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 [30] under the name of "multiplexing" in the context of quantum cryptography, and, inspired by [26] 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 [23]. 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 [24, 25]. 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 [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, 31, 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

* This is the full version of a paper published at CRYPTO 2006 [15].

** Supported by the Dutch Organization for Scientific Research (NWO).

*** Supported by the EC-Integrated Project SECOQC, No: FP6-2002-IST-1-506813.

† Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation, and Foundations in Cryptography and Security, funded by the Danish Natural Sciences Research Council.

‡ Centrum voor Wiskunde en Informatica, the national research institute for mathematics and computer science in the Netherlands.

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 *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 4.2): 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, 31, 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 may be useful for the construction and analysis of *1-2 OT* protocols in other settings, for instance in a quantum setting as demonstrated in [13], or for computationally secure *1-2 OT* with unconditional obliviousness.

Finally, we extend our result and show how our characterization of *Rand 1-2 OT* in terms of non-degenerate linear functions translates to *1-n OT* and to *1-2 OT*in a *quantum setting.*

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 $\delta\big(P,Q\big)\le\varepsilon$.

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, $[XY]$ denotes the joint distribution P_{XY} whereas $[X][Y]$ denotes the "disentangled" distribution $Q_{XY}=P_XP_Y$, and $[X|Y{=}y]$ stands for the conditional distribution $P_{X|Y=y}$. 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.

We also have to deal with *conditional independence.* Two random variables X and Y are independent conditioned on a third, Z, if $P_{XY|Z}=P_{X|Z}P_{Y|Z}$, in other words, if $X\leftrightarrow Z\leftrightarrow Y$

forms a Markov chain.[1] After multiplying both sides with P_Z^2, the condition reads $P_{XYZ}P_Z = P_{XZ}P_{YZ}$. We measure closeness to this ideal situation by $\delta\big([XYZ][Z],[XZ][YZ]\big)$, and we write $[XY] \approx_\varepsilon [X][Y] \;\big|Z$ to express that $\delta\big([XYZ][Z],[XZ][YZ]\big) \leq \varepsilon$. Note that "multiplying out" Z has the effect that no special care needs to be taken if $P_Z(z)$ vanishes or is small.

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.

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 and subtle task. For instance requiring the sender's view to be independent of the receiver's choice bit C is too strong a requirement, since his input might already depend on C. The best one can hope for is that his view is independent of C *conditioned on his input* B_0, B_1. Security against a dishonest receiver is even more subtle. 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.

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, the following properties hold:*[2]

- *ε-Correctness: For honest* S *and* R, R *outputs B_C, except with probability ε.*
- *ε-Privacy: For honest* R *and any (dishonest)* $\tilde{\mathsf{S}}$ *with output*[3] *V, $[CV] \approx_\varepsilon [C][V] \;\big|B_0B_1$.*
- *ε-Obliviousness: For honest* S *and any (dishonest)* $\tilde{\mathsf{R}}$ *with output W, there exists a binary random variable D such that $[DB_0B_1] \approx_\varepsilon [D][B_0B_1] \;\big|C$ and $[B_{1-D}W] \approx_\varepsilon [B_{1-D}][W] \;\big|B_DCD$.*

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 3.2 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]. And second, all information-theoretically secure constructions 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 *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 3.2 (*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:*

[1] Functional equalities like $P_{XY|Z} = P_{X|Z}P_{Y|Z}$ are to be understood pointwise: $P_{XY|Z}(x,y|z) = P_{X|Z}(x|z)P_{Y|Z}(y|z)$ for all x,y,z (for which $P_Z(z) > 0$); it should always be clear from the context how the arguments, here x,y,z, are to be distributed among the functions/distributions.

[2] Be aware that there is no consistent naming of these properties in the literature.

[3] Note that S's output V may consist of S's complete view on the protocol.

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

ε-Obliviousness: For honest S *and any (dishonest)* $\tilde{\mathsf{R}}$ *with output* W*, there exists a binary random variable* D *such that* $[B_{1-D} W B_D D] \approx_\varepsilon [\text{UNIF}][W B_D D]$*.*

The privacy condition simply says that 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 D and the corresponding bit B_D, then the other bit, B_{1-D}, is completely random from R's point of view.

We would like to point out that the definitions of *1-2 OT* and *Rand 1-2 OT* given in the full version of [11] look syntactically slightly different than our Definitions 3.1 and 3.2, respectively. However, it is not hard to see that they are actually equivalent. The main difference is that the definitions in [11] involve an auxiliary input Z, which is given to the dishonest player, and privacy and obliviousness as we define them are required to hold *conditioned on* Z for any Z. Considering a *constant* Z immediately proves one direction of the claimed equivalence, and the other follows from the observation that if privacy and obliviousness as we define them hold for *any* distribution $P_{B_0 B_1 C}$ (respectively P_C), then they also hold for the conditional distribution $P_{B_0 B_1 C|Z=z}$ (respectively $P_{C|Z=z}$). The other difference is that in the full version of [11], in the obliviousness condition of *Rand 1-2 OT*, B_{1-D} is required to be random and independent of W, B_D, D *and* C. This of course implies our obliviousness condition (which is without C), but it is also implied by our definition as C may be part of the output W. We feel that simplifying the definitions as we do, without changing their meaning, allows for an easier handling.

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^ℓ and *Rand 1-2* OT^ℓ can be defined along the same lines as *1-2 OT* and *Rand 1-2 OT* of *bits*: the binary random variables B_0 and B_1 as well as UNIF in Definitions 3.1 and 3.2 are simply replaced by random variables S_0 and S_1 and UNIF^ℓ 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 4.1. *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*

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

Before going into the proof which is surprisingly simple, consider the following example. Assume a candidate protocol for *Rand 1-2 OT* 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 4.1 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 $W = B_C$. In the light of Definition 3.2, 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 4.5, we skip this part of the proof.[4] $\square$

4.2 The Case of String *OT*

The obvious question after the previous section is whether there is a natural generalization of Theorem 4.1 to *1-2* OT^ℓ for $\ell \geq 2$. 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* 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 4.2. *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.*

[4] Although the special case $\ell = 1$ in Theorem 4.5 is quantitatively slightly weaker than Theorem 4.1.

Even though this is the main notion we are using, the following more relaxed notion allows to make some of our claims slightly stronger.

Definition 4.3. *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, meaning that* $\bigl|\{\sigma_1 \in \{0,1\}^\ell : \beta(s_0,\sigma_1)=0\}\bigr| = 2^\ell/2$ *and* $\bigl|\{\sigma_0 \in \{0,1\}^\ell : \beta(\sigma_0,s_1)=0\}\bigr| = 2^\ell/2$.

The following is easy to see and the proof is omitted.

Lemma 4.4. *Every non-degenerate linear function is 2-balanced.*

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

Theorem 4.5. *The* ε*-obliviousness condition for a Rand 1-2 OT*$^\ell$ *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*.*

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 4.5 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.

At first glance, Theorem 4.5 appears to be related to the so-called (information-theoretic) XOR-Lemma, commonly attributed to Vazirani [28] and nicely explained by Goldreich [20], which states that a string is close to uniform if the XOR of the bits of any non-empty substring are. As far as we can see, neither follows Theorem 4.5 from the XOR-Lemma in an obvious way nor can it be proven by modifying the proof of the XOR-Lemma, as given in [20].

Furthermore, 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 4.5: it additionally requires that one of the two strings is *a priori* uniformly distributed from the receiver's point of view.[5] 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 4.1 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 an open problem how to prove their construction secure when a different class of hash functions is used. The condition for Theorem 4.5, 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 4.5 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 4.5 for later.

The proof for the "only if" part of Theorem 4.5 is given in Appendix B; 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. The "if" part, which is the interesting direction, is proven below.

[5] 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.

The Case $\ell = 2$. We feel that in order to understand the proof of Theorem 4.5, 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 output 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, where we write a for $P_{S_0S_1W}(00,00,w)$, b for $P_{S_0S_1W}(00,01,w)$, etc. We may assume that $a \leq b,c,d$. 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. We verify what conditions $P_{S_0S_1W}(\cdot,\cdot,w)$ must satisfy such that $P_{S_0S_1DW}$ is indeed a valid extension, i.e., that $P_{S_0S_1DW}(\cdot,\cdot,0,w) + P_{S_0S_1DW}(\cdot,\cdot,1,w) = P_{S_0S_1W}(\cdot,\cdot,w)$.

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

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

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

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 now is to show that the above equation system is equivalent to another equation system, in which every equation expresses that a certain NDLF applied to S_0 and S_1 is uniformly distributed when $W = w$, which holds by assumption.

For example, 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 $W = w$). Note that it is crucial that in the above equation every variable a up to p occurs with multiplicity exactly 1. By comparing the function tables, it is now easy to verify that β coincides with the function $(s_0,s_1) \mapsto s_{02} \oplus s_{12}$, where s_{i2} denotes the second coordinate of $s_i \in \{0,1\}^2$, thus is a NDLF.

One can now show (and we are going to do this below for an arbitrary ℓ) that there are enough such equations, corresponding to NDLFs, such that these equations imply the original ones. This implies that if $\beta(S_0,S_1)$ is distributed uniformly and independently of W for every NDLF β, then the original equation system is satisfied (for any w), and thus $P_{S_0S_1DW}$ is well-defined.

Proof of Theorem 4.5 ("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^ℓ holds perfectly.

THE PERFECT CASE: Since the case $\ell = 1$ is already settled, we assume that $\ell \geq 2$. We generalize the idea from the case $\ell = 2$. The main issue will be to transform the equation guaranteed by the assumption on the linear functions into the ones required for $P_{S_0S_1DW}(\cdot,\cdot,0,w) + P_{S_0S_1DW}(\cdot,\cdot,1,w) = P_{S_0S_1W}(\cdot,\cdot,w)$.

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 $\ell = 1$ or $\ell = 2$, 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.

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, 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, because $a_0, a_1 \in \{0,1\}^\ell$ 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. In our situation, 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).

It remains to justify the assumption that $p_{\mathbf{o},\mathbf{o}} \leq p_{\mathbf{o},s_1}$ for any s_1. 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 equation $p_{s_0,t} + p_{\mathbf{o},s_1} = p_{\mathbf{o},t} + p_{s_0,s_1}$ that needs to be satisfied for $s_0 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$ and $s_1 \in \{0,1\}^\ell \setminus \{t\}$. This equality, though, can be argued as for equation (2), which we did above, simply by replacing p_{σ_0,σ_1} on both sides of (3) by $p_{\sigma_0,\sigma_1 \oplus t}$ (where $\oplus$ is the bitwise XOR). We may safely do so: doing a suitable variable substitution and using linearity of the inner product, it is easy to see that this modified equation still expresses uniformity of $\beta(S_0,S_1)$. 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 $\delta\big([\beta(S_0,S_1)W],[\text{UNIF}][W]\big) \leq 2^{-2\ell-1}\varepsilon$ 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 $\sum_w \varepsilon_{w,\beta} = \delta\big([\beta(S_0,S_1)W],[\text{UNIF}][W]\big) \leq 2^{-2\ell-1}\varepsilon$, 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

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

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 $\delta'_{s_0,s_1}, \delta''_{s_0,s_1} \geq 0$ with $\delta'_{s_0,s_1} + \delta''_{s_0,s_1} = \delta_{s_0,s_1}$, and with suitably chosen signs "+" or "−".[6] 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 $\delta\big(P_{S_{1-D}S_DDW}(\cdot,\cdot,0,w), P_{\text{UNIF}}P_{S_DDW}(\cdot,0,w)\big) \leq$

[6] 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.

$\sum_{s_0,s_1} \delta'_{s_0,s_1}$. The corresponding holds for $P_{S_0 S_1 DW}(\cdot,\cdot,1,w)$. It follows that

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

which concludes the proof. □

5 Applications

In this section we will show the usefulness of Theorem 4.5 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 4.5.

5.1 Reducing *1-2 OT*$^\ell$ 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*$^\ell$ 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*$^\ell$ to (seemingly) weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, *1-2 GOT* and *1-2 UOT* [7, 3, 5, 31, 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 $I(B_0 B_1; Y) \leq 1$ in case of *1-2 UOT*.[7]

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

[7] As a matter of fact, reducibility has been proven for any bound on $I(B_0 B_1; Y)$ strictly smaller than 2. Note that there is some confusion in the literature in what a *universal OT*, *UOT*, should be: In [3, 31, 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.

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 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 4.5, in combination with a simple observation regarding the composition of non-degenerate linear (respectively, more general, 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* [29] 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.*[8]

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 and 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 and 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 $\tilde{\mathsf{R}}$ 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 4.5.

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 4.5 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.

[8] 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 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 $H_\alpha(X|Y) \geq r$.[9] 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 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 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. 3. 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 5.2 we then show that its security follows easily from Theorem 4.5.

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 $H(F_1(X_1)|F_1, X_0 = x_0)$ 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 $S_0 \oplus S_1$.

[9] 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.

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 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 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 A.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 5.1 in combination with the privacy amplification theorem, and applying Theorem 4.5. The formal proof given below additionally keeps track of the "error term". From this proof it also becomes clear that the exponential (in ℓ) overhead in Theorem 4.5 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.

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

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

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 and consider any 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 5.1, privacy amplification (Theorem A.3) 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 4.5. □

5.3 Quantitative Comparison

We compare the simple reduction of *1-2 OT*$^\ell$ to n executions of *1-2 XOT*, *1-2 GOT* and *1-2 UOT*, respectively, using our analysis based on Theorem 4.5 as discussed in Section 5.1 together with the quantitative statement given in Theorem 5.2, with the results achieved in [4].[10] The quality

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

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*$^\ell$ 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 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. 4. 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 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 Extending the Results

6.1 *1-n OT*$^\ell$

In this section we extend our characterization of the obliviousness of *Rand 1-2 OT* to *Rand 1-n OT*. We use the following notation. For a sequence of random variables $S_0, S_1, \ldots, S_{n-1}$ and indices $i, j \in \{0, \ldots, n-1\}$, we denote by $\overline{S_{i,j}}$ the sequence of variables $\{S_k : k \in \{0, \ldots, n-1\} \setminus \{i, j\}\}$ with all indices except i and j. Similarly, $\overline{S_i}$ denotes all variables but the ith.

Definition 6.1 (*Rand 1-n OT*$^\ell$). *An ε-secure Rand 1-n OT is a protocol between* S *and* R, *with* R *having input $C \in \{0, 1, \ldots, n-1\}$ (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 $S_0, S_1, \ldots, S_{n-1} \in \{0,1\}^\ell$ and* R *outputs S_C, except with probability ε.*
- *ε-Privacy: If* R *is honest then for any (possibly dishonest) $\tilde{\mathsf{S}}$ with output V, $[CV] \approx_\varepsilon [C][V]$.*
- *ε-Obliviousness: If* S *is honest then for any (possibly dishonest) $\tilde{\mathsf{R}}$ with output W, there exists a random variable D with range $\{0, 1, \ldots, n-1\}$ such that $[\overline{S_D}\, W\, S_D\, D] \approx_\varepsilon [\text{UNIF}^\ell]^{n-1}[W\, S_D\, D]$.*

Analogous to the *1-2 OT*-case we want for obliviousness that there exists a choice D, such that when given the corresponding string (or bit) S_D all the other strings (or bits) look completely random from R's point of view.

Recall that for the characterization of obliviousness in the case of *1-2 OT*, it is sufficient that $[\beta(S_0, S_1)W] = [\text{UNIF}][W]$ for every NDLF β. In a first attempt one might try to characterize obliviousness of *1-n OT* using linear functions β that non-trivially depend on n arguments. In the case of *1-3 OT* of bits, the only linear function of this kind is the XOR of the three bits, but it can be easily verified that the condition that $B_0 \oplus B_1 \oplus B_2$ is uniform does *not* imply obliviousness in the sense defined above. Instead, as we will see below, sufficient requirements are that the XOR of *every pair of bits* is uniform *when given the value of the third.*

Theorem 6.2. *The ε-obliviousness condition for a Rand 1-n OT^ℓ is satisfied for a particular (possibly dishonest) receiver $\tilde{\mathsf{R}}$ with output W, if for all $i \neq j \in \{0,\dots,n-1\}$*

$$[\beta(S_i,S_j)\,W\,\overline{S_{i,j}}] \approx_\nu [\text{UNIF}]\,[W\,\overline{S_{i,j}}]$$

for every NDLF β, where $\nu = \varepsilon/(2^{2\ell}n(n-1))$.

The proof is given in Appendix C.

6.2 *1-2 OT* in a Quantum Setting

The techniques developed in this paper also come in handy in a quantum setting. In upcoming work [13], we present a quantum 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 4.5 which enables us to use the result about privacy amplification against quantum adversaries [27] to conclude that our protocol is oblivious against adversaries with bounded quantum memory as considered in [14]. 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.

The ε-obliviousness condition of a *quantum* protocol for *Rand 1-2 OT* coincides with Definition 3.2, except that the dishonest receiver's output is a quantum state modeled by a random state $\boldsymbol{\rho}$, and closeness is measured in terms of the trace-norm distance of the corresponding quantum states. For more details on the notation, as well as for the proof of Theorem 6.3, we refer to [13].

Theorem 6.3. *The ε-obliviousness condition for a quantum Rand 1-2 OT^ℓ is satisfied for a particular (possibly dishonest) receiver R with output $\boldsymbol{\rho}$ if*

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

for every NDLF β.

7 Conclusion

We have established a characterization of the obliviousness condition for a randomized version of *1-2 OT^ℓ* (Theorem 4.5). Using this characterization in combination with a composition result about strongly universal-two hash functions (Proposition 5.1), 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^ℓ*. 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 2-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. Crepeau. 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)*, 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. Crepeau, 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.
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. In *Advances in Cryptology—CRYPTO '06*, Lecture Notes in Computer Science. Springer, 2006.
16. I. B. Damgard, 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*. 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. O. Goldreich. Three XOR-lemmas - an exposition. *Electronic Colloquium on Computational Complexity (ECCC)*, 2(56), 1995.
21. 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.
22. 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.

23. J. Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, 1988.
24. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17), 1997.
25. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17), 1997.
26. M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
27. 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*. Springer, 2005. Also available at `http://arxiv.org/abs/quant-ph/0403133`.
28. U. V. Vazirani. *Randomness, adversaries and computation.* PhD thesis, University of California, Berkeley, 1986.
29. 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.
30. S. Wiesner. Conjugate coding. *ACM Special Interest Group on Automata and Computability Theory (SIGACT News)*, 15, 1983. Original manuscript written circa 1970.
31. 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 A.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 A.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 which 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 the *left-over hash lemma* [22, 21]:

Theorem A.3 ([21]). *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 4.5 ("only if" part)

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

$$\frac{1}{2}\sum_{w,d,s_0,s_1}\big|P_{S_{1-D}S_DDW}(s_{1-d},s_d,d,w) - 2^{-\ell}P_{S_DDW}(s_d,d,w)\big| \leq \varepsilon.$$

In order to upper bound

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

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

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

and

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

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

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

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

C Proof of Theorem 6.2

We first consider and prove the perfect case.

THE PERFECT CASE: Like in the proof of Theorem 4.5, we fix an output w of the receiver and consider the non-normalized probability distribution $P_{S_0 \dots S_{n-1} W}(\cdot, \dots, \cdot, w)$. We use the variable $p_{s_0,\dots,s_{n-1}}$ to refer to $P_{S_0 \dots S_{n-1} W}(s_0, \dots, s_{n-1}, w)$ and $\mathbf{o}$ for the all-zero string $(0, \dots, 0) \in \{0,1\}^\ell$. Furthermore, we use bold font to denote a collection of strings $\mathbf{s} := (s_0, s_1, \dots, s_{n-1}) \in \{0,1\}^{\ell n}$, and we write $\overline{\mathbf{s}_i}$ for $(s_0, \dots, s_{i-1}, s_{i+1}, \dots, s_{n-1})$, the collection $\mathbf{s}$ without s_i. Finally, for a collection $\mathbf{t} = (t_0, \dots, t_{k-1}) \in \{0,1\}^{\ell k}$ of arbitrary size k, we define sets of indices with one (respectively two) non-zero substrings:

$$\mathcal{S}_1(\mathbf{t}) := \{(\mathbf{o}, \dots, \mathbf{o}, t_i, \mathbf{o}, \dots, \mathbf{o}) : i \in \{0, \dots, k-1\}\}$$
$$\mathcal{S}_2(\mathbf{t}) := \{(\mathbf{o}, \dots, \mathbf{o}, t_i, \mathbf{o}, \dots, \mathbf{o}, t_j, \mathbf{o}, \dots, \mathbf{o}) : i < j \in \{0, \dots, k-1\}\}$$

where the t_i (and t_j) are at ith (and jth) position. As in the proof of Theorem 4.5, we assume for the clarity of exposition that for all $i \in \{0, \dots, n-1\}$ and $s_i \in \{0,1\}^\ell$, it holds that $p_{\mathbf{o},\dots,\mathbf{o}} \le p_{\mathbf{o},\dots,\mathbf{o},s_i,\mathbf{o},\dots,\mathbf{o}}$ (where s_i is at position i). For symmetry reasons, the general case can be handled along the same lines.

We extend the distribution $P_{S_0 \dots S_{n-1} W}(\cdot, \dots, \cdot, w)$ along the lines of (1): for every $\mathbf{s} \in \{0,1\}^{\ell n}$, we set

$$\begin{aligned}
P_{S_0 \dots S_{n-1} D W}(s_0, \dots, s_{n-1}, 0, w) &:= p_{s_0, \mathbf{o}, \dots, \mathbf{o}}, \\
P_{S_0 \dots S_{n-1} D W}(s_0, \dots, s_{n-1}, 1, w) &:= p_{\mathbf{o}, s_1, \mathbf{o}, \dots, \mathbf{o}} - p_{\mathbf{o}, \dots, \mathbf{o}}, \\
&\;\;\vdots \\
P_{S_0 \dots S_{n-1} D W}(s_0, \dots, s_{n-1}, n-2, w) &:= p_{\mathbf{o}, \dots, s_{n-2}, \mathbf{o}} - p_{\mathbf{o}, \dots, \mathbf{o}}, \\
P_{S_0 \dots S_{n-1} D W}(s_0, \dots, s_{n-1}, n-1, w) &:= p_{\mathbf{o}, \dots, \mathbf{o}, s_{n-1}} - p_{\mathbf{o}, \dots, \mathbf{o}}.
\end{aligned}$$

In order to show that this is a valid extension, we have to show that for every $\mathbf{s} \in \{0,1\}^{\ell n}$

$$p_{\mathbf{s}} = \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - (n-1) p_{\mathbf{o}, \dots, \mathbf{o}}. \tag{5}$$

If this holds, then the random variable D is well defined, and the $\overline{S_D}$ are uniformly distributed given D, S_D and W.

We now show that (5) follows from the assumed uniformity property that $[\beta(S_i, S_j)\, W | \overline{S_{i,j}} = \overline{\mathbf{s}_{i,j}}] = [\text{UNIF}]\,[W | \overline{S_{i,j}} = \overline{\mathbf{s}_{i,j}}]$ for every non-degenerate linear function β and any $i \neq j$. This is done by induction on n. The case $n = 2$ is covered by the proof of Theorem 4.5, and by induction assumption we may assume that it also holds for $n-1$. Let us fix some $\mathbf{s} \in \{0,1\}^{\ell n}$ and $i \in \{0, \dots, n-1\}$. It is easy to see that the assumed uniformity property on $S_0, \dots, S_{n-1}, W$ implies the corresponding uniformity property on $\overline{S_i}, W$ when conditioning on $S_i = s_i$, and therefore, by induction assumption and "multiplying out the conditioning",

$$p_{\mathbf{s}} = \sum_{\mathbf{t}} p_{\mathbf{t}} - (n-2) p_{\mathbf{o}, \dots, \mathbf{o}, s_i, \mathbf{o}, \dots, \mathbf{o}}\,. \tag{6}$$

where the sum is over all $\mathbf{t} \in \{0,1\}^{\ell n}$ with $t_i = s_i$ and $\overline{\mathbf{t}_i} \in \mathcal{S}_1(\overline{\mathbf{s}_i})$. Summing all the equations over $i \in \{0, \dots, n-1\}$ yields

$$n \cdot p_{\mathbf{s}} = 2 \sum_{\mathbf{t} \in \mathcal{S}_2(\mathbf{s})} p_{\mathbf{t}} - (n-2) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}}\,. \tag{7}$$

By a similar reasoning we can also derive from the case $n = 2$ that equations of type (2) hold conditioned on the event that all but two of the S_i's are zero. More formally, we have that for all $i < j \in \{0, \dots, n-1\}$,

$$p_{\mathbf{o}, \dots, \mathbf{o}, s_i, \mathbf{o}, \dots, \mathbf{o}, s_j, \mathbf{o}, \dots, \mathbf{o}} = p_{\mathbf{o}, \dots, \mathbf{o}, s_i, \mathbf{o}, \dots, \mathbf{o}} + p_{\mathbf{o}, \dots, \mathbf{o}, s_j, \mathbf{o}, \dots, \mathbf{o}} - p_{\mathbf{o}, \dots, \mathbf{o}}. \tag{8}$$

Summing these equations over all $i < j \in \{0, \ldots, n-1\}$ yields

$$\sum_{\mathbf{t} \in \mathcal{S}_2(\mathbf{s})} p_{\mathbf{t}} = (n-1) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - \binom{n}{2} p_{\mathbf{o},\ldots,\mathbf{o}} \tag{9}$$

We conclude by substituting (9) into (7) as follows

$$\begin{aligned} n \cdot p_{\mathbf{s}} &= 2 \sum_{\mathbf{t} \in \mathcal{S}_2(\mathbf{s})} p_{\mathbf{t}} - (n-2) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} \\ &= 2 \left((n-1) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - \binom{n}{2} p_{\mathbf{o},\ldots,\mathbf{o}} \right) - (n-2) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} \\ &= n \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - n(n-1) p_{\mathbf{o},\ldots,\mathbf{o}}, \end{aligned}$$

which is equation (5) after dividing by n, and thus finishes the induction step and the claim for $\varepsilon = 0$.

THE GENERAL CASE: For the non-zero error case, we follow the above argument, but keep track of the error. For technical reasons, we assume that the S_i's are independent and uniformly distributed, and we assume that the assumed uniformity property with respect to NDLFs holds conditioned on $\overline{S_{i,j}} = \overline{\mathbf{s}_{ij}}$ for *any* $\overline{\mathbf{s}_{ij}}$, not just on average, i.e., $[\beta(S_i, S_j) W | \overline{S_{i,j}} = \overline{\mathbf{s}_{ij}}] \approx_\nu [\textsc{unif}] [W | \overline{S_{i,j}} = \overline{\mathbf{s}_{ij}}]$ for any $\overline{\mathbf{s}_{ij}} \in \{0,1\}^{\ell(n-2)}$. We show at the end of the proof how to argue in general. Write

$$\delta_{\mathbf{s}} = \Big| \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - (n-1) p_{\mathbf{o},\ldots,\mathbf{o}} - p_{\mathbf{s}} \Big|$$

such that (5) holds up to the error $\delta_{\mathbf{s}}$. Note that $\delta_{\mathbf{s}}$ depends on w; we also write $\delta_{\mathbf{s}}(w)$ to make this dependency explicit. We will argue, following the induction proof, that

$$\sum_{w,\mathbf{s}} \delta_{\mathbf{s}}(w) \leq n(n-1) \cdot 2^{2\ell} \cdot \nu = \varepsilon \,.$$

The proof can then be completed analogue to the proof of Theorem 4.5 by "correcting" the values for $P_{S_0 \ldots S_{n-1} DW}$'s appropriately.

By the proof of Theorem 4.5, the claimed inequality holds in case $n = 2$. For the induction step, note that by induction assumption, (6) holds up to $\delta_{\overline{\mathbf{s}_i}}(w) P_{S_i}(s_i)$ where

$$\sum_{w,\overline{\mathbf{s}_i}} \delta_{\overline{\mathbf{s}_i}}(w) \leq (n-1)(n-2) \cdot 2^{2\ell} \cdot \nu \,.$$

Furthermore, from the case $n = 2$ it follows that (8) holds up to $\delta_{s_i,s_j}(w) P_{\overline{S_{ij}}}(\mathbf{o} \cdots \mathbf{o})$, where

$$\sum_{w,s_i,s_j} \delta_{s_i,s_j}(w) \leq 2^{2\ell+1} \cdot \nu$$

and, by the additional assumption posed on the S_i's, $P_{\overline{S_{ij}}}(\mathbf{o} \cdots \mathbf{o}) = 2^{-(n-2)\ell}$. It follows that (5) holds up to

$$\delta_{\mathbf{s}} = \frac{1}{n} \Big(\sum_i \delta_{\overline{\mathbf{s}_i}} P_{S_i}(s_i) + 2 \sum_{i<j} \delta_{s_i,s_j} P_{\overline{S_{ij}}}(\mathbf{o} \cdots \mathbf{o}) \Big)$$

such that

$$
\begin{aligned}
\sum_{w,\mathbf{s}} \delta_{\mathbf{s}}(w) &= \frac{1}{n}\Big(\sum_i \sum_{w,\overline{\mathbf{s}_i}} \delta_{\overline{\mathbf{s}_i}}(w) \sum_{s_i} P_{S_i}(s_i) + 2\sum_{i<j}\sum_{\overline{\mathbf{s}_{ij}}}\sum_{w,s_i,s_j} \delta_{s_i,s_j}(w) P_{\overline{S_{ij}}}(\mathbf{o}\cdots\mathbf{o})\Big) \\
&\le (n-1)(n-2)\cdot 2^{2\ell}\cdot\nu + (n-1)\cdot 2^{(n-2)\ell}\cdot 2^{2\ell+1}\cdot 2^{-(n-2)\ell}\cdot\nu \\
&= \big((n-1)(n-2)\cdot 2^{2\ell} + 2\cdot(n-1)\cdot 2^{2\ell}\big)\cdot\nu \\
&\le n(n-1)\cdot 2^{2\ell}\cdot\nu = \varepsilon\,.
\end{aligned}
$$

It remains to argue the case where the S_i's are not independent uniformly distributed and/or the assumed uniformity property holds only on average over the $\overline{\mathbf{s}_{ij}}$'s. We first argue that we may indeed assume without loss of generality that the S_i's are random: We consider $\tilde{S}_0,\ldots,\tilde{S}_{n-1},\tilde{W}$ defined as $\tilde{S}_i = S_i \oplus R_i$ and $\tilde{W} = [W, R_0, \ldots, R_{n-1}]$ for independent and uniformly distributed R_i's in $\{0,1\}^\ell$. It is easy to see that the assumed uniformity condition with respect to NDLFs on $S_0,\ldots,S_{n-1},W$ implies the corresponding uniformity condition on $\tilde{S}_0,\ldots,\tilde{S}_{n-1},\tilde{W}$ with the same "error" ν, and it is obvious that the $\tilde{S}_i$'s are independent and uniformly distributed. Furthermore, it is easy to see that the ε-obliviousness condition for $\tilde{S}_0,\ldots,\tilde{S}_{n-1},\tilde{W}$ implies the ε-obliviousness condition for $S_0,\ldots,S_{n-1},W$ with the same ε. Thus it suffices to prove the claim for the case of random S_i's.

Finally, in order to reason that we may assume that the uniformity property holds conditioned on every $\overline{\mathbf{s}_{ij}}$, where we now may already assume that the S_i's are random due to the above observation, we again consider $\tilde{S}_0,\ldots,\tilde{S}_{n-1},\tilde{W}$ defined as above. It is not hard to verify that due to this randomization and since the S_i's are random, the average near-uniformity of $\beta(S_i,S_j)$ translates to a "worst-case" near-uniformity of $\beta(\tilde{S}_i,\tilde{S}_j)$ with the same ν. □