathcal{F}$ of hash functions from, say, $\{0,1\}^n$ to $\{0,1\}^\ell$ is *strongly* universal-two [WC79] 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 5.1. *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 $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ be a 2-balanced function. Consider the class $\mathcal{F}$ of all 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.*[7]

Proof. Fix distinct $x = (x_0, x_1)$ and $x' = (x'_0, x'_1)$ in $\{0,1\}^{n_0} \times \{0,1\}^{n_1}$. Assume without loss of generality that $x_1 \neq x'_1$. Fix $f_0 \in \mathcal{F}_0$, and set $s_0 = f_0(x_0)$ and $s'_0 = f_0(x'_0)$. By assumption on $\mathcal{F}_1$, the random variables $F_1(x_1)$ and $F_1(x'_1)$ are independent uniformly distributed over $\{0,1\}^\ell$ (where F_1 represents the random choice for $f_1 \in \mathcal{F}_1$). By the assumption on β, this implies that $\beta(f_0(x_0), F_1(x_1))$ and $\beta(f_0(x'_0), F_1(x'_1))$ are independent uniformly distributed (over $\{0,1\}$). This holds no matter how f_0 is chosen, and thus proves the claim. □

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 R has "high" collision entropy in X. Hence, for any 2-balanced function β, we can apply the privacy amplification theorem [BBCM95] (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 4.3.

We save the quantitative analysis (Theorem 5.2) 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 Section 5.3 the quality of the analysis of the above reductions based on Theorem 4.3 with the results in [BCW03]. It turns out that our analysis is tighter for *1-2 GOT* and *1-2 UOT*, whereas the analysis in [BCW03] is tighter for *1-2 XOT*.

5.2 Reducing *1-2 OT* 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] As a side remark, it is easy to see that 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 obviously not universal-two.

Universal Oblivious Transfer. The probably weakest flavor of OT is the *Universal OT* (UOT), introduced in [Cac98], 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 because "*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 for instance 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 (String) OT* 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 3, 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 two random and independent $f_0, f_1 \in \mathcal{F}$, 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. 3. Protocol *OT2UOT* for *Rand1-2 String OT*.

In [Cac98] it is claimed that, for appropriate parameters, protocol *OT2UOT* is a secure *Rand 1-2 (String) OT* (respectively, the resulting protocol for *1-2 OT* is secure). However, we argue below that the proof given is not correct (and fixing it seems to be hard). In Theorem 5.2 we then show that its security in fact follows easily from Theorem 4.3.

A Flaw in the Security Proof. In [Cac98] the security of protocol *OT2UOT* is argued as follows. Using (rather complicated) *spoiling-knowledge techniques*, it is shown that, conditioned on the receiver's view (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 Renyi 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 $H(F_1(X_1)|F_1, X_0 = x_0)$ is close to ℓ, and, similarly, at least 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 that *OT2UOT* is 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 $H(F_0(X_0)|F_0)$ 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

[8] Note that this notion of UOT is slightly more general than the one considered in [Cac98], where it was required that $H_\alpha(X|Y{=}y) \geq r$ for all y.

receiver to learn the (bitwise) XOR $S_0 \oplus S_1$, which is clearly forbidden by the obliviousness condition.

We also argue that it appears to be hard to fix the proof given in [Cac98]. In order to *correctly* conclude by applying the privacy amplification theorem to X_0 or X_1 (the one with the higher entropy), one needs to show that at least one out of $H_2(X_0|X_1 = x_1)$ and $H_2(X_1|X_0 = x_0)$ is large. But this is not possible since R may choose to learn $X_0 \oplus X_1$. 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 R obviously learns $S_0 \oplus S_1$.

Reducing *1-2 (String) OT* 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 5.2. *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 ℓ-String OT to a (perfect) $(2,r)$-UOT$(\{0,1\}^{2n})$ with $n \geq r \geq 4\ell + 3\kappa + 4$ (i.e., with $n \geq H_2(X|Y) \geq 4\ell + 3\kappa + 4$).*

Using the bounds from Lemma A.2 on the different orders of Renyi entropy, the reduceability of *1-2 String OT* 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 5.1 in combination with the privacy amplification theorem, and applying Theorem 4.3. The following formal proof keeps track of the "error term".

Proof. Define the event $\mathcal{E} = \{y : H_2(X|Y = y) \geq H_2(X|Y) - \kappa - 1\}$. By Lemma A.1 $P[\mathcal{E}] \geq 1 - 2^{-\kappa-1}$. We will show below that conditioned on $\mathcal{E}$, the obliviousness condition of Definition 3.2 holds with "error term" $2^{-\kappa-1}$. It then follows that

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

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 2-balanced function $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$. 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 5.1, privacy amplification (Theorem A.3) guarantees that

$$\delta\big(P_{B F_0 F_1|Y=y}, P_{\text{UNIF}} P_{F_0 F_1|Y=y}\big) \leq 2^{-\frac{1}{2}(H_2(X|Y=y)+1)} \leq 2^{-\frac{1}{2}(4\ell+2\kappa+4)} = 2^{-2\ell-\kappa-2}$$

It now follows that

$$\delta\big([\beta(S_0, S_1) W], [\text{UNIF}]\,[W]\big) = \delta\big(P_{B F_0 F_1 Y}, P_{\text{UNIF}} P_{F_0 F_1 Y}\big)$$

$$= \sum_y \delta\big(P_{BF_0F_1|Y=y}, P_{\text{UNIF}} P_{F_0F_1|Y=y}\big) P_Y(y)$$
$$\leq 2^{-2\ell-\kappa-2}.$$

Theorem 4.3 now concludes the proof. □

From this proof it also becomes clear that the exponential (in ℓ) overhead in Theorem 4.3 is unavoidable. Indeed, a sub-exponential overhead would allow ℓ in Theorem 5.2 to be super-linear (in n), which of course is nonsense.

5.3 Quantitative Comparison

We compare the reduction of *1-2 ℓ-String OT* to n executions of *1-2 XOT*, *1-2 GOT* and *1-2 UOT*, respectively, using our analysis based on Theorem 4.3 as discussed in Section 5.1 (together with the quantitative statement given in Theorem 5.2), with the results achieved in [BCW03]. 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 ℓ-String OT* 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 4 (we focus on c_{len} and c_{sec} since c_{const} is not really relevant, unless really large).

	1-2 XOT		*1-2 GOT*		*1-2 UOT*	
	c_{len}	c_{sec}	c_{len}	c_{sec}	c_{len}	c_{sec}
[BCW03]	2	2	4.8	4.8	14.6	14.6
this work	4	3	4	3	13.2	10.0

Fig. 4. Comparison of the reduction parameters.

The parameters in the first line can easily be extracted from Theorems 5, 7 and 9 of [BCW03] (where in Theorem 9 $p_e \approx 0.19$). The parameters in the second line corresponding to the reductions to *1-2 XOT* and *1-2 GOT* follow immediately from Theorem 5.2, 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 5.2 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 $c_{\text{sec}} \approx 3/0.3$.

6 Conclusion

We have shown a characterization of the obliviousness condition of (a slightly modified version of) *1-2 (String) OT* (Theorem 4.3), which (once given) allows to reason about the

reduceability of *1-2 (String) OT* to weaker versions of *OT* by a very simple argument. In particular, the reduceability of *1-2 OT* of *bits* can be argued easily via Theorem 4.1, which itself has a simple proof, and hence the reduceability can be argued easily *from scratch*. This is rather surprising, taking into account the amount of work that has been done in that area.

In this paper, we focused on *1-2 (String) OT*. It seems that Theorem 4.3 can be generalized to *1-m (String) OT* and m-balanced functions, where a m-balanced function is defined to be a m-variate function such that fixing any one of the arguments gives a balanced function (in the usual sense). Unfortunately, Proposition 5.1 does *not* generalize to this notion of balanced functions; thus, the generalization of Theorem 4.3 to *1-m (String) OT* does not seem to have the same impact.

Acknowledgments

We would like to thank Renato Renner for bringing up the idea of characterizing obliviousness in terms of the XOR. We are also grateful to Claude Crépeau, George Savvides and Juerg Wullschleger for enlightening discussions regarding the formal definition of *1-2 OT*.

References

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6), 1995.

[BC97] Gilles Brassard and Claude Crepeau. Oblivious transfers and privacy amplification. In *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*. Springer, 1997.

[BCW03] Gilles Brassard, Claude Crépeau, and Stefan Wolf. Oblivious transfer and privacy amplification. *Journal of Cryptology*, 16(4), 2003.

[Cac98] Christian Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology—EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*. Springer, 1998.

[CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *39th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 493–502, 1998.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 1988.

[CMW04] Claude Crepeau, Kirill Morozov, and Stefan 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.

[Cré87] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In *Advances in Cryptology—CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*. Springer, 1987.

[DFMS04] Ivan B. Damgård, Serge Fehr, Kirill Morozov, and Louis Salvail. Unfair noisy channels and oblivious transfer. In *Theory of Cryptography Conference (TCC)*, volume 2951 of *Lecture Notes in Computer Science*. Springer, 2004.

[DFSS05] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2005.

[DHRS04] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen 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.

[Din01] Yan Zong Ding. Oblivious transfer in the bounded storage model. In *Advances in Cryptology—CRYPTO '01*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.

[DKS99] Ivan B. Damgard, Joe Kilian, and Louis 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.

[EGL82] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*. Plenum Press, 1982.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4), 1999.

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *21st Annual ACM Symposium on Theory of Computing (STOC)*, 1989.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, 1988.

[LC96] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? Quantum Physics ePrint Archive, Report quant-ph/9603004, 1996. `http://arXiv.org`.

[May96] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1996.

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

[WC79] Mark N. Wegman and J. Lawrence Carter. New classes and applications of hash functions. In *20th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 1979.

[Wie83] Stephen Wiesner. Conjugate coding. *ACM Special Interest Group on Automata and Computability Theory (SIGACT News)*, 15, 1983. Original manuscript written circa 1970.

[Wol00] Stefan 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 A.1. *Let $\alpha > 1$ (allowing $\alpha = \infty$) and $t \geq 0$. Then $H_\alpha(X|Y=y) \geq H_\alpha(X|Y) - t$ with probability at least $1 - 2^{-t}$ (over the choice of y).*

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 A.2. *For any $1 < \alpha < \infty$ it holds that $H_2(X|Y) \geq H_\infty(X|Y) \geq \frac{\alpha-1}{\alpha} H_\alpha(X|Y)$.*

Finally, our notion of average conditional Renyi entropy is such that the privacy amplification theorem of [BBCM95] 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 [BBCM95]). However, for us it is convenient to express the smoothness in terms of variational distance rather than entropy, as in [ILL89, HILL99]:

Theorem A.3 ([HILL99]). *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 Proof of Theorem 4.3 ("only if" part)

According to Definition 3.2, the ε-obliviousness for *Rand 1-2 OT* is satisfied for a receiver R with view W if there exists a random variable D with range $\{0,1\}$ such that

$$\sum_{w,d,s_0,s_1} \left| P_{S_{1-D}S_D DW}(s_{1-d}, s_d, d, w) - 2^{-\ell} P_{S_D DW}(s_d, d, w) \right| \leq \varepsilon.$$

In order to upperbound

$$\delta([\beta(S_0,S_1)W], [\text{UNIF}][W]) = \sum_{w,b} \left| P_{\beta(S_0,S_1)W}(b,w) - \frac{1}{2} P_W(w) \right|$$

we expand the terms on the right hand side as follows.

$$P_{\beta(S_0,S_1)W}(b,w) = \sum_d P_{\beta(S_0,S_1)DW}(b,d,w) = \sum_d \sum_{\substack{s_d, s_{1-d} \\ \beta(s_0,s_1)=b}} P_{S_{1-D}S_D DW}(s_{1-d}, s_d, d, w)$$

and

$$P_W(w) = \sum_d \sum_{s_d} P_{S_D DW}(s_d, d, w) = \sum_d 2^{-\ell+1} \cdot \sum_{\substack{s_d, s_{1-d} \\ \beta(s_0,s_1)=b}} P_{S_D DW}(s_d, d, w)$$

where the last equality holds because there are $2^{\ell-1}$ values for s_{1-d} such that $\beta(s_0,s_1) = b$, as β is a 2-balanced function. Using those two expansions we conclude that

$$\begin{aligned}
&\delta([\beta(S_0,S_1)W], [\text{UNIF}][W]) \\
&\quad \leq \sum_{w,b} \sum_d \sum_{\substack{s_d, s_{1-d} \\ \beta(s_0,s_1)=b}} \left| P_{S_{1-D}S_D DW}(s_{1-d}, s_d, d, w) - 2^{-\ell} P_{S_D DW}(s_d, d, w) \right| \\
&\quad = \sum_{w,d,s_0,s_1} \left| P_{S_{1-D}S_D DW}(s_{1-d}, s_d, d, w) - 2^{-\ell} P_{S_D DW}(s_d, d, w) \right| \leq \varepsilon.
\end{aligned}$$

where the first inequality follows follows from the above expansions and the triangle inequality and the last inequality is our initial assumption. □