On the Foundations of Oblivious Transfer

Christian Cachin*

MIT Laboratory for Computer Science
545 Technology Square
Cambridge, MA 02139, USA
cachin@acm.org

Abstract. We show that oblivious transfer can be based on a very general notion of asymmetric information difference. We investigate a *Universal Oblivious Transfer*, denoted UOT(X, Y), that gives Bob the freedom to access Alice's input X in an arbitrary way as long as he does not obtain full information about X. Alice does not learn which information Bob has chosen. We show that oblivious transfer can be reduced to a single execution of UOT(X, Y) with Bob's knowledge Y restricted in terms of Rényi entropy of order $\alpha > 1$. For independently repeated UOT the reduction works even if only Bob's Shannon information is restricted, i.e. if $H(X|Y) > 0$ in every UOT(X, Y). Our protocol requires that honest Bob obtains at least half of Alice's information X without error.

Keywords. Cryptographic Protocols, Oblivious Transfer, Shannon Entropy, Rényi Entropy, Statistical Security, Multiparty Computation.

1 Introduction

Oblivious transfer is a cornerstone in the foundations of cryptography. Oblivious transfer was introduced some time ago in several variations [24,15] and has since become the basis for realizing a broad class of interactive protocols, such as bit commitment, zero-knowledge proofs, and general secure multiparty computation [26,16,17,21].

In this paper, we view oblivious transfer (OT) as asymmetric information distribution between two participants. An OT from Alice to Bob corresponds to a pair of correlated random variables X and Y with specially connected distributions. Alice's input X is transformed into Bob's output Y according to the specification of the OT protocol.

In Rabin's OT, Alice sends a bit that is received by Bob with probability $\frac{1}{2}$ [24]; in chosen one-out-of-two OT, denoted by $\binom{2}{1}$-OT, Bob has the choice of obtaining one of two bits sent by Alice [15]. A generalized oblivious transfer (GOT) allows Bob to choose among all binary functions from Alice's two bits [5].

All of these are protocols in which Alice is willing to apply a probabilistic mapping to her information X, i.e., to send X over some channel $X \to Y$ to Bob, where Bob may choose the channel hidden from Alice from a previously agreed-on set and/or the channel may add noise to the transmission.

* Supported by the Swiss National Science Foundation (SNF).

The question we investigate is: What if we allow Bob to choose from a much more general class of channels that is characterized only by the *amount of information* that observing the channel output gives about the input? The corresponding primitive is called a *universal oblivious transfer* (UOT) and has been proposed by Brassard and Crépeau [4]. For example, Bob could be allowed to read both of Alice's bits through a binary symmetric channel, which flips each bit independently with some probability. Or Bob could compute secretly any function of Alice's information as long as the function's range is smaller than its domain.

In terms of correlated random variables, UOT is a protocol in which Bob can choose P_{XY}, the joint distribution of X and Y, subject only to an upper limit on the amount of information that Y will give him about X. (Naturally, his choice has to be consistent with P_X, Alice's view of the UOT.) Bob can obtain some part of X without error; our reductions require this part to be at least one half of X, generally.

Key factors that distinguish different flavors of UOT are whether repeated execution of UOT is allowed and which information measure is used to restrict Bob's knowledge.

As an example of UOT consider the black-box function model, as e.g. studied by Kilian [20]. This paper shows how a black box computing any function f with a certain property can be used as the basis for secure two-party protocols. (The extension to multi-party computation is given by Kushilevitz *et al.* [22].) In the two-party case, Alice and Bob send their inputs to f over private channels to the black box but the output of f is public and available to both. The particular f computed by the box is known to Alice and Bob. UOT can be considered as a generalization of this scenario where the box is produced by Bob and f is unknown to Alice; she can only observe the size of the public output.

We stress that this work is not about realizing UOT in terms of other primitives (as e.g. [19]). Furthermore, the results on general secure multiparty computation cited before imply that GOT and its extension to arbitrary lengths can be reduced to $\binom{2}{1}$-OT. (Such a reduction seems however not possible for UOT because Bob can choose to access Alice's information in infinitely many different ways.) The focus of UOT is to weaken Alice's security requirements in oblivious transfer by giving Bob more options to choose from. The question we investigate is how much freedom Bob can be given such that UOT still retains the power of oblivious transfer.

1.1 Our Results

Let a *universal oblivious transfer* $\mathrm{UOT}(X, Y)$ be a protocol for a sender Alice and a receiver Bob, where Alice sends a random variable X with alphabet $\mathcal{X}$ and Bob obtains a random variable Y. Bob can secretly specify the distributions $P_{Y|X=x}$ for all $x \in \mathcal{X}$ such that Y does not give Bob complete information about X.

We present security proofs for the reduction of $\binom{2}{1}$-OT to UOT. The results are stated in terms of the extension of $\binom{2}{1}$-OT to k-bit string oblivious transfer,

denoted $\binom{2}{1}$-OT^k [15]. The protocol is essentially the same as used by Brassard and Crépeau for simplifying the implementation of string OT from $\binom{2}{1}$-OT [4] and is based on privacy amplification [2]. In extension of their work, our protocol can be based on any universal hash function. Bob's information is measured in terms of min-entropy H_∞, Rényi entropy H_α of order $\alpha > 1$, and Shannon entropy H (see Section 2 for definitions).

UOT Without Repetition—Rényi Entropy, Min-Entropy (Thm. 3): $\binom{2}{1}$-OT^k string OT can be reduced to a single execution of UOT(X, Y) when $H_\alpha(X|Y = y) = \Omega(\frac{\alpha}{\alpha-1}k)$ for all $y \in \mathcal{Y}$ and $\alpha > 1$; in particular also if $H_\infty(X|Y = y) = \Omega(k)$ for all $y \in \mathcal{Y}$.

Independent Repeated UOT—Shannon Entropy (Thm. 5): String OT can be reduced to independent repetitions of UOT(X, Y) when $H(X|Y) > 0$.

Adaptive Repeated UOT—Shannon Entropy (Thm. 6): String OT can be reduced to n repetitions UOT$(X^{(i)}, Y^{(i)})$ for $i = 1, \ldots, n$, where Bob can choose $P_{X^{(i)}Y^{(i)}}$ adaptively when for all $y^{(1)}, \ldots, y^{(n)}$, it holds $H(X^{(i)}|Y^{(1)} = y^{(1)}, \ldots, Y^{(n)} = y^{(n)}) > 0$.

Connecting the second and third results (Theorems 5 and 6), we show also that string OT cannot be reduced to adaptively linked repetitions of UOT if only $H(X|Y) > 0$ is assumed.

The security of the reductions is statistical, tolerating an exponentially small failure probability and leakage of an exponentially small amount of information.

1.2 Related Work

Reductions among oblivious transfers and disclosure problems have a long history in cryptography. It is known how to implement any of the basic variants, OT, $\binom{2}{1}$-OT, and GOT, in terms of each other [5,11], even in a way where an online protocol uses only precomputed transfers [1]. Several ways to weaken the security assumptions for oblivious transfer were considered previously by Crépeau and Kilian [13].

Research on reductions from $\binom{2}{1}$-OT^k string OT to bitwise $\binom{2}{1}$-OT has for a long time concentrated on using self-intersecting codes for the constructions [6], but recent work by Brassard and Crépeau [4] shows that the reduction can be done much more efficiently using privacy amplification [3,18,2]. This technique allows to weaken the security assumptions for Bob, permitting him not only to read one of the two bits, but also the XOR of both bits or even any binary function of them (GOT). Brassard and Crépeau also suggested the further generalization to UOT. This paper extends their work [4] and solves most of their open problems.

1.3 Organization of the Paper

UOT and the protocol for reducing $\binom{2}{1}$-OT^k to UOT are introduced in Section 3. In Section 4, reduction to one execution of UOT is investigated. Conditions

under which $\binom{2}{1}$-OT^k can be reduced to repeated use of UOT are described in Section 5 and Section 6 examines a further generalization of UOT. We start with defining terminology, assembling some tools, and introducing information-theoretic notions.

2 Preliminaries

We consider four basic variants of oblivious transfer:

OT: In Rabin's OT, Alice sends a bit b and Bob receives either Δ ("failed") or b, both with probability $\frac{1}{2}$, but Alice does not learn which one.

$\binom{2}{1}$-OT: In chosen one-out-of-two OT, Alice has two input bits b_0 and b_1, Bob chooses c and obtains b_c, but Alice does not learn c.

$\binom{2}{1}$-OT^k: In string OT, Alice has two k-bit input strings w_0 and w_1, Bob chooses c and obtains w_c, but Alice does not learn c.

GOT: In generalized OT, Alice has input bits b_0 and b_1, Bob chooses any function $f : \{0,1\}^2 \to \{0,1\}$ and obtains $f(b_0, b_1)$, but Alice does not learn f.

Our reductions follow the information-theoretic definitions of unconditional security for oblivious transfer and other multiparty protocols [6,4,14], but formal treatment lies not in the scope of this paper. Informally, an OT protocol is *correct* if it accomplishes the transmission of information between honest parties. The protocol is *private* if a malicious party cannot obtain information about the honest party's input beyond the specification, except with negligible probability. Since UOT is by definition perfectly private for Bob, privacy is only an issue with respect to Alice (against a malicious Bob).

We now repeat some definitions of information theory [10] and introduce the notation. A random variable X induces a probability distribution P_X over an alphabet $\mathcal{X}$. Random variables are denoted by capital letters. The cardinality of a set $\mathcal{S}$ is denoted by $|\mathcal{S}|$ and logarithms are to the base 2. Usually, the alphabet of a random variable is denoted by the corresponding script letter. Concatenation is denoted by $\circ$ or by juxtaposition.

The *(Shannon) entropy* of a random variable X with probability distribution P_X and alphabet $\mathcal{X}$ is defined as

$$H(X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x).$$

The *binary entropy function* is $h(p) = -p \log p - (1-p) \log(1-p)$. The *conditional entropy* of X conditioned on a random variable Y is

$$H(X|Y) = \sum_{y \in \mathcal{Y}} P_Y(y) H(X|Y = y)$$

where $H(X|Y = y)$ denotes the entropy of the conditional probability distribution $P_{X|Y=y}$.

The *Rényi entropy of order* α of a random variable X with alphabet $\mathcal{X}$ is

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_{x \in \mathcal{X}} P_X(x)^\alpha$$

for $\alpha \geq 0$ and $\alpha \neq 1$ [25]. The limit of Rényi entropy for $\alpha \to 1$ is Shannon entropy. The other limiting case $\alpha \to \infty$ is *min-entropy*, defined as

$$H_\infty(X) = -\log \max_{x \in \mathcal{X}} P_X(x).$$

For a fixed random variable X, Rényi entropy is a continuous positive decreasing function of α. For $0 < \alpha < \beta$, we have $H_\alpha(X) \geq H_\beta(X)$, with equality if and only if X is the uniform distribution over a subset of $\mathcal{X}$. In particular

$$\log |\mathcal{X}| \geq H(X) \geq H_2(X) \geq H_\infty(X). \tag{1}$$

The well-known *Fano inequality* gives a lower bound on the error probability of guessing X from knowledge of a correlated random variable Y [10]. W.l.o.g. the estimate $\widehat{X}$ for X is a function of Y. The Fano inequality states that the error probability $p_e = \mathrm{P}[\widehat{X} \neq X]$ satisfies

$$h(p_e) + p_e \log(|\mathcal{X}| - 1) \geq H(X|Y). \tag{2}$$

Universal hash functions were introduced by Carter and Wegman [9]. A *universal hash function* is a set $\mathcal{G}$ of functions $\mathcal{X} \to \mathcal{Y}$ if, for all distinct $x_1, x_2 \in \mathcal{X}$, there are at most $|\mathcal{G}|/|\mathcal{Y}|$ functions g in $\mathcal{G}$ such that $g(x_1) = g(x_2)$.

Entropy smoothing by universal hashing is a widely-used technique to concentrate the randomness inherent in a probability distribution known in different contexts as privacy amplification [3,2] or the leftover hash lemma [18].

In cryptography, privacy amplification can be used to extract a short secret key from shared information about which an adversary has partial knowledge. Assume Alice and Bob share a random variable W, while an eavesdropper Eve knows a correlated random variable V that summarizes her knowledge about W. The details of the distribution P_{WV}, and thus of Eve's information V about W, are unknown to Alice and Bob, except that they assume a lower bound on the Rényi entropy of order 2 of $P_{W|V=v}$ for the particular value v that Eve observes.

Using a public channel, which is susceptible to eavesdropping but immune to tampering, Alice and Bob wish to agree on a function g such that Eve knows nearly nothing about $g(W)$. The following theorem shows that if Alice and Bob choose g at random from a universal hash function $\mathcal{G} : \mathcal{W} \to \mathcal{Y}$ for suitable $\mathcal{Y}$, then Eve's information about $Y = g(W)$ is negligible.

Theorem 1 (Privacy Amplification [2]). *Let X be a random variable over the alphabet $\mathcal{X}$ with Rényi entropy $H_2(X)$, let G be the random variable corresponding to the random choice (with uniform distribution) of a member of a universal hash function $\mathcal{G} : \mathcal{X} \to \mathcal{Y}$, and let $Y = G(X)$. Then*

$$H(Y|G) \geq \log |\mathcal{Y}| - \frac{2^{\log |\mathcal{Y}| - H_2(X)}}{\ln 2}. \tag{3}$$

To apply the theorem in the described scenario, replace P_X by the conditional probability distribution $P_{W|V=v}$. The theorem can be extended from Rényi entropy of order 2 to any order $\alpha > 1$ [8].

Proofs for applications of privacy amplification often involve *spoiling knowledge* [2,7]: Suppose side information is made available to Bob by an oracle. The side information is tailored for Bob's distribution and serves the purpose of increasing his Rényi entropy of order 2. This can be exploited to extract a larger secret key by privacy amplification. Note that the oracle giving spoiling knowledge is used only as a proof technique and not for carrying out privacy amplification.

We will need the following lemma about the reduction of min-entropy induced by observing side information.

Lemma 2. *Let X and U be random variables with alphabets $\mathcal{X}$ and $\mathcal{U}$, respectively, and let s be a security parameter. With probability at least $1 - 2^{-s}$, U takes on a value u for which*

$$H_\infty(X|U=u) \;\geq\; H_\infty(X) - \log|\mathcal{U}| - s.$$

Proof. Let $p_0 = 2^{-s}/|\mathcal{U}|$. Then values u for which $P_U(u) < p_0$ occur with probability less than 2^{-s}. Thus, for all u with $P_U(u) \geq p_0$ and for any x

$$P_{X|U=u}(x) \;=\; \frac{P_{XU}(x,u)}{P_U(u)} \;\leq\; \frac{P_X(x)}{P_U(u)} \;\leq\; \frac{P_X(x)}{p_0} \;=\; P_X(x)\cdot|\mathcal{U}|\cdot 2^s.$$

The lemma follows by taking logarithms. □

3 Universal Oblivious Transfer (UOT)

We introduce our notion of a universal oblivious transfer, in which only the amount of information that Bob obtains about the input is bounded and describe the protocol that is used for reducing string OT to UOT under several assumptions.

Definition 1. A *universal oblivious transfer*, denoted by $\mathrm{UOT}(X,Y)$, is a protocol for a sender Alice and a receiver Bob, where Alice sends a random variable X with alphabet $\mathcal{X}$ and Bob obtains a random variable Y. Bob can secretly specify the distributions $P_{Y|X=x}$ for all $x \in \mathcal{X}$ such that Y does not give Bob complete information about X.

Remark. The requirement that Bob "is not given complete information" about X is deliberately imprecise. In terms of entropy this could be expressed by the condition $H(X|Y) > 0$. But for the reductions to UOT, we usually need stronger and more complex assumptions about P_{XY}. It is therefore the general idea of Bob choosing and obtaining some, but not all information that the notion of a universal oblivious transfer tries to capture. We insist, however, that the restriction of Bob's information is given in terms of an information measure, such as entropy. In particular, the size of Y is not explicitly bounded, as is the case for $\binom{2}{1}$-OT or GOT.

Since Bob's input to the UOT, the distributions $P_{Y|X=x}$ for $x \in \mathcal{X}$, is equivalent to specifying P_{XY} consistent with Alice's P_X, these formulations are used interchangeably. For the simplicity of notation, we assume that Alice's input to the UOT is a binary string of fixed length.

We use the following protocol to implement UOT and prove its security later with different restrictions on Bob's information about X. This protocol has been used by Brassard and Crépeau for the efficient reduction of string OT to $\binom{2}{1}$-OT and to GOT [4].

In the protocol and the security proofs in Section 4, X is a binary string of length $2n$ that is the concatenation of two n-bits strings X_0 and X_1. However, X could be any uniformly distributed random variable with at least 2^{2n} values. The protocol implements a reduction of $\binom{2}{1}$-$\mathrm{OT}^k(w_0, w_1)(c)$ to $\mathrm{UOT}(X, Y)$, such that $\mathcal{X} = \{0,1\}^{2n}$.

3.1 The Protocol for $\binom{2}{1}$-$\mathrm{OT}^k(w_0, w_1)(c)$

1: Let $X = X_0 \circ X_1$, where X_0 and X_1 both are random binary strings of length n and chosen by Alice according to the uniform distribution.
2: Alice and Bob run $\mathrm{UOT}(X, Y)$, where Bob chooses $P_{Y|X=x}$ for $x \in \mathcal{X}$ to obtain X_c, i.e. such that $Y = X_c$.
3: Alice chooses independently two members G_0, G_1 from a universal hash function mapping n-bit strings to k-bit strings and announces them to Bob.
4: Alice computes $M_0 = G_0(X_0)$ and $M_1 = G_1(X_1)$. She encodes w_0 and w_1 as $Z_0 = M_0 \oplus w_0$ and $Z_1 = M_1 \oplus w_1$ and sends Z_0 and Z_1 to Bob.
5: Bob computes w_c as $G_c(Y) \oplus Z_c$.

We first investigate a single execution of UOT in Section 4. Then we slightly modify the protocol for Section 5 and examine the repeated use of UOT in step 2 of the protocol. It makes sense to distinguish these two cases: On the one hand, repetitions can often be treated independently of each other—such methods are used widely. On the other hand, there are scenarios in which repetition of an experiment does not help because the adversary is free to link repetitions arbitrarily.

4 UOT Without Repetition

We show under what conditions a k-bit string OT, $\binom{2}{1}$-$\mathrm{OT}^k(w_0, w_1)(c)$, can be reduced to a single execution $\mathrm{UOT}(X, Y)$. Recall that Bob free to specify P_{XY} at his choice and that $X = X_0 \circ X_1$ consists of two n-bit strings. If Bob is honest, he follows the above protocol and obtains $Y = X_c$. Alice knows only X and the restriction on Bob's output Y.

Theorem 3. *Let $s > 0$, let $\alpha > 1$, and let $UOT(X, Y)$ be a universal oblivious transfer such that X is a $2n$-bit string and $H_\alpha(X|Y = y) \geq l$ for all $y \in \mathcal{Y}$, where*

$$n \geq l \geq \frac{\alpha}{\alpha - 1}\big(2k + \log(n + s + 3) + 3s + 2\big). \tag{4}$$

Then $\binom{2}{1}$-OT^k string OT can be reduced to a single execution of $UOT(X, Y)$.

In particular, these conditions hold if $H_\infty(X|Y=y) \geq l$ *for all* $y \in \mathcal{Y}$, *where*

$$n \;\geq\; l \;\geq\; 2k + \log(n+s+3) + 3s + 2. \tag{5}$$

Remark. In all our results, s is implicitly used as the security parameter. The resulting $\binom{2}{1}$-OT^k protocol is perfectly private for Bob (Alice learns nothing about Bob's choice by the definition of the UOT) and unconditionally private for Alice with leaking at most 2^{-s} bits of information to Bob, except with probability 2^{-s}.

Proof. It is straightforward to verify that the protocol is correct. We show that Bob has substantial uncertainty about at least one of X_0, X_1 after step 3 of the protocol. From this we conclude that he obtains at most an exponentially small amount of information about either M_0 or M_1 and thus also about one of w_0, w_1 because w_0 and w_1 are encrypted with a one-time pad using M_0 and M_1 as keys, respectively.

In the proof we examine Bob's uncertainty about X_0 and his uncertainty about X_1 given any particular value of X_0. A similar argument applies with X_0 and X_1 interchanged.

First, we note that the main statement of the theorem (4) follows from the second statement (5) by the following observation. For any $\alpha > 1$ and any random variable V, it holds

$$\frac{\alpha}{\alpha-1} H_\infty(V) \;=\; \frac{1}{1-\alpha} \log \max_{v \in \mathcal{V}} P_V(v)^\alpha \;\geq\; \frac{1}{1-\alpha} \log \sum_{v \in \mathcal{V}} P_V(v)^\alpha \;=\; H_\alpha(V).$$

Therefore, if $H_\alpha(X|Y=y)$ is at least $\frac{\alpha}{\alpha-1}$ times bigger than $H_\infty(X|Y=y)$, the general bound (4) follows from (5). This leaves to prove the particular case (5).

Fix the particular y that Bob has received. Suppose he obtains from an Oracle side information that depends on his distribution $P_{X_0|Y=y}$. The purpose of side information is to induce an almost uniform distribution on Bob's view of X_0. Although Bob may not actually receive the side information, he cannot deny having seen it and therefore have *more* knowledge.

The side information is the random variable $U = f(X_0)$ with alphabet $\mathcal{U} = \{0, \ldots, d\}$ for some fixed d to be specified later, defined by

$$f(x) \;=\; \begin{cases} d & \text{if } P_{X_0|Y=y}(x) \leq 2^{-d} \\ \lfloor -\log P_{X_0|Y=y}(x) \rfloor & \text{otherwise.} \end{cases}$$

(Side information U of this type has also been called *log-partition spoiling knowledge* [8]). U partitions the values of X_0 into sets of approximately equal probability under $P_{X_0|Y=y,U=u}$. For $d \geq \log|\mathcal{X}|_0 = n$, the values of the probability distributions $P_{X_0|Y=y,U=u}$ differ at most by a factor of two for all u except for $u = d$ and therefore

$$\frac{1}{2} \max_{x_0} P_{X_0|Y=y,U=u}(x_0) \;\leq\; \min_{x_0} P_{X_0|Y=y,U=u}(x_0). \tag{6}$$

We now make sure that $U \neq d$ with high probability. Choosing $d = n + s + 2$ guarantees that

$$\mathrm{P}[U = d] \;=\; \sum_{x_0 \,:\, P_{X_0|Y=y}(x_0) < 2^{-d}} P_{X_0|Y=y}(x_0) \;\leq\; 2^{n-d} \;<\; 2^{-s-1}. \qquad (7)$$

We assume $u \neq d$ for the rest of the proof. Lemma 2 imposes an upper bound on the reduction of Bob's min-entropy about X_0X_1 induced by observing the side information U. With probability at least $1 - 2^{-s-1}$, U takes on a value u such that

$$\begin{aligned} H_\infty(X_0X_1|Y = y, U = u) \;&\geq\; H_\infty(X_0X_1|Y = y) - \log(d+1) - s - 1 \\ &\geq\; 2k + 2s + 1, \end{aligned} \qquad (8)$$

where the second step follows from the assumption of the theorem. We have for all x_0 and x_1

$$\begin{aligned} &\max_{(x_0', x_1')} P_{X_0X_1|Y=y,U=u}(x_0', x_1') \\ &\qquad \geq P_{X_0|Y=y,U=u}(x_0) \cdot P_{X_1|Y=y,U=u,X_0=x_0}(x_1) \\ &\qquad \geq \min_{x_0'} P_{X_0|Y=y,U=u}(x_0') \cdot P_{X_1|Y=y,U=u,X_0=x_0}(x_1) \\ &\qquad \geq \frac{1}{2} \max_{x_0'} P_{X_0|Y=y,U=u}(x_0') \cdot P_{X_1|Y=y,U=u,X_0=x_0}(x_1) \end{aligned}$$

where the last step follows from (6). Because this holds for all x_1, we can rewrite it in terms of min-entropy. Inserting (8) we obtain

$$\begin{aligned} H_\infty(X_0|Y = y, U = u) + H_\infty(X_1|Y = y, U = u, X_0 = x_0) \\ \geq\; H_\infty(X_0X_1|Y = y, U = u) - 1 \;\geq\; 2k + 2s \end{aligned} \qquad (9)$$

for all x_0. Either the min-entropy of X_0 or the min-entropy of X_1 given any particular value of X_0 is at least $k + s$.

Privacy amplification transforms the n-bit strings X_0 and X_1 into the k-bit strings M_0 and M_1. Because the min-entropy of a random variable is a lower bound for its Rényi entropy of order two, Theorem 1 guarantees that Bob's information about either M_0 or M_1 given any $X_0 = x_0$ is exponentially small in s. Formally, there is a value $t \geq 0$ such that $H_\infty(X_0|Y = y, U = u) = t$ and

$$H(M_0|G_0, Y = y, U = u) \;\geq\; k - 2^{k-t}/\ln 2$$

on the one hand and $H_\infty(X_1|Y = y, U = u, X_0 = x_0) \geq H_\infty(X_0X_1|Y = y, U = u) - t \geq 2k + 2s - t$ and

$$H(M_1|G_1, Y = y, U = u, X_0 = x_0) \;\geq\; k - 2^{-k+t-2s}/\ln 2$$

for any x_0 on the other hand. (To apply Theorem 1, we have made implicit use of (1).) At least one of the exponents is not greater than $-s$. This analysis can fail in (7) or (8) with probability at most 2^{-s-1} each, so that the overall failure probability is bounded by 2^{-s}. □

In particular, the above theorem covers the case that Bob knows any deterministic function of X with output size no more than $2n - l$ bits, i.e. such that $Y = f(X)$ satisfies $\log|\mathcal{Y}| \leq 2n - l$. The following corollary is an immediate consequence of fact that P_X is the uniform distribution over $2n$-bit strings.

Corollary 4. *Let $s > 0$ and let UOT$(X, f(X))$ be a universal oblivious transfer such that X is a $2n$-bit string and Bob can obtain $f(X)$ for any function f of his choice with output size at most $2n-l$ bits, where $n \geq l \geq 2k+\log(n+s+3)+3s+2$. Then $\binom{2}{1}$-OT^k string OT can be reduced to a single execution of UOT$(X, f(X))$.*

As mentioned in Section 1.2, string OT can be reduced to generalized oblivious transfer (GOT), where Bob can obtain any *binary* function from a pair of bits held by Alice [4]. The reduction from string OT uses GOT n times, so that Bob in fact can obtain any n-bit function of n pairs of bits that can be computed pairwise. Corollary 4 generalizes this to arbitrary n-bit functions of Alice's $2n$ bits.

We note that Theorem 3 is the most general result with respect to α that we can obtain in the non-repetitive case. For $\alpha \to 1$, Rényi entropy of order α becomes Shannon entropy, but a lower bound on the Shannon entropy $H(X|Y = y)$ is not sufficient for applying privacy amplification [2]. For example, suppose $H(X|Y = y) \geq l$. Then Bob could choose to obtain the complete $2n$-bit string X with probability $\approx 1 - \frac{l}{2n}$ and an uncorrelated $2n$-bit string otherwise. No matter what Alice does, Bob obtains Alice's complete information with constant probability.

5 Repeated UOT

In this section we consider repeated application UOT from pairs of bits. The n bit pairs sent by Alice are denoted by

$$X^{(1)} = X_0^{(1)} \circ X_1^{(1)} \ , \ \ldots \ , \ X^{(n)} = X_0^{(n)} \circ X_1^{(n)}$$

and the random variables received by Bob are $Y^{(1)}, \ldots, Y^{(n)}$. The repetitions are denoted by UOT$(X^{(i)}, Y^{(i)})$ for $i = 1, \ldots, n$ and the second step in the protocol is replaced by:

2': For $i = 1, \ldots, n$, Alice and Bob run UOT$(X^{(i)}, Y^{(i)})$, where Bob chooses $P_{Y^{(i)}|X^{(i)}=x^{(i)}}$ for $x^{(i)} \in \{0, 1\}$ such that he obtains $X_c^{(i)}$.

Repeated UOT was proposed by Brassard and Crépeau [4] without explicitly addressing the question of independence among the instances of UOT. We distinguish between three forms of dependence for the repetition of UOT in order of increasing generality, corresponding to increasing power for Bob.

Independent UOT: In the most restrictive case, Bob must choose all n UOT to be independent. For example, Bob would have the freedom to obtain all of Alice's bits over a discrete memoryless channel.

Dependent UOT: Bob can induce some dependence among successive UOT such that the resulting probability distribution can be seen as a discrete channel with memory.

Adaptive UOT: The most powerful strategy available to Bob is adaptive. Thus, he chooses the distribution for the i-th UOT based on the outcome of the first $i-1$ UOT.

We consider first independent UOT. In this case, Bob has to fix $P_{Y^{(i)}|X^{(i)}=x^{(i)}}$ for $i = 1, \ldots, n$ in advance and his knowledge about $X^{(i)}$ is determined only by $Y^{(i)}$. We show that if in every UOT Bob does not get the full information about Alice's bits in terms of Shannon entropy, then string OT can be realized from independent repetitions of UOT.

Theorem 5. *Let $s > 0$ and $\beta > 0$. Then $\binom{2}{1}$-OT^k string OT can be reduced to n independent repetitions of UOT(X,Y) such that $X \in \{0,1\}^2$ with uniform distribution, $H(X|Y) \geq \beta$, and $n = \Theta\big((k+s)/\log \frac{1}{p_\beta}\big)$, where p_β is a constant depending on β.*

Proof. Again, the protocol from Section 3 is used, which is easily seen to be correct.

Because Alice's input to the UOT are uniformly random bits and Bob's choices of $P_{Y^{(i)}|X^{(i)}=x^{(i)}}$ are independent, we have for all $i = 1, \ldots, n$,

$$H(X^{(i)}|Y^{(1)} \ldots Y^{(n)}) = H(X^{(i)}|Y^{(i)}).$$

For guessing the value of $X^{(i)}$, Bob needs only consider $Y^{(i)}$. Let $\widehat{X}^{(i)} = f_i(Y^{(i)})$ denote Bob's optimal guess for $X^{(i)}$ and let $p_e^{(i)} = \mathrm{P}[\widehat{X}^{(i)} \neq X^{(i)}]$. Then we have $\mathrm{P}[\widehat{X}^{(1)} = X^{(1)}, \ldots, \widehat{X}^{(n)} = X^{(n)}] = \prod_{i=1}^{n}(1 - p_e^{(i)})$. It follows from the Fano inequality (2) that

$$h(p_e^{(i)}) + p_e^{(i)} \log 3 \;\geq\; H(X^{(i)}|Y^{(i)}) \;\geq\; \beta$$

for all $i = 1, \ldots, n$. Let p_β be the unique value in $[0, \frac{3}{4}]$ satisfying $h(p_\beta) + p_\beta \log 3 = \beta$. It follows that p_β is a lower bound for all $p_e^{(i)}$. The probability that Bob can guess $X^{(1)}, \ldots, X^{(n)}$ correctly is at most $p_\beta{}^n$ and his min-entropy about $X^{(1)}, \ldots, X^{(n)}$, given any particular observation $Y^{(1)} = y^{(1)}, \ldots, Y^{(n)} = y^{(n)}$ satisfies

$$H_\infty(X^{(1)} \ldots X^{(n)}|Y^{(1)} = y^{(1)}, \ldots, Y^{(n)} = y^{(n)}) \;\geq\; -n \log p_\beta.$$

Theorem 3 completes the proof. □

If Bob is allowed *dependent* choice of the UOT, then this reduction is not possible. Consider the following adaptive strategy. Alice transmits n pairs of bits $X^{(i)}$ for $i = 1, \ldots, n$. Let B be a uniformly random bit chosen before the protocol starts. When $B = 0$, Bob chooses his distributions such that $Y^{(i)} = X^{(i)}$ for all $i = 1, \ldots, n$. Otherwise, he does not want to learn anything about

$X^{(1)}, \ldots, X^{(n)}$ at all (e.g. $Y^{(i)} = \Delta$ for all i). This choice satisfies $H(X^{(i)}|Y^{(i)}) \geq 1$ and even $H(X^{(i)}|Y^{(1)} \ldots Y^{(i)}) \geq 1$, but Bob obtains everything from Alice with probability $\frac{1}{2}$.

Although this example suggests that dependence gives Bob too much freedom, *adaptive UOT* can nevertheless be used when Bob's information is restricted in every particular case and not only on the average through the conditional entropy, as in Theorem 5.

Theorem 6. *Let $s > 0$ and $\beta > 0$. Then $\binom{2}{1}$-OT^k string OT can be reduced to n adaptive repetitions of UOT(X, Y) such that $X^{(i)} \in \{0,1\}^2$ with uniform distribution and $H(X^{(i)}|Y^{(1)} = y^{(1)}, \ldots, Y^{(n)} = y^{(n)}) \geq \beta$ for $i = 1, \ldots, n$ and all $y^{(1)}, \ldots, y^{(n)}$, where $n = \Theta\big((k+s)/\log \frac{1}{p_\beta}\big)$ for some constant p_β depending on β.*

Proof. In contrast to the proof of the preceding theorem, Bob's information about $X^{(i)}$ can depend on all of $Y^{(1)}, \ldots, Y^{(n)}$. W.l.o.g. his optimal guess $\widehat{X}^{(i)}$ for $X^{(i)}$ is a deterministic function $f_i(Y^{(1)}, \ldots, Y^{(n)})$ for $i = 1, \ldots, n$. Then for all $y^{(1)}, \ldots, y^{(n)}$, we have conditional independence

$$\mathrm{P}[\widehat{X}^{(1)} = X^{(1)}, \ldots, \widehat{X}^{(1)} = X^{(1)} | Y^{(1)} = y^{(1)}, \ldots, Y^{(n)} = y^{(n)}]$$
$$= \prod_{i=1}^{n} \mathrm{P}[\widehat{X}^{(i)} = X^{(i)} | Y^{(1)} = y^{(1)}, \ldots, Y^{(n)} = y^{(n)}].$$

and the theorem follows from the Fano inequality and from Theorem 3 in a similar way as Theorem 5. □

6 Extensions

In a UOT as described so far, Bob can always access at least half of X without error. It seems possible to extend UOT to the notion of a *noisy UOT*, where Bob cannot obtain even a small part of Alice's information without the chance of an error.

In non-repeated use of noisy UOT, error correction has to succeed always except with negligible probability; methods similar to those used in worst-case communication complexity [23] can be employed to correct errors, but the matter is complicated by the fact that interaction is generally not possible or Alice could learn something about Bob's choice.

For an example of a noisy UOT, assume that in an UOT(X, Y), any number of up to l bits in Alice's bit string $X = X_0 \circ X_1$, are flipped before it is sent over the channel selected by Bob. Then our protocol can still be used to reduce $\binom{2}{1}$-OT^k to noisy UOT when Alice sends Bob also the syndromes of X_0 and X_1 using a linear systematic code that corrects up to l errors. (The reduction of Bob's entropy can be bounded by Lemma 2.)

In repeated use of noisy UOT, better error correction techniques can be applied and the scenario resembles the repeated use of a binary symmetric channel in work to reduce OT to a noisy channel from Alice to Bob [13,12].

The noisy channel model differs from UOT in another way: knowledge about the channel characteristics is *symmetric* for Alice and Bob (both of them know the transition probabilities). In contrast, UOT is inherently asymmetric. We raise the question whether there is a concept of information distribution between two parties that encompasses both UOT and the noisy channel model as special cases.

Acknowledgment

I am grateful to Amos Beimel, Claude Crépeau, Ivan Damgård, Julien Marcil, Ueli Maurer, Markus Stadler, and Alain Tapp for helpful comments and discussions on this work.

References

1. D. Beaver, "Precomputing oblivious transfer," in *Advances in Cryptology: CRYPTO '95* (D. Coppersmith, ed.), vol. 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*, vol. 41, pp. 1915–1923, Nov. 1995.
3. C. H. Bennett, G. Brassard, and J.-M. Robert, "How to reduce your enemy's information," in *Advances in Cryptology: CRYPTO '85* (H. C. Williams, ed.), vol. 218 of *Lecture Notes in Computer Science*, pp. 468–476, Springer, 1986.
4. G. Brassard and C. Crépeau, "Oblivious transfers and privacy amplification," in *Advances in Cryptology: EUROCRYPT '97* (W. Fumy, ed.), vol. 1233 of *Lecture Notes in Computer Science*, pp. 334–347, Springer, 1997.
5. G. Brassard, C. Crépeau, and J.-M. Robert, "Information theoretic reductions among disclosure problems," in *Proc. 27th IEEE Symposium on Foundations of Computer Science (FOCS)*, 1986.
6. G. Brassard, C. Crépeau, and M. Sántha, "Oblivious transfers and intersecting codes," *IEEE Transactions on Information Theory*, vol. 42, pp. 1769–1780, Nov. 1996.
7. C. Cachin, *Entropy Measures and Unconditional Security in Cryptography*, vol. 1 of *ETH Series in Information Security and Cryptography*. Konstanz, Germany: Hartung-Gorre Verlag, 1997. ISBN 3-89649-185-7 (Reprint of Ph.D. dissertation No. 12187, ETH Zürich).
8. C. Cachin, "Smooth entropy and Rényi entropy," in *Advances in Cryptology: EUROCRYPT '97* (W. Fumy, ed.), vol. 1233 of *Lecture Notes in Computer Science*, pp. 193–208, Springer-Verlag, 1997.
9. J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.
10. T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, 1991.
11. C. Crépeau, "Equivalence between two flavours of oblivious transfer," in *Advances in Cryptology: CRYPTO '87* (C. Pomerance, ed.), vol. 293 of *Lecture Notes in Computer Science*, pp. 350–354, Springer, 1988.

12. C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Advances in Cryptology: EUROCRYPT '97* (W. Fumy, ed.), vol. 1233 of *Lecture Notes in Computer Science*, pp. 306–317, Springer, 1997.
13. C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions," in *Proc. 29th IEEE Symposium on Foundations of Computer Science (FOCS)*, 1988.
14. I. B. Damgård, T. P. Pedersen, and B. Pfitzmann, "Statistical secrecy and multi-bit commitments." BRICS Report, RS-96-45, 1996.
15. S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," in *Proc. CRYPTO '82* (R. L. Rivest, A. Sherman, and D. Chaum, eds.), pp. 205–210, Plenum Press, 1983.
16. O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Proc. 19th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 218–229, 1987.
17. O. Goldreich and R. Vainish, "How to solve any protocol problem – an efficiency improvement," in *Advances in Cryptology: CRYPTO '87* (C. Pomerance, ed.), vol. 293 of *Lecture Notes in Computer Science*, pp. 73–86, Springer, 1988.
18. R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. 21st Annual ACM Symposium on Theory of Computing (STOC)*, pp. 12–24, 1989.
19. Y. Ishai and E. Kushilevitz, "Private simultaneous messages protocols with applications," in *Proc. 5th Israel Symposium on the Theory of Computing and Systems*, 1997.
20. J. Kilian, "A general completeness theorems for 2-party games," in *Proc. 23rd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 553–560, 1991.
21. J. Kilian, "Founding cryptography on oblivious transfer," in *Proc. 20th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 20–31, 1988.
22. E. Kushilevitz, S. Micali, and R. Ostrovsky, "Reducibility and completeness in multi-party private computations," in *Proc. 35th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 478–489, 1994.
23. A. Orlitsky, "Worst-case interactive communication I: Two messages are almost optimal," *IEEE Transactions on Information Theory*, vol. 36, pp. 1111–1126, Sept. 1990.
24. M. O. Rabin, "How to exchange secrets by oblivious transfer," Tech. Rep. TR-81, Harvard, 1981.
25. A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symposium on Mathematical Statistics and Probability*, vol. 1, pp. 547–561, Univ. of Calif. Press, 1961.
26. A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. 27th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 162–167, 1986.