Efficient Oblivious Transfer Protocols Achieving a Non-Zero Rate from Any Non-Trivial Noisy Correlation

Hideki Imai[*,†] Kirill Morozov[†] Anderson C. A. Nascimento[‡]

Abstract

Oblivious transfer (OT) is a two-party primitive which is one of the cornerstones of modern cryptography. We focus on providing information-theoretic security for both parties, hence building OT assuming noisy resources (channels or correlations) available to them. This primitive is about transmitting two strings such that the receiver can obtain one (and only one) of them, while the sender remains ignorant of this choice. Recently, Winter and Nascimento proved that oblivious transfer capacity is positive for any non-trivial discrete memoryless channel or correlation in the case of passive cheaters. Their construction was inefficient. The OT capacity characterizes the maximal efficiency of constructing OT using a particular noisy primitive. Building on their result, we extend it in two ways: 1) we construct efficient passively-secure protocols achieving the same rates; 2) we show that an important class of noisy correlations actually allows to build OT with non-zero rate secure against active cheating (before, positive rates were only achieved for the erasure channel).

Keywords: Information-theoretical security, oblivious transfer, noisy resources

1 Introduction

Oblivious transfer (OT) [24, 20, 9] is an important and well-studied cryptographic primitive. Being one of the corner stones of modern cryptography,

[*]Department of Electrical, Electronic and Communication Engineering, Chuo University, Japan. Email: h-imai@aist.go.jp

[†]RCIS, AIST, Japan. Email: kirill.morozov@aist.go.jp

[‡]Department of Electrical Engineering, University of Brasilia, Brazil. Email: andclay@ene.unb.br

it implies any secure two-party computation [13]. It comes in many flavors, but all of them turned out to be equivalent [4]. Informally, OT is a means to transmit data such that the sender is guaranteed that the data will be partially lost during the transmission, but he does not know what exactly the receiver gets. It is impossible to obtain OT "from scratch", i.e., in the plain model when information-theoretical security is required for both the sender and the receiver. Hence, one needs additional assumptions. One of them is the use of noisy resources (channels or pre-distributed noisy data, i.e. noisy correlations). This assumption seems quite natural as the real communication channels are inherently noisy. Recently, the concept of oblivious transfer capacity was introduced by Nascimento and Winter [19] (following the manuscript [18]). The OT capacity is a measure of how efficient one can use a noisy resource in order to obtain oblivious transfer from it. In this paper, they proved that any non-trivial discrete memoryless noisy resource can be used for obtaining noisy channels (this was first independently proved in [18] and in [7]). Moreover, for the case of passive cheating, they proved that for any non-trivial noisy resource, its OT capacity is positive by presenting protocols achieving non-zero rate. However, those protocols were inefficient (as they relied on random coding arguments).

In this paper, we show that the results of [19] can be obtained using efficient protocols. For any non-trivial correlation, we present such efficient protocols with non-zero rate, hereby showing that oblivious transfer capacity of these correlations is bounded away from zero in the case of honest-but-curious sender but completely malicious receiver.

Additionally, for a wide class of noisy correlations (here called symmetric basic correlations (SBC)), we completely characterize the oblivious transfer capacity in the case of passive cheaters (with efficient protocols) and show protocols which are optimal up to a constant in the case of active adversaries. We emphasize that previously, all the reductions achieving non-zero rates and based on noisy channels [6, 5, 18, 7] (with the exception of reductions to the erasure channel[1] [8]) always considered an honest-but-curious sender. Hereby, we enlarge the class of channels for which oblivious transfer is practical to SBC.

Symmetric basic correlations are important as many previous protocols for obtaining oblivious transfer from noisy resources used it as an intermediate step towards obtaining a fully secure OT. Thus, computationally efficient and rate-efficient constructions of SBC from noisy resources are of special relevance in noise-based cryptography.

[1] Which is the same as Rabin oblivious transfer [20].

Related work. Crépeau and Kilian [6] showed that any binary symmetric channel provides us with oblivious transfer. The efficiency of this result was consequently improved in [5]. Crepeau's result was extended to any non-trivial binary symmetric channel in [23]. A general characterization of which noisy channels yield oblivious transfer was independently obtained in [14] (with efficient protocols) and in [18] (where the classification was also extended to noisy correlations).

Winter *et al.* [25] introduced the concept of cryptographic capacity of a channel for secure two-party computations. They derived a single-letter characterization of the commitment capacity of a discrete memoryless channel. Recently, Imai *et al.* [12], showed the OT capacity of the erasure channel to be equal to 1/2 in the case of passive cheaters and presented a protocol achieving the rate 1/4 for the case of active cheaters. Using the Interactive Hashing [17], Crépeau and Savvides [8] showed a reduction of string OT to bit OT achieves an optimal rate of 1/2. We conjecture that their protocol can be changed to provide the reduction of the string OT to Rabin OT achieving the optimal rate of 1/2.

Structure of the paper. Section 2 establishes the notation and provides some useful facts from information theory and cryptography. In Section 3, oblivious transfer is formally described and its security definition is provided. The main results together with security proofs are contained in Section 4. Our concluding remarks and the open questions are given in Section 5.

2 Preliminaries

Here we introduce our notation and some tools that are useful in proving our main result.

Given a sample space (a set of events), a random variable X is a mapping from the sample space to a certain range $\mathcal{X}$ and it is characterized by its probability distribution P_X that assigns to every $x \in \mathcal{X}$ the probability $P_X(x)$ of the event that X takes on the value x.

We deal with two kinds of noise: a discrete memoryless channel, generated by the stochastic map $W : \mathcal{X} \longrightarrow \mathcal{Y}$; and secondly: independent, identically distributed (i.i.d.) realizations of a pair of random variables (X, Y) (range $\mathcal{X} \times \mathcal{Y}$ with distribution P_{XY}, in both cases with finite sets $\mathcal{X}, \mathcal{Y}$).

For elements of information theory, we refer the reader to the book by Thomas and Cover [22].

The Shannon entropy of a random variable is a measure of the uncertainty of a random variable X

$$H(X) = -\sum_x P_X(x) \log P_X(x)$$

assuming that $0 \log 0 = 0$. All the logarithms in this papers are taken to the base 2.

The mutual information between two random variables is defined as

$$I(X;Y) = \sum_{x,y} P(x,y) \log \frac{P(x,y)}{P(x)P(y)}$$

The min-entropy of X is

$$H_\infty(X) = \min_y \log(1/P_X(x))$$

The min-entropy of X conditioned on Y is

$$H_\infty(X) = \min_y H_\infty(X|Y=y)$$

We also will use the following quantities

$$H_0(X) = \log |\{x \in X | P_X(x) > 0\}|$$

and

$$H_0(X|Y) = \max_y H_0(X|Y=y)$$

We will use the so-called smooth entropies as defined by Renner and Wolf [21]. For $1 > \epsilon \geq 0$ the ϵ-smooth min-entropy is defined as

$$H_\infty^\epsilon(X) = \max_{X' : \|P_{X'} - P_X\| \leq \epsilon} H_\infty(X)$$

where $\|P_{X'} - P_X\|$ denotes the statistical distance between the distributions $P_{X'}$ and P_X. The conditional min-entropies are defined similarly:

$$H_\infty^\epsilon(X|Y) = \max_{X'Y' : \|P_{X'Y'} - P_{XY}\| \leq \epsilon} H_\infty(X|Y)$$

Analogous definitions exist for smooth $H_0(X)$ and its conditioned version. Smooth entropies are of special importance since many nice properties of Shannon entropies (such as sub-additivity, chain rule and monotonicity), which are known to not hold for H_0 and H_∞, do hold in an approximated

version for smooth entropies [21]. Two of these properties are important for our result.

For any $\epsilon, \epsilon' > 0$, and any distribution P_{XYZ} we have

$$H_\infty^{\epsilon+\epsilon'}(X|YZ) \geq H_\infty^{\epsilon}(XY|Z) - H_0(Y|Z) - \log(1/\epsilon') \tag{1}$$

$$H_\infty^{\epsilon+\epsilon'}(XY|Z) \geq H_\infty^{\epsilon}(X|Z) + H_\infty^{\epsilon'}(Y|XZ) \tag{2}$$

Assuming that Z is independent of XY, we obtain

$$H_\infty^{\epsilon+\epsilon'}(X|Y) \geq H_\infty^{\epsilon}(XY) - H_0(Y) - \log(1/\epsilon') \tag{3}$$

$$H_\infty^{\epsilon+\epsilon'}(XY) \geq H_\infty^{\epsilon}(X) + H_\infty^{\epsilon'}(Y|X) \tag{4}$$

The smooth min-entropy gives us the amount of randomness that can be extracted from a random variable X given some side information Y, as proved in [21]. We will make use of the Left-over Hash-Lemma [15] (also known as privacy amplification [2]). We state the version presented in [11].

Theorem 1 *Let X be a random variable over $\{0,1\}^n$. Let U^n and U^m be independent and uniform over $\{0,1\}^n$ and $\{0,1\}^m$, respectively. There exists an efficient function $Ext : \{0,1\}^n \times \{0,1\}^m$, such that, if $H_\infty(X|Y) \geq m + 2\log(1/\epsilon)$, then $\|(Ext(X,U^n),U^n,Y) - (U^m,U^n,Y)\| \leq \epsilon$.*

A particular example of such efficient function Ext is a two-universal hash function [3]. Finally, we need the following result originated from [10]. The basic idea is to concatenate a random linear code with the Reed-Solomon code.

Theorem 2 *There exists an error-correcting code, efficiently encodable and decodable, such that for any channel $W : \mathcal{X} \longrightarrow \mathcal{Y}$, it achieves the capacity of W.*

For the definition of triviality for noisy correlations see [25, 19] for details.

3 Oblivious Transfer Protocols

In this section, we give the definition of security used in this paper. We closely follow [19] for this presentation. A two-party protocol consists of a program which describes a series of messages to be exchanged (over a noisy and/or a noiseless channel) and local computations to be performed by the two parties. The protocol is said to halt if no more local computations or

message exchanges are required. At the end of an execution of a protocol, each party emits an accept/reject message, depending on the messages he/she received and on the result of local computations. In this paper we concentrate on 1-out-of-2 oblivious transfer protocols.

In an oblivious transfer protocol, there are two parties: a sender (Alice) and a receiver (Bob). The sender's inputs to the protocol consist of two strings of length k. We denote those strings by $U_i = b_0^{(i)} b_1^{(i)} \dots b_{k-1}^{(i)}$, $i \in \{0,1\}$, where $b_j^{(i)} \in \{0,1\}$, $0 \leq j \leq k-1$. The receiver's input is a single bit c. At the end of the protocol Bob receives U_c as his output, while Alice receives nothing. Informally speaking, the protocol is correct, if for honest players, Bob receives his desired output and both players do not abort the protocol. It is said to be private if Alice has no information on Bob's choice and Bob learns information concerning at most one string.

The protocol (for honest players) or more generally any strategy (in the case of cheaters) defines random variables for all the messages exchanged and results of computations performed during an execution of the protocol, depending on their mutual inputs. For the sake of simplicity, we use the same notation for outcomes of a random experiment and their random variables. Denote by $V_A(V_B)$ the random variable which represents all the information in possession of Alice (Bob) at the end of the protocol (including the results of all local computations, local random samplings, local inputs and messages exchanged). This information is also known as the *view of a player*. We denote an execution of a program G by players A and B on inputs x_A and x_B which generates the outcomes y_A and y_B by $\mathsf{G}[A,B](x_A,x_B) = (y_A,y_B)$. A party receiving no output is represented by $y = \Delta$.

We restrict the following definition and analysis to the particular case where the inputs of the honest players are chosen at random. This does not compromise the generality of our results, as random instances of oblivious transfer can easily be converted into OT protocols with specific inputs without any further assumptions, as shown in [1].

Definition 3 *A protocol $\mathsf{G}[A,B](x_A,x_B) = (y_A,y_B)$ is an ϵ-correct implementation of a 1-out-of-2 string oblivious transfer protocol, $\binom{2}{1} - OT^k$ for short, if at the end of its execution for honest players Alice and Bob, we have that*

$$\Pr\big\{\mathsf{G}[A,B]((U_0,U_1),c) \neq (\Delta,U_c)\big\} \leq \epsilon \tag{5}$$

for any $U_i \in \{0,1\}^k$, $i \in \{0,1\}$ and $c \in \{0,1\}$.

It is ϵ-private for Bob if for any possible behavior of Alice,

$$I(V_A;C) \leq \epsilon \tag{6}$$

where $I(\cdot;\cdot)$ is Shannon's mutual information, V_A is the random variable which represents Alice's view after the completion of the protocol and C is the random variable which represents Bob's input c (assuming uniform distribution).

Consider the set of all possible pairs of k-bit strings τ, $\{\tau : (t_0, t_1), t_0, t_1 \in \{0,1\}^k\}$. Let T be a random variable uniformly distributed on τ and T_i be the random variable, corresponding to t_i, $i \in \{0,1\}$. The protocol is ϵ-private for Alice if for any behavior of Bob, for any T, there exists a random binary variable $\tilde{i}$ independent of T such that such that

$$I(T; V_B | T_{\tilde{i}}) \leq \epsilon, \tag{7}$$

where $\tilde{i} = c$ in the case of honest Bob.

A protocol is said to be ϵ-private if it ϵ-private for both Alice and Bob.

A protocol $\mathsf{G}[A,B](x_A, x_B) = (y_A, y_B)$ is said to be an ϵ-private, ϵ-correct 1-out-of-2 string oblivious transfer protocol secure against honest-but-curious *Alice when in the above definitions Alice has to follow the protocol but tries to gather as much information as she can from her view of the protocol V_A.*

Let $\mathsf{G}[A,B](x_A, x_B) = (y_A, y_B)$ be a protocol implementing ϵ-private, ϵ-correct $\binom{2}{1}$-OT^k, based on a noisy channel $W : \mathcal{X} \longrightarrow \mathcal{Y}$ or a noisy correlation P_{XY} on $\mathcal{X} \times \mathcal{Y}$. Let n be the number of invocations of the noisy channel/correlation. The 1-out-of-2 rate of $\mathsf{G}[A,B](x_A, x_B) = (y_A, y_B)$ is defined as: $R_2 = \frac{k}{n}$.

A rate R^* is said to be achievable if for any $\epsilon, \gamma > 0$, there exists a protocol $\mathsf{G}[A,B](x_A, x_B) = (y_A, y_B)$ implementing ϵ-private, ϵ-correct $\binom{2}{1}$-OT^k which, for sufficiently large n, has $R_2 \geq R^* - \gamma$. The supremum of all achievable rates is called the 1-*out-of*-2 *OT capacity* of the channel W or of the correlation P, denoted $C_{\binom{2}{1}\text{-OT}}(W)$ or $C_{\binom{2}{1}\text{-OT}}(P)$.

4 Main Result

According to the result of [19], in order to prove that the oblivious transfer capacity for the honest-but-curious sender and malicious receiver is positive for any non-trivial correlation, we just need to prove it is positive for a particular kind of correlation, called in [19] a *symmetric basic correlation* (SBC). We assume that the players have access to an unlimited bi-directional noiseless channel.

There are three main settings for the considered protocols: 1) Both players can cheat actively; 2) Alice is passive and Bob is active; 3) Both

players are passive. In Setting 1, secure OT can be achieved only based on SBC, while in Settings 2 and 3, our result works for any non-trivial noisy correlation.

Now, we formally define SBC, introduce our protocol (which is in the spirit of [4]) and argue its security for all the above cases.

Let p be a constant such that $0 < p < 1$. In SBC (X, Y), X is uniformly distributed on $\{0,1\}$ and the range $\mathcal{Y}$ of Y is partitioned into three sets: $\mathcal{Y} = \mathcal{U}_0 \cup \mathcal{E} \cup \mathcal{U}_1$, of non-zero probability under the distribution of Y, with the following properties.

- For all $y \in \mathcal{E}$, $\Pr\{Y = y|X = 0\} = \Pr\{Y = y|X = 1\}$.
- $\mathcal{U}_1 = \{\ y'$: for all $y \in \mathcal{U}_0$ we have

$$\begin{array}{r} \Pr\{Y = y|X = x\} = \Pr\{Y = y'|X = \overline{x}\} \quad \wedge \\ \Pr\{Y = y|X = 1\} < \Pr\{Y = y|X = 0\} \quad \wedge \\ \Pr\{Y = y'|X = 1\} > \Pr\{Y = y'|X = 0\} \qquad \} \end{array}$$

- $\Pr\{Y \in \mathcal{E}\} = 1 - p$.

From Alice's point of view it looks like the uniform input to a binary channel, while for Bob it looks like the output of a distinguishable mixture of two channels: an erasure channel and a channel $W : \{0,1\} \longrightarrow \mathcal{U}_0 \cup \mathcal{U}_1$, with conditional probabilities $W(y|x) = \frac{1}{p} \Pr\{Y = y|X = x\}$. If Bob finds $y \in \mathcal{E}$ he has no information at all about the input (a perfect erasure), but for $y \in \mathcal{U}_i$ he has a (more or less weak) indication that $x = i \in \{0,1\}$ because the likelihood for $x = 1 - i$ is smaller.

It is clear that the correlation (X, Y) is completely characterized by p and W. Thus, we denote this distribution $\mathrm{SBC}_{p,W}$. For the sake of simplicity of this presentation, we analyze the case when $p = 1/2$. However, our protocols and proofs can be easily adapted for the case $0 < p < 1$.

Suppose Alice and Bob are given n identical, independent executions of $\mathrm{SBC}_{1/2,W}$. Thus, Alice and Bob receive n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$, respectively.

Remember that by Theorem 2, for any channel W there exists an efficient encodable and decodable error-correcting code $\mathcal{C}$ achieving the capacity of W.

In our protocol, Alice has inputs $U_0, U_1 \in \{0,1\}^k$ and Bob has input $c \in \{0,1\}$.

Protocol I

1. Bob chooses two sets S_0 and S_1, s.t. $S_0, S_1 \subset \{1, 2, \ldots, n\}$, $S_0 \cap S_1 = \emptyset$, $|S_0| = |S_1| = (1/2 - \eta)n$, $0 < \eta < 1/2$, where $(1/2 - \eta)n$ is an integer. Define $q = (1/2 - \eta)n$. Bob chooses S_0 and S_1 so that, for any $i \in S_c$, y_i is not an erasure. Bob sends the sets S_0 and S_1 to Alice over the noiseless channel.

2. Denote the jth element of S_i by $S_i(j)$. After receiving S_0 and S_1, Alice computes the tuples $\rho_0 = (x_{S_0(1)}, \ldots, x_{S_0(q)})$, $\rho_1 = (x_{S_1(1)}, \ldots, x_{S_1(q)})$. Alice then computes the syndromes of ρ_0 and ρ_1 by using an error correcting code $\mathcal{C}$ with rate $Cap(W) - \gamma$, where $\gamma > 0$ and $Cap(W)$ is the Shannon capacity of the channel W. She sends the syndromes to Bob.

3. Alice picks up a random matrix G dimension $(1/2 - \eta)n \times nR$, where R is the rate of the protocol. She computes the vectors $A_0 = \rho_0 * G$ and $A_1 = \rho_1 * G$ where "$*$" is the usual matrix multiplication, and then encrypts her inputs as follows: $B_0 = A_0 \oplus U_0$ and $B_1 = A_1 \oplus U_1$ where "$\oplus$" is a bit-wise exclusive-or. She sends G, B_0 and B_1 to Bob over the noiseless channel.

   Using its respective syndrome, Bob computes ρ_c and then calculates $A_c = \rho_c * G$. He obtains $U_c = A_c \oplus B_c$.

   If Bob experiences a decoding error when computing ρ_c, he defines U_c as the zero-vector.

Before analyzing the protocol security, we note that with exponentially bounded probability Bob sees a number of non-erasures between $(1/2 - \delta)\, n$ and $(1/2 + \delta)\, n$, for some positive constant δ, thus we assume that this is the case. Note also that, for the positions where Bob does not receive erasures his view is exactly like the output of the channel W with input X.

We state our main result. Let X and Z be random variables describing the input of $\mathrm{SBC}_{1/2,W}$ and the output of W, respectively.

Theorem 4 *Protocol I implements an ϵ-private, ϵ-correct 1-out-of-2 oblivious transfer protocol for any $R < I(X;Z)/4$ against active cheaters and $R < I(X;Z)/2$ against passive cheaters.*

Active cheating. We sketch here a proof of why this theorem holds, the complete proof is given in the full version of the paper.

Let's first analyze if the protocol is secure against a malicious Bob. We should prove that Bob obtains knowledge about at most one of Alice's strings.

Dishonest Bob who tries to obtain knowledge on both Alice's inputs U_0 and U_1 will distribute positions where he did not receive an erasure into both sets S_0 and S_1. The number of non-erasures that Bob sees is in between $(1/2-\delta)\,n$ and $(1/2+\delta)\,n$, for some positive constant δ. Thus, we can assume that in one of the sets, let's say S_1 we will have a number of non-erasures no larger than $(1/4+\delta)\,n$. Denote the random variable associated with the syndrome of ρ_1 by Syn_1. We will slightly abuse the notation and denote by ρ_1 the string computed by Alice and, at the same time, its corresponding random variable.

We are interested in the following quantity $H_\infty^\varepsilon(\rho_1|Y^nSyn_1)$ which gives us how much secret information Bob can extract from ρ_1. We first note that $q=(1/2-\eta)n$ symbols of Y^n will not be related to ρ_1 at all, because they will be used for constructing ρ_0 and because of the i.i.d. assumption on (X,Y). Denote the remaining q symbols of Y^n which are possibly related to ρ_1 by Y^q. Also, note that ρ_1 will consist of q general instances of X, again because of the i.i.d. assumption on (X,Y). Thus, instead of ρ_1 we will just write X^q to denote the part of X^n that is used to compute ρ_1. Finally, observe that no more than just $(1/4+\delta)\,n$ bits of the remaining Y^q bits related to ρ_0 will be non-erasures. Thus, we are left with

$$H_\infty^\varepsilon(\rho_1|Y^nSyn_1)=H_\infty^\varepsilon(X^q|Y^qSyn_1) \tag{8}$$

By sequentially applying (1) and (2) we obtain

$$H_\infty^{2\varepsilon}(X^q|Y^qSyn_1)\geq H_\infty^{\varepsilon/2}(X^q|Y^q)+H_\infty^{\varepsilon/2}(Syn_1|X^qY^q)-H_0(Syn_1)-\log(1/\varepsilon) \tag{9}$$

that gives us

$$H_\infty^{2\varepsilon}(X^q|Y^qSyn_1)\geq H_\infty^{\varepsilon/2}(X^q|Y^q)-H_0(Syn_1)-\log(1/\varepsilon) \tag{10}$$

Denote the equivocation of the channel W specified in $SBC_{p,W}$ by $H(X|Z)$. It is clear that $H_0(Syn_1)\leq\frac{n}{2}(H(X|Z)-\gamma)$. We state the following lemma whose proof appears in the full version of this paper.

Lemma 5 *For any $0<\varepsilon'<\varepsilon<1,\delta'>0$ we have*

$$H_\infty^\varepsilon(X^q|Y^q)\geq H_\infty^{\varepsilon'/2}(X^{(1/4-\delta')n})+H_\infty^{\varepsilon'/2}(X^{(1/4+\delta')n}|Z^{(1/4+\delta')n})$$

The intuition behind the lemma is that we can split Y^q in two random variables $Y_\Delta^{q'}$, where $q' = (1/4 - \delta')n$ which consists of the positions where, with an exponentially small (in n) probability, there will be only erasures and $Z^{q''}, q'' = (1/4 + \delta')n$ which consists of the positions where Bob receives X through the channel W. We then split the input random variable X^q accordingly in $X_\Delta^{q'}$ for those inputs where Bob received erasures and $X^{q''}$ for those inputs where Bob received them as through W. Note that, $Y_\Delta^{q'} Z^{q''}$, for large enough n is the typical space of Y^q, thus, the statistical difference of these two distributions goes to zero exponentially as n becomes large by the asymptotic equipartition property. Therefore, we can find appropriate $0 < \varepsilon' < \varepsilon < 1$ so that we have:

$$H_\infty^\varepsilon(X^q|Y^q) \geq H_\infty^{\varepsilon'}(X_\Delta^{q'} X^{q''}|Y_\Delta^{q'} Z^{q''})$$

As $Y_\Delta^{q'}$ is completely useless for Bob (it gives no information at all on X^q), we obtain

$$H_\infty^\varepsilon(X^q|Y^q) \geq H_\infty^{\varepsilon'}(X_\Delta^{q'} X^{q''}|Z^{q''})$$

By applying Equation (2), we get

$$H_\infty^{\varepsilon'}(X_\Delta^{q'} X^{q''}|Z^{q''}) \geq H_\infty^{\varepsilon'/2}(X_\Delta^{q'}|Z^{q''}) - H_\infty^{\varepsilon'/2}(X^{q''}|Z^{q''})$$

However, by definition, $Z^{q''}$ is independent from $X_\Delta^{q'}$, thus we obtain

$$H_\infty^\varepsilon(X^q|Y^q) \geq H_\infty^{\varepsilon'/2}(X_\Delta^{q'}) - H_\infty^{\varepsilon'/2}(X^{q''}|Z^{q''})$$

our desired result.

We then note that according to [11] for general random variables (X, Y), we have $H_\infty^\varepsilon(X^n|Y^n) \geq nH(X|Y) - 4\sqrt{n \log(1/\varepsilon)} \log(|\mathcal{X}|)$.

Putting everything together,

$$H_\infty^\varepsilon(\rho_1|Y^n Syn_1) \geq \left(1/4 - \delta'\right) nH(X) + \left(1/4 + \delta'\right) nH(X|Z) - \frac{n}{2}(H(X|Z) - \gamma) - \log(1/\varepsilon) - 8\sqrt{n \log(1/\varepsilon)} \log(|\mathcal{X}|), \quad (11)$$

and by the definition of mutual information,

$$H_\infty^\varepsilon(\rho_1|Y^n Syn_1) \geq n(I(X;Z)/4 - \delta' I(X;Z) - \gamma) - \log(1/\varepsilon) - 8\sqrt{n \log(1/\varepsilon)} \log(|\mathcal{X}|) \quad (12)$$

Noting that $\log(|\mathcal{X}|) = 1$, making $\varepsilon = 2^{-\alpha n}$, $\alpha > 0$ and choosing an appropriate constant $\epsilon' > 0$ satisfying simultaneously $\epsilon'/3 > \delta' I(X;Z) - \gamma$, $\epsilon'/3 > 8\sqrt{\alpha}$ and $\epsilon'/3 > \alpha$ we obtain

$$H_{\infty}^{\varepsilon}(\rho_1|Y^n Syn_1) \geq n(I(X;Z)/4 - \epsilon')$$

Note that the random matrix G is, in fact, a two-universal hash function[2]. Hence, applying Theorem 1 with $m = (\frac{1}{4}I(X;Z) - \epsilon - 2\alpha)n = Rn$, we can see that Bob's amount of information on A_1 will be at most $2^{-\alpha n}$. Thus, a cheating Bob cannot obtain simultaneously knowledge on Alice's two inputs.

The correctness of the protocol follows from the fact that, with high probability, by using its respective syndrome, Bob can compute ρ_c and then calculate $A_c = \rho_c * G$. He obtains $U_c = A_c \oplus B_c$.

Security against malicious Alice: it is easy to see by inspecting the protocol that she has only two ways to cheat. First, she may try to distinguish the sets S_0 and S_1 as for which contains erasures and which does not. However, the probability to become erasure is equal for both inputs 0 and 1 of SBC, therefore, Alice's best strategy here is guessing at random. The second way is sending a random string instead of one of the syndromes. Indeed, this will lead Bob to a decoding error with high probability, if Alice spoils the syndrome Syn_c. In this case, Bob could complain but this would disclose his choice c. If he does not complain, then his output is undefined. When Alice happens to spoil Syn_{1-c}, honest Bob simply accepts the protocol, again disclosing his choice. Note that all the above cases contradict Definition 3.

It is easy to see that the last instruction of Step 3 makes this kind of cheating useless for Alice because even if she sends an incorrect syndrome, Bob's output is always well-defined. Besides, he may mark Alice as a cheating player for the higher order protocols.

Passive cheating. In the case of passive cheating, Bob would not split his erasures between S_0 and S_1, thus one can see that the achievable rate will be twice the one achieved in the previously stated analysis. Therefore, in the case of passive adversaries we have that any rate $R < I(X;Z)/2$ is achievable.

Upper bounds. In [26], it was proved that the mutual information between two noisy correlations is a secure monotone, in the sense it can not be increased by local computations and noiseless communications between the

[2]In principle, any efficiently computable two-universal hash function can be used in our protocol.

parties holding the correlations. This fact implies that the mutual information between the correlations is an upper bound on their oblivious transfer capacity. Thus, in the case of an $SBC_{p,W}$, its oblivious transfer capacity is upper bounded by its mutual information of $I(X;Y) = pI(X;Z)$. For $p = 1/2$ we obtain that $C_{OT}(SBC_{1/2,W}) < I(X;Z)/2$ thus showing that our protocols are optimal in the case of passive cheaters.

5 Conclusions and Future Works

In this paper, we presented an efficient protocol for implementing oblivious transfer that achieves a non-zero rate for any non-trivial correlation. In the case of symmetric basic correlations, we show that for passive adversaries, the oblivious transfer capacity is efficiently achievable. In the case of active adversaries, our protocol is optimal up to a constant. An open question left by this work is to obtain the oblivious transfer capacity of symmetric noisy correlations in the case of active adversaries. A possible way of doing this is by using interactive hashing in order to prevent Bob from cheating, as proposed in [8] in the case of 1-out-of-2 bit OT. The problem of computing the oblivious transfer capacity for general correlations remains wide open.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and corrections.

References

[1] D. Beaver, "Precomputing Oblivious Transfer, Proc. CRYPTO '95, LNCS 963, pp. 97–109, Springer, 1995.

[2] C. H. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized Privacy Amplification," IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, 1995.

[3] J.L. Carter, M.N. Wegman, "Universal Classes of hash functions," J. of Computer and Syst. Sci., vol. 18, pp. 143–154, 1979.

[4] C. Crépeau, "Equivalence between two flavors of oblivious transfers", Proc. CRYPTO '87 , LNCS 293, pp. 350–354, Springer, 1988.

[5] C. Crépeau, "Efficient Cryptographic Protocols Based on Noisy Channels", Proc. EUROCRYPT '97 , pp. 306–317, Springer, 1997.

[6] C. Crépeau, J. Kilian, "Achieving oblivious transfer using weakened security assumptions", Proc. 29$^{\text{th}}$ FOCS, pp. 42–52, IEEE, 1988.

[7] C. Crépeau, K. Morozov, S. Wolf: "Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel," Proc. SCN '04, LNCS 3352, pp. 47–59, Springer, 2004.

[8] C. Crépeau, G. Savvides, "Optimal Reductions Between Oblivious Transfers Using Interactive Hashing," Proc. EUROCRYPT '06, LNCS 4004, pp. 201–221, Springer, 2006.

[9] S. Even, O. Goldreich, A. Lempel, "A Randomized Protocol for Signing Contracts", Comm. ACM, vol. 28, no. 6, pp. 637–647, 1985.

[10] G.D. Forney, "Concatenated codes," MIT Press, 1966.

[11] T. Holenstein and R. Renner, "One-Way Secret-Key Agreement and Applications to Circuit Polarization and Immunization of Public-Key Encryption," Proc. CRYPTO '05, LNCS 3621, Springer, pp. 478–493, 2005.

[12] H. Imai, K. Morozov, A.C.A. Nascimento, "On the Oblivious Transfer Capacity of the Erasure Channel," Proc. ISIT '06, pp. 1428-1431, IEEE, 2006.

[13] J. Kilian: "Founding Cryptography on Oblivious Transfer," Proc. STOC '88, pp. 20–31, 1988.

[14] V. Korjik, K. Morozov, "Generalized Oblivious Transfer Protocols Based on Noisy Channels," Proc. MMM ACNS '01, LNCS 2052, Springer, pp. 219–229, 2001.

[15] J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby, "A Pseudorandom Generator from any one-way function," *SIAM J. on Comp.*, vol. 28, no. 4., pp. 1364–1396, 1999.

[16] U. Maurer, "Secret Key Agreement by Public Discussion", IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, 1993.

[17] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung, "Perfect Zero-Knowledge Arguments for NP using any one-way permutation", J. of Cryptology, vol. 11, no. 2, 1998.

[18] A. Nascimento, A. Winter, "Oblivious Transfer from any Genuine Noise", pre-print version, 2004.

[19] A. Nascimento, A. Winter, "On the Oblivious Transfer Capacity of Noisy Correlations", Proc. ISIT '06, pp. 1871–1875, IEEE, 2006.

[20] M. O. Rabin, "How to exchange secrets by oblivious transfer", Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.

[21] R. Renner, S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," Proc. ASIACRYPT '05, LNCS 3788, pp. 199–216, Springer-Verlag, 2005.

[22] T.M. Cover, J.A. Thomas, "Elements of Information Theory," Wiley, 1991.

[23] D. Stebila, S. Wolf, "Efficient oblivious transfer from any non-trivial binary-symmetric channel", Proc. ISIT 2002 (Lausanne), p. 293, IEEE, 2002.

[24] S. Wiesner, "Conjugate coding", Sigact News, vol. 15, no. 1, 1983, pp. 78–88; original manuscript written ca. 1970.

[25] A. Winter, A. C. A. Nascimento, H. Imai, "Commitment Capacity of Discrete Memoryless Channels", Proc. 9^{th} IMA Int. Conf. on Cryptography and Coding, LNCS 2898, pp. 35–51, Springer, 2003.

[26] S. Wolf, J. Wullschleger, "New monotones and lower bounds in unconditional two-party computation," CRYPTO '05, LNCS 3621, pp. 467–477, Springer, 2005.

[27] S. Wolf, J. Wullschleger, "Oblivious transfer is symmetric" EUROCRYPT '06, LNCS 4004, pp. 222–232, Springer, 2006.

[28] A. Wyner, "The Wire Tap Channel", Bell System Tech. J., vol. 54, pp. 1355–1387, 1975.