# Achieving Oblivious Transfer Capacity of Generalized Erasure Channels in the Malicious Model

Adriana C. B. Pinto, Rafael Dowsley, Kirill Morozov and Anderson C. A. Nascimento

***Abstract*—Information-theoretically secure string oblivious transfer (OT) can be constructed based on discrete memoryless channel (DMC). The oblivious transfer capacity of a channel characterizes – similarly to the (standard) information capacity – how efficiently it can be exploited for secure oblivious transfer of strings. The OT capacity of a Generalized Erasure Channel (GEC) – which is a combination of a (general) DMC with the erasure channel – has been established by Ahlswede and Csizar at ISIT'07 in the case of passive adversaries. In this paper, we present the protocol that achieves this capacity against malicious adversaries for GEC with erasure probability at least 1/2. Our construction is based on the protocol of Crépeau and Savvides from Eurocrypt'06 which uses interactive hashing (IH). We solve an open question posed by the above paper, by basing it upon a constant round IH scheme (previously proposed by Ding et al at TCC'04). As a side result, we show that Ding et al IH protocol can deal with transmission errors.**

***Index Terms*—Information-theoretic security, oblivious transfer, oblivious transfer capacity, generalized erasure channel, interactive hashing.**

## I. Introduction

Oblivious Transfer (OT) is one of the central cryptographic primitives, since it implies secure two-party (and multi-party) computation [19], [24], [12]. It was initially proposed in different flavors by Wiesner [33] and Rabin [29], but both flavors were later shown to be equivalent by Crépeau [9]. In this work, we will consider the *one-out-of-two string oblivious transfer*, string-OT, in which Alice transmits two input strings $U_0, U_1 \in \{0,1\}^k$ and Bob uses a choice bit $c$ to choose the string $U_c$ that he will receive. This protocol ensures that a dishonest Alice cannot learn $c$, while a dishonest Bob cannot learn both $U_0$ and $U_1$.

The potential of noisy channels for implementing information-theoretically secure cryptographic protocols was first noted by the pioneering work of Wyner [34], with respect to secret key agreement. Crépeau and Kilian proved that noisy channels can be used to implement oblivious transfer [11]. This result was later improved in [10], [25], [32], [13], [26].

The question of determining the optimal rate at which oblivious transfer can be implemented using a noisy channel (i.e., the oblivious transfer capacity of the channel) was raised by Nascimento and Winter in [26]. They also characterized the noise resources that provide strictly positive oblivious transfer capacity. Imai et al [21] obtained the oblivious transfer capacity of the Erasure Channels. Ahlswede and Csiszár [1] proved new bounds on those capacities and also obtained the oblivious transfer capacity of the Generalized Erasure Channels (GEC) in the passive adversary model (where the players always follow the protocol). The related notion of commitment capacity was proposed by Imai et al in [22].

*Our contribution:* In this paper, we show that the rates achieved in [1] against passive players can actually be achieved even against malicious ones (i.e. those that can arbitrarily deviate from the protocol). As the upper bounds proved in [1] for the case of passive players still hold against active ones, we thus establish the oblivious transfer capacity of the Generalized Erasure Channels [1] in the malicious adversary model. Moreover, we prove security of our protocols using definitions by Crépeau and Wullschleger [15], which are known to imply sequential composability.

The main tool for obtaining our results is Interactive Hashing (IH), originally introduced by Ostrovsky et al [28]. Our solution is based on the protocol proposed by Savvides [31] (building on the results of [14]) for oblivious transfer from erasure channels that employs information-theoretic Interactive Hashing [5] as a sub-protocol. However, instead of directly adapting Savvides' solution to our scenario, we show that it is possible to use the constant round interactive hashing protocol by Ding et al [17]. Hereby, we obtain the constant round oblivious transfer protocol, thus answering an open question posed by [31].

*Outline of the Paper:* The paper is organized as follows: In Section II, we establish our notation, provide some facts that we use in the remaining part of this paper and introduce the constant round interactive hashing protocol that we used. In Section III, we present definitions of the Generalized Erasure Channel and oblivious transfer security. We also state our main result about the oblivious transfer capacity of those channels. Finally, in Section IV, we present our protocol, its security proof and show that it achieves the oblivious transfer capacity.

Adriana C. B. Pinto and Anderson C. A. Nascimento are with the Department of Electrical Engineering, University of Brasilia. Campus Universitário Darcy Ribeiro, Brasília, CEP: 70910-900, Brazil. E-mails: adrianacbp@redes.unb.br, andclay@ene.unb.br.

Rafael Dowsley is with the Computer Science and Engineering Department, University of California at San Diego (UCSD), 9500 Gilman Drive, La Jolla, California 92093, USA. Email: rdowsley@cs.ucsd.edu. This work was done while the author was with the Department of Electrical Engineering, University of Brasilia.

Kirill Morozov is with the Faculty of Mathematics, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan. Email: morozov@math.kyushu-u.ac.jp. This work was done while the author was with the Research Center for Information Security, National Institute of Advanced Industrial Science and Technology (AIST), Japan.

## II. Preliminaries

### A. Notation

We will denote by calligraphic letters the domains of random variables and other sets, by $|\mathcal{X}|$ the cardinality of a set $\mathcal{X}$, by upper case letters the random variables and by lower case letters one realization of the random variable. For a random variable $X$ over $\mathcal{X}$, we denote its probability distribution by $P_X : \mathcal{X} \to [0,1]$ with $\sum_{x\in\mathcal{X}} P_X(x) = 1$. For a joint probability distribution $P_{XY} : \mathcal{X} \times \mathcal{Y} \to [0,1]$, let $P_X(x) := \sum_{y\in\mathcal{Y}} P_{XY}(x,y)$ denote the marginal probability distribution and let $P_{X|Y}(x|y) := \frac{P_{XY}(x,y)}{P_Y(y)}$ denote the conditional probability distribution if $P_Y(y) \neq 0$. We write $X \in_R \mathcal{X}$ for a random variable uniformly distributed over $\mathcal{X}$.

If $a$ and $b$ are two bit strings of the same dimension, we denote by $a \oplus b$ their bitwise XOR. The logarithms used in this paper are in base 2. The entropy of $X$ is denoted by $H(X)$ and the mutual information between $X$ and $Y$ by $I(X;Y)$. We write $[n]$ for $\{1,...,n\}$ and $\binom{[n]}{l}$ for the set of all subsets $\mathcal{K} \subseteq [n]$, where $|\mathcal{K}| = l$. For $X^n = (X_1, X_2, \ldots, X_n)$ and $\mathcal{S} \subset [n]$, we write $X^{\mathcal{S}}$ for the restriction of $X^n$ to the positions in the subset $\mathcal{S}$. Similarly for a set $\mathcal{R}$, $\mathcal{R}^{\mathcal{S}}$ is the subset of $\mathcal{R}$ consisting of the elements determined by $\mathcal{S}$.

### B. Strong Extractors and Leftover-Hash Lemma

The statistical distance between two probability distributions $P_X$ and $P_Y$ over the same domain $\mathcal{V}$ is

$$\mathsf{SD}(P_X, P_Y) := \frac{1}{2}\sum_{v\in\mathcal{V}} |P_X(v) - P_Y(v)|.$$

For a finite alphabet $\mathcal{X}$, the min-entropy of a random variable $X \in \mathcal{X}$ is defined as

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

Its conditional version, defined over $\mathcal{Y}$ with finite alphabet is

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

We define now the notion of strong randomness extractors [27], [18]. Let $U_r$ denote a vector uniformly chosen from $\{0,1\}^r$.

**Definition 1** (Strong Randomness Extractors)**.** *Let* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^l$ *be a probabilistic polynomial time function which uses* $r$ *bits of randomness. We say that* $\mathsf{Ext}$ *is an efficient* $(n,m,l,\epsilon)-$strong extractor *if for all probability distributions* $P_W$ *with* $\mathcal{W} = \{0,1\}^n$ *and such that* $H_\infty(W) \geq m$*, we have that* $\mathsf{SD}(P_{\mathsf{Ext}(W;U_r),U_r}, P_{U_l,U_r}) \leq \epsilon$.

Strong extractors can extract at most $l = m - 2\log(\epsilon^{-1}) + O(1)$ bits of nearly random bits [30] and this optimal bound is achieved by Universal Hash Function [6] that we define below.

**Definition 2** (Universal Hash Function)**.** *A class* $\mathcal{G}$ *of functions* $\mathcal{A} \to \mathcal{B}$ *is* 2-universal *if, for any distinct* $x_1, x_2 \in \mathcal{A}$*, the probability that* $g(x_1) = g(x_2)$ *is at most* $|\mathcal{B}|^{-1}$ *when* $g$ *is chosen uniformly at random from* $\mathcal{G}$.

The Leftover-Hash Lemma (similarly the Privacy-Amplification Lemma) [23], [20], [4], [3], [18] guarantees that the Universal Hash Functions allow us to extract $l = m - 2\log(\epsilon^{-1}) + 2$ bits.

**Lemma 1** (Leftover-Hash Lemma)**.** *Assume that a class* $\mathcal{G}$ *of functions* $G : \{0,1\}^n \to \{0,1\}^l$ *is 2-universal. Then for* $G$ *selected uniformly at random from* $\mathcal{G}$ *we have that*

$$\mathsf{SD}(P_{G(W),G}, P_{U_l,G}) \leq \frac{1}{2}\sqrt{2^{-H_\infty(W)}2^l}.$$

*In particular, Universal Hash Functions are* $(n,m,l,\epsilon)-$strong extractor *when* $l \leq m - 2\log(\epsilon^{-1}) + 2$.

### C. Encoding Scheme of Subsets

Cover showed [8] that there is an efficiently computable one to one mapping $F : \binom{[n]}{l} \to [\binom{n}{l}]$ for every integer $l \leq n$. Hence, we can encode the set $\binom{[n]}{l}$ in bit strings of length $m = \lceil \log \binom{n}{l} \rceil$ (see [5, Section 3.1] for more details). Nevertheless, the strings that represent valid encodings may constitute only slightly more than a half of all strings. We use here the modified encoding of [31, Section 4.2.1] in which each string $w \in \{0,1\}^m$ encodes the same subset as $w \mod \binom{n}{l}$, which is always a valid encoding in the original scheme [5].

Consider a subset of $\binom{[n]}{l}$ encoded by strings in $\{0,1\}^m$, according to the above scheme. Since each subset correspond to either 1 or 2 strings in $\{0,1\}^m$, this scheme can at most double the fraction of the strings that map to the subset of interest. This fact is formalized and proved in [31, Lemma 4.1].

### D. Interactive Hashing

Interactive Hashing [28] is a cryptographic primitive between two players, the sender (Bob) and the receiver (Alice). It takes as input a string $w \in \{0,1\}^m$ from Bob, and produces as output two $m$-bit strings, one of which is $w$ and the other is $w' \neq w$. Let the two output strings be $w_0$ and $w_1$, according to lexicographic order. There exists a $d \in \{0,1\}$ such that $w_d = w$. The output strings are available to both Bob and Alice. Interactive Hashing has, briefly and informally, the following properties: a) The cheating Alice cannot tell which of $(w, w')$ was Bob's input (as long as $w$ and $w'$ are a priori equally likely to be the input), and b) At least one of $(w, w')$ is effectively beyond the control of the cheating Bob. We will focus on the information-theoretic variant of IH, which originates from [5].

**Definition 3** (Security of Interactive Hashing [17])**.** *An interactive hashing protocol is* secure for Bob *if for every unbounded strategy of Alice (*$A'$*), and every* $W$*, if* $W_0$*,* $W_1$ *are the outputs of the protocol between an honest Bob with input* $W$ *and* $A'$*, then the distributions* $\{View_{A'}^{\langle A',B\rangle}(W)|W = W_0\}$ *and* $\{View_{A'}^{\langle A',B\rangle}(W)|W = W_1\}$ *are identical, where* $View_{A'}^{\langle A',B\rangle}(W)$ *is Alice's view of the protocol when Bob's input is* $W$*. An interactive hashing protocol is* $(s,\rho)$-secure for Alice *if for every* $S \subseteq \{0,1\}^m$ *of size at most* $2^s$ *and every unbounded strategy of Bob (*$B'$*), if* $W_0$*,* $W_1$ *are the outputs of the protocol, then*

$$\Pr[W_0, W_1 \in S] < \rho,$$

*where the probability is taken over the coin tosses of Alice and Bob. An interactive hashing protocol is* $(s, \rho)$-secure *if it is secure for Bob and* $(s, \rho)$-secure for Alice.

*Let* $a \in \{0,1\}$ *be such that* $W_a = W$. *If the distribution of the string* $W_{\bar{a}}$ *over the randomness of the two parties is* $\eta$*-close to uniform on all strings not equal to* $W_a$, *then the protocol is called* $\eta$-uniform *interactive hashing.*

*Constant Round Interactive Hashing:* We present the constant round IH protocol of [17, Section 5.4]. One of the principal tools used in this protocol is $\eta$-almost $t$-wise independent permutation. Let $\pi$ be a $t$-wise independent permutation, then when $\pi$ is applied in any $t$ points in $\{0,1\}^m$, $\pi$ behaves as a truly random permutation. In an $\eta$-almost $t$-wise independent permutations $\pi'$, the distribution on any $t$ points has statistical distance at most $\eta$ to the distribution induced on these points by a truly random permutation. A 2-wise independent permutation can be built choosing $a, b \in_R GF(2^m)$, $a \neq 0$ (the strings $\{0,1\}^m$ are identified with the field $GF(2^m)$) and defining the permutation by $g(x) = ax + b$ (see, e.g., [17, Section 5.2] for a survey).

Another tool used in this protocol is the 2-1 hash function. Let $h$: $\{0,1\}^m \to \{0,1\}^{m-1}$ be a 2-1 hash function. Then, for each output of $h$ there are exactly 2 pre-images. Notice that to construct a 2-wise independent 2-1 hash function, one can take a 2-wise independent function and omit the last bit of its output.

Let the set $S \subset \{0,1\}^m$ have size $|S| = 2^s$. Note that we think of $S$ as a subset whose strings have some particular property and the sender's input to IH is $w \in \{0,1\}^m$. Then, the parameters of the protocol are $m$ and $s$, also we set $t = m$ and $\eta = (\frac{1}{2^v})^t$, where $v = s - \log m$. The protocol uses the following tools:

- A family $\Pi$ of $\eta$-almost $t$-wise independent permutations $\pi$: $\{0,1\}^m \to \{0,1\}^m$,
- A family $G$ of 2-wise independent 2-1 hash functions $g$: $\{0,1\}^{m-v} \to \{0,1\}^{m-v-1}$,
- A family $H$ (induced by $\Pi$ and $G$) of 2-1 hash functions $h$: $\{0,1\}^m \to \{0,1\}^{m-1}$ defined as:

$$h(x) \triangleq \pi(x)_1, ..., \pi(x)_v, g(\pi(x)_{v+1}, ..., \pi(x)_m),$$

where $\pi(x)_i$ denotes the $i^{th}$ bit of $\pi(x)$.

Let Bob be the sender and Alice be the receiver. Bob has the input $w \in \{0,1\}^m$.

**Protocol 1.**

1) Alice chooses $\pi \in_R \Pi$ and sends the description of $\pi$ to Bob.
2) Bob computes $\pi(w) = z_1...z_m$, where $z_i$ is the $i^{th}$ bit of $\pi(w)$, and sends the bits $z_1...z_v$ to Alice.
3) Alice chooses $g \in_R G$ and sends the description of $g$ to Bob.
4) Bob computes and sends $g(z_{v+1}...z_m)$ to Alice.
5) Both compute and output $(w_0, w_1)$ such that $h(w) = h(w_0) = h(w_1)$.

It has been shown in [17, Section 5.4] that for all $s, m$ such that $s \geq \log m + 2$, the above protocol is a $(s, 2^{-(m-s)+O(\log m)})$-secure $\eta'$-uniform interactive hashing protocol for $\eta' = (2^{s-\log m-1})^{-m} < 2^{-m}$.

## III. Oblivious Transfer Protocols

In the so-called one-out-of-two string oblivious transfer (String OT), Alice inputs two strings $b_0, b_1 \in \{0,1\}^k$ and Bob inputs a bit $c$ called the *choice bit*. Bob receives $b_c$ and remains ignorant about $b_{\bar{c}}$, while Alice remains ignorant about Bob's choice. In this work, we assume that the inputs are uniformly random. It can be done without loss of generality due to the (very efficient) randomized self-reduction of OT [2, Section 3.2].

We assume a malicious (a.k.a. active) adversary that can have an arbitrary behavior. The players are connected by a noiseless channel and by a Generalized Erasure Channel [1] (which, loosely speaking, is a combination of a discrete memoryless channel and the erasure channel).

**Definition 4** (Generalized Erasure Channel [1])**.** *A discrete memoryless channel* $\{W : \mathcal{X} \to \mathcal{Y}\}$ *will be called the* Generalized Erasure Channel *if the output alphabet* $\mathcal{Y}$ *can be decomposed as* $\mathcal{Y}_0 \cup \mathcal{Y}^*$ *such that* $W(y|x)$ *does not depend on* $x \in \mathcal{X}$, *if* $y \in \mathcal{Y}^*$. *For a GEC, we denote* $W_0(y|x) = \frac{1}{1-p^*}W(y|x)$, $x \in \mathcal{X}$, $y \in \mathcal{Y}_0$, *where* $p^*$ *is the sum of* $W(y|x)$ *for* $y \in \mathcal{Y}^*$ *(not depending on* $x$*).*

We will use the security definition of String OT from [15]. In particular, this definition implies that the String OT protocol, which satisfies it, is sequentially composable. The following notions and the theorem come from [15]. The statistical information of $X$ and $Y$ given $Z$ is defined as

$$I_S(X;Y|Z) = \mathsf{SD}(P_{XYZ}, P_Z P_{X|Z} P_{Y|Z}).$$

A $\mathcal{F}$-hybrid protocol consists of a pair of algorithms $\mathcal{P} = (A_1, A_2)$ that can interact by means of two-way message exchange and have access to some functionality $\mathcal{F}$. A pair of algorithms $\widetilde{A} = (\widetilde{A_1}, \widetilde{A_2})$ is admissible for protocol $\mathcal{P}$ if at least one of the parties is honest, that is, if at least one of the equalities $\widetilde{A_1} = A_1$ and $\widetilde{A_2} = A_2$ is true. Let $B$ denote $(B_0, B_1)$.

**Theorem 1.** *A protocol* $\mathcal{P}$ *securely realizes String OT (for strings of dimension* $k$*) with an error of at most* $6\epsilon$ *if for every admissible pair of algorithms* $\widetilde{A} = (\widetilde{A_1}, \widetilde{A_2})$ *for protocol* $\mathcal{P}$ *and for all inputs* $(B, C)$, $\widetilde{A}$ *produces outputs* $(U, V)$ *such that the following conditions are satisfied:*

- *(Correctness) If both parties are honest, then* $U = \perp$ *and* $\Pr[V = B_C] \geq 1 - \epsilon$.
- *(Security for Alice) If Alice is honest, then we have* $U = \perp$ *and there exists a random variable* $C'$ *distributed according to* $P_{C'|B,C,V}$, *such that* $I_S(B; C'|C) \leq \epsilon$ *and* $I_S(B; V|C, C', B_{C'}) \leq \epsilon$.
- *(Security for Bob) If Bob is honest, we have* $V \in \{0,1\}^k$ *and* $I_S(C; U|B) \leq \epsilon$.

*The protocol is secure if* $\epsilon$ *is negligible in the security parameter* $n$.

If the GEC is used $n$ times, the *oblivious transfer rate* of the protocol is given by $R_{OT} = \frac{k}{n}$.

The *oblivious transfer capacity* [26] is the supremum of the achievable rates when the protocol is secure. In this work, we considered the oblivious transfer capacity of the Generalized Erasure Channel when the adversaries are malicious.

**Theorem 2.** *For a Generalized Erasure Channel with $p^* \geq \frac{1}{2}$, the oblivious transfer capacity in the case of malicious adversaries is $(1-p^*)C(W_0)$ where $C(W_0)$ is the Shannon capacity of the discrete memoryless channel $\{W_0 : \mathcal{X} \to \mathcal{Y}_0\}$.*

In the next section, we prove the direct part. The converse follows from the fact that is not possible to achieve greater oblivious transfer rates even when only passive adversaries are considered [1].

## IV. String OT Protocol Based on GEC

Now, we present our protocol for string oblivious transfer from Generalized Erasure Channel. It is based on the protocol for String OT from the erasure channel [31, Protocol 5.1].

**Protocol 2.**

1) Alice and Bob select a (typically very small) positive constant $\alpha < \frac{1-p^*}{7}$ and set $\beta = 1 - p^* - 2\alpha$.
2) Alice randomly chooses $x^n$ according to the probability distribution that achieves the Shannon capacity of $W_0$ and sends $x^n$ to Bob through the GEC.
3) Bob receives the string $y^n$ and collects the *good* (those corresponding to $y \in \mathcal{Y}_0$) and the *bad* (those corresponding to $y \in \mathcal{Y}^*$) positions in sets $\mathcal{G}$ and $\mathcal{B}$, respectively. He aborts if $|\mathcal{G}| < (1-p^*-\alpha)n = \beta n + \alpha n$.
4) Bob chooses $c \in_R \{0,1\}$ and $w \in_R \{0,1\}^m$, where $m = \lceil \log \binom{\beta n}{\alpha n} \rceil$. He decodes $w$ into a subset $\mathcal{S}$ of cardinality $\alpha n$ (out of $\beta n$) using the encoding scheme of Section II-C. Bob then defines two disjoint sets $\mathcal{R}_c$ and $\mathcal{R}_{\overline{c}}$ of cardinality $\beta n$. $\mathcal{R}_c$ consists only of positions from $\mathcal{G}$, chosen randomly and without repetition. $\mathcal{R}_{\overline{c}}$ has $\alpha n$ positions from $\mathcal{G}$ (defining the subset $\mathcal{R}_{\overline{c}}^{\mathcal{S}}$) and the remaining positions are chosen from $\mathcal{G} \cup \mathcal{B}$, randomly and without repetition. Bob sends the descriptions of $\mathcal{R}_0$ and $\mathcal{R}_1$ to Alice.
5) Alice checks that no position is repeated in the sets $\mathcal{R}_0$ and $\mathcal{R}_1$, otherwise she aborts.
6) Bob sends $w$ to Alice using Interactive Hashing (Protocol 1). Let $w_0, w_1$ be the output strings, let $\mathcal{S}_0$, $\mathcal{S}_1$ be the corresponding subsets of cardinality $\alpha n$ and let $b \in \{0,1\}$ be such that $w_b = w$.
7) Bob announces $a = b \oplus c$ as well as $y^{\mathcal{R}_0^{\mathcal{S}_{\overline{a}}}}$ and $y^{\mathcal{R}_1^{\mathcal{S}_a}}$.
8) Alice checks if $y^{\mathcal{R}_0^{\mathcal{S}_{\overline{a}}}}$ and $y^{\mathcal{R}_1^{\mathcal{S}_a}}$ are $2\epsilon$ jointly typical for a discrete memoryless channel $\{W_0 : \mathcal{X} \to \mathcal{Y}_0\}$ (see the appendix) with her input on these positions. If they are not jointly typical, Alice aborts.
9) Alice chooses randomly 2-universal hash functions $g_0, g_1 : \mathcal{X}^{\beta n} \to \{0,1\}^{\beta n[H(X|Y\in\mathcal{Y}_0)+\epsilon]}$ (with $\epsilon > 0$ such that the output length is integer). She computes $g_0(x^{\mathcal{R}_0})$ and $g_1(x^{\mathcal{R}_1})$. She also randomly chooses 2-universal hash functions $h_0, h_1 : \mathcal{X}^{\beta n} \to \{0,1\}^{\delta n}$, where $\delta = (\beta - 5\alpha)H(X) - \beta(H(X|Y \in \mathcal{Y}_0) + \epsilon) - \gamma$ and $\gamma > 0$ such that the output length is integer. She sends $g_0(x^{\mathcal{R}_0})$, $g_1(x^{\mathcal{R}_1})$ and the descriptions of $g_0$, $g_1$, $h_0$, $h_1$ to Bob. Alice outputs $r_0 = h_0(x^{\mathcal{R}_0})$ and $r_1 = h_1(x^{\mathcal{R}_1})$.
10) Bob computes all possible $\widetilde{x}^{\mathcal{R}_c}$ that are jointly typical with $y^{\mathcal{R}_c}$ and satisfy $g_c(\widetilde{x}^{\mathcal{R}_c}) = g_c(x^{\mathcal{R}_c})$. If there exists exactly one such $\widetilde{x}^{\mathcal{R}_c}$, Bob outputs $r_c = h_c(\widetilde{x}^{\mathcal{R}_c})$. Otherwise, he outputs $r_c = 0^{\delta n}$.

**Remark 1.** *Since in Step 10 Bob uses the output of universal hash functions to correct errors, the above protocol is not computationally efficient. However, this suffices for our result as we only claim possibility of achieving the OT capacity.*

**Theorem 3.** *The above string oblivious transfer protocol is secure.*

*a) Correctness:* When Alice and Bob are honest, Bob does not obtain the correct output either if he aborts in Step 3, or if he does not obtain exactly $\widetilde{x}^{\mathcal{R}_c} = x^{\mathcal{R}_c}$ in Step 10. By the Chernoff bound [7], the probability that Bob aborts in Step 3 is a negligible function of $n$. Bob does not obtain exactly $\widetilde{x}^{\mathcal{R}_c} = x^{\mathcal{R}_c}$ either if $x^{\mathcal{R}_c}$ is not jointly typical with $y^{\mathcal{R}_c}$ (which according to the definition of joint typicality occurs only with probability negligible in $n$), or if there exists another $\overline{x}^{\mathcal{R}_c}$ that is both jointly typical with $y^{\mathcal{R}_c}$ and has $g_c(\overline{x}^{\mathcal{R}_c}) = g_c(x^{\mathcal{R}_c})$. However, the number of $\overline{x}^{\mathcal{R}_c}$ that are jointly typical with $y^{\mathcal{R}_c}$ is upper bounded by $2^{\beta n[H(X|Y\in\mathcal{Y}_0)+\epsilon']}$ (for $0 < \epsilon' < \epsilon$ and $n$ sufficiently large), so the Leftover-Hash Lemma guarantees that for $n$ sufficiently large with overwhelming probability the output of $g_c$ on these $\overline{x}^{\mathcal{R}_c}$ is not equal to $g_c(x^{\mathcal{R}_c})$. As all the failure probabilities are negligible in $n$, the protocol meets the correctness requirement.

*b) Security for Bob:* Since in GEC, every input symbol $x$ is erased (i.e. ends up in $\mathcal{Y}^*$) with probability $p^*$ independent of $x$, Alice does not know which input symbols were erased. Hence, the distribution of $(\mathcal{R}_0, \mathcal{R}_1)$ is independent of $c$ from Alice's point of view. Another point where Bob uses $c$ to generate messages to Alice is in Step 7. Upon receiving $a$, Alice can correctly guess $c$ if and only if she can correctly guess $b$, but the security of Interactive Hashing protocol guarantees that the view of Alice is the same for $b = 0$ and $b = 1$, except with negligible probability. Remember that Alice's views in the IH protocol are identical. Also, the IH protocol is $\eta' < 2^{-m}$ uniform, as mentioned in Section II-D. However, $\eta'$ is negligible, since $m = \lceil \log \binom{\beta n}{\alpha n} \rceil = O(n)$, that follows by applying Stirling's approximation. This implies that the probability that $w_{\overline{b}}$ is non-uniform in $\{0,1\}^m \setminus w$ (and hence the probability that Alice's views are not identical) is negligible.

Finally, note that no matter what the malicious Alice actually sends in Step 9, Bob will not abort. In particular, this prevents reaction attacks. Therefore, the distribution of Alice's view of the protocol does not depend on $c$ with overwhelming probability.

*c) Security for Alice:* Our proof follows the lines of Savvides' proof [31, Section 5.1]. We first present some definitions.

**Definition 5.** *Let $u(\mathcal{R})$ be the number of positions contained in $\mathcal{R}$ such that the corresponding output at this position was an erasure.*

**Definition 6.** *$\mathcal{S}$ is called* good *for $\mathcal{R}$ if $u(\mathcal{R}^{\mathcal{S}}) < \alpha^2 n$, otherwise it is called* bad *for $\mathcal{R}$.*

There are two cases to consider: (i) both $u(\mathcal{R}_0)$ and $u(\mathcal{R}_1)$ are greater than or equal to $2\alpha n$, (ii) either $u(\mathcal{R}_0)$ or $u(\mathcal{R}_1)$ is less than $2\alpha n$. We will prove the security for Alice in each case. For the first case we need the following two lemmas from [31, Section 5.1] which follow from the Chernoff bound, the union bound and the properties of the encoding scheme used.

**Lemma 2.** *Let $\mathcal{R}$ be a set of cardinality $\beta n$ such that $u(\mathcal{R}) \geq 2\alpha n$. Then the fraction $f$ of subsets $\mathcal{S}$ of cardinality $\alpha n$ that are good for $\mathcal{R}$ satisfies $f < e^{-\alpha^2 n/4}$.*

**Lemma 3.** *Let $\mathcal{R}_0, \mathcal{R}_1$ be sets of cardinality $\beta n$ such that $u(\mathcal{R}_0) \geq 2\alpha n$ and $u(\mathcal{R}_1) \geq 2\alpha n$. Then the fraction of strings $w$ that decode to subsets $\mathcal{S}$ that are good for either $\mathcal{R}_0$ or $\mathcal{R}_1$ is no larger than $4e^{-\alpha^2 n/4}$.*

Since the fraction of the strings $w \in_R \{0,1\}^m$ that are good for either $\mathcal{R}_0$ or $\mathcal{R}_1$ is no larger than $4e^{-\alpha^2 n/4}$, we can set the security parameter $s$ of the interactive hashing protocol to $\log(4e^{-\alpha^2 n/4}2^m) = m - \frac{\alpha^2 n}{4}\log e + 2$. Therefore we have that $\rho = 2^{-(m-s)+O(\log m)} = 2^{-\alpha^2 \log(e) n/4 + O(\log n)}$ and so, by the security of the interactive hashing protocol, the probability that Bob gets both $w_0$ and $w_1$ to be good for either $\mathcal{R}_0$ or $\mathcal{R}_1$ is a negligible function of $n$. Then, with overwhelming probability, one of the sets (w.l.o.g. $\mathcal{R}_0$) will have $u(\mathcal{R}_0^{\mathcal{S}_{\overline{a}}}) \geq \alpha^2 n$.

We know by lemma 4 (in the appendix), that if two $n$ long strings are not jointly typical at a randomly chosen (according to a uniform distribution) linear fraction of positions, this implies the non joint-typicality of these $n$ long strings. Therefore, Bob succeeds in the test of Step 8 (i.e., finds $y^{\mathcal{R}_0^{\mathcal{S}_{\overline{a}}}}$ jointly typical with Alice's input) only if he correctly guesses $y$'s values for the bad positions that are jointly typical with Alice's input. For $n$ sufficiently large, there are at most $2^{\alpha^2 n[H(Y \in \mathcal{Y}_0|X)+\epsilon]}$ ($\epsilon > 0$) sequences of $y$'s values that are jointly typical with Alice's input, and there are at least $2^{\alpha^2 n[H(Y \in \mathcal{Y}_0)-\epsilon]}$ typical sequences for the $y$'s values, so the probability that Bob succeeds in the test is less than $2^{\alpha^2 n[H(Y \in \mathcal{Y}_0|X)-H(Y \in \mathcal{Y}_0)+2\epsilon]} = 2^{-\alpha^2 n[C(W_0)-2\epsilon]}$ which is a negligible function of $n$. As all the possibilities of Bob cheating successfully in the protocol occur only with negligible probability, the protocol is secure for Alice in the case that both $u(\mathcal{R}_0)$ and $u(\mathcal{R}_1)$ are at least $2\alpha n$.

We now analyze the security if either $u(\mathcal{R}_0)$ or $u(\mathcal{R}_1)$ is less than $2\alpha n$ (w.l.o.g. we assume that $u(\mathcal{R}_0) < 2\alpha n$). By the Chernoff bound, we have that $|\mathcal{B}| > (p^* - \alpha)n$ with overwhelming probability. Since only $(1-2\beta)n$ positions were not used in $\mathcal{R}_0, \mathcal{R}_1$, then $u(\mathcal{R}_0) + u(\mathcal{R}_1) + (1-2\beta)n > (p^* - \alpha)n$ and so $u(\mathcal{R}_1) > (1 - p^* - 7\alpha)n = \beta n - 5\alpha n$. Since more than $\beta n - 5\alpha n$ positions from $\mathcal{R}_1$ are erasures and Alice only sends $\beta n[H(X|Y \in \mathcal{Y}_0) + \epsilon]$ bits of information about $x^{\mathcal{R}_1}$ in Step 9, we have that $H_\infty(X^{\mathcal{R}_1}|\mathrm{View}_{\mathrm{Bob}}) > n[(\beta - 5\alpha)H(X) - \beta H(X|Y \in \mathcal{Y}_0) - \beta\epsilon]$, where $\mathrm{View}_{\mathrm{Bob}}$ denotes all the information that Bob knows. So the property of the 2-universal hash function $h_1$ for extracting $n[(\beta - 5\alpha)H(X) - \beta H(X|Y \in \mathcal{Y}_0) - \beta\epsilon - \gamma]$ bits of information (with $\gamma > 0$) follows from the Leftover-Hash Lemma. Therefore, Bob has only negligible information about $r_1$, and the security follows for the case that either $u(\mathcal{R}_0)$ or $u(\mathcal{R}_1)$ is less than $2\alpha n$.

### A. Achieving the Oblivious Transfer Capacity

For $n$ sufficiently large, $\alpha$, $\epsilon$ and $\gamma$ can be made arbitrarily small without compromising the security of the protocol. So the limit of strings lengths can go to $n(1-p^*)[H(X) - H(X|Y \in \mathcal{Y}_0)]$ that is equal to $n(1-p^*)C(W_0)$ since the probability distribution of $X$ in the protocol is the one that achieves the Shannon capacity of the channel $W_0$. So the limit of oblivious transfer rate can go to $(1-p^*)C(W_0)$ for $n$ sufficiently large, thus proving the direct part of the theorem 2.

## V. Acknowledgments

We would like to thank George Savvides and the anonymous reviewers for their helpful comments.

## References


[1] R. Ahlswede, I. Csiszár. On Oblivious Transfer Capacity. *ISIT 2007*, pages 2061-2064, 2007.

[2] D. Beaver. Precomputing Oblivious Transfer. In D. Coppersmith, editor, *CRYPTO*, volume 963 of Lecture Notes in Computer Science, pages 97-109, Springer, 1995.

[3] C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer: Generalized privacy amplification. *IEEE Transactions on Information Theory* 41(6), pages 1915-1923 (1995).

[4] C. H. Bennett, G. Brassard, J. Robert: Privacy Amplification by Public Discussion. *SIAM J. Comput.* 17(2), pages 210-229 (1988).

[5] C. Cachin, C. Crépeau, and J. Marcil. Oblivious Transfer with a Memory-Bounded Receiver. In *Proceedings.39th IEEE Annual Symposium on Foundations of Computer Science*, pages 493-502, 1998.

[6] J.L. Carter and M.N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18, pages 143154, 1979.

[7] H. Chernoff, A Measure of Asymptotic efficiency for Tests of a Hypothesis Based on the Sum of Observations. *Ann. Math. Statistics*, vol. 23, pages 493-507, 1952.

[8] T. M. Cover. Enumerative Source Encoding. In *IEEE Transactions on Information Theory*, Volume 19, Issue 1, pages 73-77, 1975.

[9] C. Crépeau. Equivalence Between Two Flavours of Oblivious Transfers. In *Proceedings. CRYPTO 87*, volume 293 of Lecture Notes in Computer Science, pages 350-354, 1987.

[10] C. Crépeau. Efficient Cryptographic Protocols Based on Noisy Channels. *EUROCRYPT 1997*, pages 306-317.

[11] C. Crépeau, J. Kilian. Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract). *FOCS 1988*, pages 42-52.

[12] C. Crépeau, J. van de Graaf, A. Tapp. Committed Oblivious Transfer and Private Multi-Party Computation. *CRYPTO 1995*, pages 110-123.

[13] C. Crépeau, K. Morozov, S. Wolf. Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel. *SCN 2004*, LNCS 3352, pages 47-59.

[14] C. Crépeau, G. Savvides. Optimal Reductions Between Oblivious Transfers Using Interactive Hashing. *EUROCRYPT 2006*, LNCS 4004, pages 201–221.

[15] C. Crépeau, J. Wullschleger. Statistical Security Conditions for Two-Party Secure Function Evaluation. *ICITS 2008*, LNCS 5155, pages 86-99.

[16] I. Csiszár, J. Körner. Information Theory: Coding Theorems for Discrete Memoryless Channels. New York: Academic, 1981.

[17] Y. Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel. Constant-round oblivious transfer in the bounded storage model. In *J. Cryptology*, 20(2), pages 165-202, 2007. Conference version appeared at TCC '04.

[18] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* 38(1), pages 97-139, 2008. Conference version appeared in EUROCRYPT 2004.

[19] O. Goldreich, S. Micali, and A. Wigderson. How to Play Any Mental Game, or: A Completeness Theorem for Protocols with Honest Majority. In *Proceedings 19th ACM STOC*, pages 20-31, 1997.

[20] J. Håstad, R. Impagliazzo, L.A. Levin, and M. Luby. A Pseudorandom Generator from Any One-way Function. *SIAM Journal on Computing*, 28(4), pages 13641396, 1999.

[21] H. Imai, K. Morozov, and A. C. A. Nascimento. On the Oblivious Transfer Capacity of the Erasure Channel. In *2006 IEEE International Symposium on Information Theory*, pages 1428-1431, 2006.

[22] H. Imai, A. C. A. Nascimento, A. Winter. Commitment Capacity of Discrete Memoryless Channels. *IMA Int. Conf. 2003*, pages 35-51.

[23] R. Impagliazzo, L. A. Levin, M. Luby. Pseudo-random Generation from One-way Functions (Extended Abstracts). *STOC 1989*, pages 12-24.

[24] J. Kilian. Founding Cryptography on Oblivious Transfer. *STOC 1988*, pages 20-31.

[25] V. Korjik, K. Morozov, Generalized Oblivious Transfer Protocols Based on Noisy Channels. *MMM ACNS 2001*, LNCS 2052, pages 219-229.

[26] A. C. A. Nascimento, A. Winter. On the Oblivious-Transfer Capacity of Noisy Resources. *IEEE Transactions on Information Theory*, 54(6), pages 2572-2581, 2008. Conference version appears at 2006 IEEE International Symposium on Information Theory. Manuscript available since 2004.

[27] N. Nisan, D. Zuckerman. Randomness is Linear in Space. *Journal of Computer and System Sciences*, 52(1), pages 4353, 1996.

[28] R. Ostrovsky, R.Venkatesan, M. Yung. Fair games against an all-powerful adversary. *AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 155-169, 1993.

[29] M. O. Rabin. How to Exchange Secrets by Oblivious Transfer. In *Technical Report TR-81, Aiken Computation Laboratory, Harvard University*, 1981.

[30] J. Radhakrishnan, A. Ta-Shma. Bounds for Dispersers, Extractors, and Depthtwo Superconcentrators. *SIAM Journal on Discrete Mathematics*, 13(1), pages 224, 2000.

[31] G. Savvides. Interactive Hashing and reductions between Oblivious Transfer variants. PhD thesis, School of Computer Science, McGill University, Montreal, Canada, 2007.

[32] D. Stebila, S. Wolf. Efficient Oblivious Transfer from any Non-Trivial Binary-Symmetric Channel. In Proc. IEEE Int. Symp. Information Theory (ISIT), Lausanne, Switzerland, Jun./Jul. 2002, page 293.

[33] S. Wiesner. Conjugate Coding. In *ACM SIGACT News*, Volume 15, Issue 1, pages 78-88, 1983.

[34] A. Wyner. The Wire-tap Channel. Bell Syst. Tech. J., vol. 54, pages 1355-1387, 1975.


## APPENDIX

The following definitions follow largely the book of Csiszár and Körner [16].

**Definition 7.** *For a probability distribution $P$ on $\mathcal{X}$ and $\epsilon > 0$ the* $\epsilon$-typical sequences *form the set*

$$\mathcal{T}^n_{P,\epsilon} = \{x^n \in \mathcal{X}^n : \forall x \in \mathcal{X} \ |N(x|x^n) - nP(x)| \leq \epsilon n \ \& \\ P(x) = 0 \Rightarrow N(x|x^n) = 0\},$$

*with the number $N(x|x^n)$ denoting the number of symbols $x$ in the string $x^n$.*

The *type* of $x^n$ is the probability distribution $P_{x^n}(x) = \frac{1}{n}N(x|x^n)$. Then, $x^n \in \mathcal{T}^n_{P,\epsilon} \Rightarrow |P_{x^n}(x) - P(x)| \leq \epsilon, \forall x \in \mathcal{X}$.

**Properties 1.**

1) $P^{\otimes n}(\mathcal{T}^n_{P,\epsilon}) \geq 1 - 2|\mathcal{X}| \exp(-n\epsilon^2/2)$.
2) $|\mathcal{T}^n_{P,\epsilon}| \leq \exp(nH(P) + n\epsilon D)$.
3) $|\mathcal{T}^n_{P,\epsilon}| \geq (1 - 2|\mathcal{X}| \exp(-n\epsilon^2/2)) \exp(nH(P) - n\epsilon D)$,

*with the constant $D = \sum_{x:P(x)\neq 0} - \log P(x)$. See [16] for more details.*

Extending this concept to the conditional $\epsilon$-typical sequences, we have:

**Definition 8.** *Consider a channel $W : \mathcal{X} \to \mathcal{Y}$ and an input string $x \in \mathcal{X}^n$. For $\epsilon > 0$, the* conditional $\epsilon$-typical sequences *form the set*

$$\begin{aligned} \mathcal{T}^n_{W,\epsilon}(x^n) &= \{y^n : \forall x \in \mathcal{X}, y \in \mathcal{Y} \ |N(xy|x^n y^n) \\ &\quad -nW(y|x)P_{x^n}(x)| \leq \epsilon n \\ &\quad \& \, W(y|x) = 0 \Rightarrow N(xy|x^n y^n) = 0\} \\ &= \prod_x \mathcal{T}^{\mathcal{I}_x}_{W_x, \epsilon P_{x^n}(x)^{-1}}, \end{aligned}$$

*where $\mathcal{I}_x$ are the sets of positions in the string $x^n$ where $x_k = x$.*

**Properties 2.**

1) $W^n_{x^n}(\mathcal{T}^n_{W,\epsilon}) \geq 1 - 2|\mathcal{X}||\mathcal{Y}| \exp(-n\epsilon^2/2)$.
2) $|\mathcal{T}^n_{W,\epsilon}| \leq \exp(nH(W|P_{x^n}) + n\epsilon E)$.
3) $|\mathcal{T}^n_{W,\epsilon}| \geq \left(1 - 2|\mathcal{X}||\mathcal{Y}| \exp(-n\epsilon^2/2)\right)$ $\cdot \exp(-nH(W|P_{x^n}) - n\epsilon E)$,

*with the constant $E = max_x \sum_{y:W(y)\neq 0} - \log W_x(y)$ and the conditional entropy $H(W|P) = \sum_x P(x)H(W_x)$. See [16] for more details.*

It is a well know fact that if $x^n$ and $y^n$ are conditional $\epsilon$-typical according the definition 8, then

$$|\mathcal{T}^n_{W,\epsilon}| \leq 2^{n(H(Y|X)+\epsilon)}.$$

We now prove the following lemma:

**Lemma 4.** *Let $W : \mathcal{X} \to \mathcal{Y}$ be a discrete memoryless channel and $x^n \in \mathcal{X}^n$, $y^n \in \mathcal{Y}^n$ be the input and output strings of this channel. Let $\mathcal{A}$ be a random subset of $[n]$ such that $|\mathcal{A}| = \delta n$, $0 < \delta \leq 1$. Let $x^{\mathcal{A}}$ and $y^{\mathcal{A}}$ be the restrictions of $x^n$ and $y^n$ to the positions in the set $\mathcal{A}$. If $x^n$ and $y^n$ are conditional $\epsilon$-typical, then $x^{\mathcal{A}}$ and $y^{\mathcal{A}}$ are conditional $2\epsilon$-typical for any $\epsilon > 0$ and $n$ large enough.*

*Proof:*

By hypothesis $x^n$ and $y^n$ are conditional $\epsilon$-typical, so for every symbols $x$ and $y$ we have that

$$|N(xy|x^n y^n) - nP_{x^n}(x)W(y|x)| \leq \epsilon n,$$

for a large enough $n$.

Given the conditional $\epsilon$-typical strings $x^n$ and $y^n$, the probability of selecting one pair with the specific values $x$ and $y$ for the substrings $x^{\mathcal{A}}$ and $y^{\mathcal{A}}$ is $\frac{N(xy|x^n y^n)}{n}$. We have that

$$P_{x^n}(x)W(y|x) - \epsilon \leq \frac{N(xy|x^n y^n)}{n} \leq P_{x^n}(x)W(y|x) + \epsilon.$$

Therefore, by the Chernoff bound [7], for $n$ large enough with overwhelming probability the number of pairs of $x$ and $y$ in the substrings $x^{\mathcal{A}}$ and $y^{\mathcal{A}}$, $N(xy|x^{\mathcal{A}} y^{\mathcal{A}})$, is limited by

$$\begin{aligned} \delta n \left(P_{x^n}(x)W(y|x) - \epsilon - \epsilon'\right) &\leq N(xy|x^{\mathcal{A}} y^{\mathcal{A}}) \\ &\leq \delta n \left(P_{x^n}(x)W(y|x) + \epsilon + \epsilon'\right), \end{aligned}$$

for any $\epsilon' > 0$. Making $\epsilon' = \epsilon$ we have that the substrings $x^{\mathcal{A}}$ and $y^{\mathcal{A}}$ are conditional $2\epsilon$-typical. ■