On the Oblivious Transfer Capacity of the Erasure Channel

Hideki Imai*†, Kirill Morozov†, Anderson C. A. Nascimento‡
* Department of Electrical, Electronic and Communication Engineering,
Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
† National Institute of Advanced Industrial Science and Technology (AIST),
1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan
Email: {h-imai,kirill.morozov}@aist.go.jp
This work is done in part at Institute of Industrial Science, University of Tokyo, Japan
‡ Department of Electrical Engineering, University of Brasilia, 70910-900, Brasilia, DF, Brazil
E-mail: andclay@ene.unb.br

***Abstract*— One of the most important primitives in two-party distrustful cryptography is oblivious transfer, a complete primitive for two-party computation. Recently introduced, the oblivious transfer capacity of a noisy channel measures an efficiency of information theoretical reductions from 1-out-of-k, l-string oblivious transfer to noisy channels. It is defined as the maximal achievable ratio l/n, where l is the length of the strings which are to be transferred and n is the number of times the noisy channel is invoked. This quantity is unknown in a general case. For discrete memoryless channels, it is known to be non-negligible for honest-but-curious players, but the non-zero rates have not ever been proved achievable in the case of malicious players. Here, we show that in the particular case of the erasure channel, more precise answers can be obtained. We compute the OT capacity of the erasure channel for the case of honest-but-curious players and, for the fully malicious players, we give its lower bound.**

I. Introduction

Being invented in a number of different settings by Wiesner [25], Rabin [23] and Even, Goldreich and Lempel [17], oblivious transfer (OT) is a primitive of particular importance in cryptography as it is complete for two-party secure computation which was shown in the computational model [18] as well as in the unconditional model [20]. Oblivious transfer is about transmitting secrets from a sender Alice to a receiver Bob in such a way that Alice is only sure that Bob did not learn all of them without knowing what exactly he learned. There are two flavors[1] of this primitive: first, where Bob is allowed to choose what he will receive, the *1-out-of-2* OT [25], [17]. In this paper, we are concerned with implementing this type and henceforth we shall refer to as just OT. The other flavor is *Rabin* OT [23], where Alice sends a secret and with probability 1/2 Bob receives this secret or nothing at all and he always learns which case has occurred. In the communication theory, this primitive is known as the erasure channel. In this paper, we shall be concerned with *how efficiently* one can implement OT based on it.

In our scenario, we demand *information-theoretic* (or *unconditional*) security for the two mutually distrustful players Alice and Bob, i.e., they are allowed unlimited computing power, while only a negligible (in some security parameter) failure probability can be tolerated. It is a well-known fact that in this setting, OT is impossible "from scratch", i.e., using only error-free communication and local randomness. This means that one needs some additional assumptions which could be, e.g., a noisy communication channel connecting the parties [7], [5], [15], [11], [21], [8], trusted initializer [24], pre-distributed correlated randomness [21], bounded storage model (BSM) [6], [10], [14], quantum channel and bounded quantum storage [13], [12], hybrid[2] bounded storage model BSM [19].

The implementations of OT based on noisy channels is of particular interest since noise is inherently present in any physical channel. At the same time, a common drawback of the noise-based OT implementations is their (in)efficiency. The required number of the noisy channel uses is of order $O(\log(1/\alpha)^{2+\varepsilon})$ for any $\varepsilon > 0$ where α is an upper bound on all security failure probabilities in the protocol [8]. In the notation which we introduce in this work, this means that the rate (that is the ratio of the length of Alice's secrets to the overall number of noisy channel uses) of such implementation is zero. The rate can only be non-zero if the number of channel uses is of order $O(\log(1/\alpha))$ (or lower). This means that the OT capacity (being a supremum of all achievable rates) is, in particular, a good measure for *practical* applicability of a given primitive for building OT based on it. We note that an efficient and practical OT protocol based in bounded quantum memory model (together with the model itself) was proposed by Damgård, Fehr, Salvail and Schaffner in [12], but the notion of the OT capacity for quantum channels is still to be defined. In this paper, we are only concerned with classical communications.

Speaking of the related results, we first note that the OT capacity is unknown for noisy channels in general. It is known to be non-negligible for honest-but-curious (or passively cheating) players [21], [8] (implicitly, it can be found already in [7]), but the non-zero rates have not ever been achieved in

[1] Which appeared to be equivalent [4] in the sense that they can be efficiently reduced to each other.

[2] Basically, this is a BSM with an additional computational assumption which must hold only online (i.e., while the protocol is taking place) and later it can be compromised but this will not influent the security of the protocol. If an additional assumption holds then this will be information-theoretically secure.

For the sake of completeness, we note that such flavor of security (i.e., as long as an online assumption holds, the protocol is unconditionally secure no matter what happens afterwards) was introduced in [1] under name of *everlasting* security.

1-4244-0504-1/06/$20.00 ©2006 IEEE

the case of fully malicious players. The problem of reducibility between different weaker primitives to OT received a lot of attention in the recent years which is not surprising as it seems difficult to find a (classical) physical device or phenomena which would produce OT as a black box.

In this paper, we begin to investigate the OT capacity of some particular known primitives by showing that for the erasure channel, in the case of passive adversaries, one can compute this quantity. This is not very surprising in the light of the fact that OT and the erasure channel (or Rabin Oblivious Transfer [23]) are equivalent [4]. Although, in this work, we exploit the protocol in the spirit of [5]. Furthermore, for the case of malicious players, we introduce a lower bound for the OT capacity.

Our protocol is similar to Protocol 3.2 by Brassard, Crépeau and Wolf [3] but their protocol is based on 1-out-of-2 OT, so some modification is needed to employ the erasure channel. The lower bound of Lemma 7 is similar to lower bounds by Dodis and Micali [16], and Wolf and Wullschleger [26] which were obtained in a context of reducibility between flavors of k-out-of-n OT for strings of different length.

Independently of this work, Crépeau and Savvides in their recent paper [9] provide, in particular, an optimal reduction from 1-out-of-2 OT to the erasure channel. Their reduction has a rate 1/2, i.e., it achieves the OT capacity of the erasure channel. The improvement is based on employing Interactive Hashing [22] which, at the same time, gives a substantial communication complexity overhead comparing to our protocol. The optimal protocol requires $O(k)$ rounds of communication[3] where k is the length of the secret bit-strings. Ours is constant-round, actually it requires only 3 messages. As a matter of fact, we believe that our protocol is round-optimal, but we do not claim it here.

Our paper is organized as follows: in Section II, we give some useful notation and definitions. In Section III, we show a lower bound for the OT capacity in the case of malicious players. Section IV is devoted to calculation of the OT capacity for the case of honest-but-curious players.

II. Preliminaries

We begin with some basic definitions, most of them were first introduced in [21]. 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 an oblivious transfer protocol, the sender's input consists of m strings, each one having length k. We denote those strings by $U_i = b_0^{(i)} b_1^{(i)} \dots b_{k-1}^{(i)}$, $0 \le i < m$, where $b_j^{(i)} \in \{0,1\}$, $0 \le j \le k-1$. The receiver's input is a single integer c, $0 \le c < m$. At the end of the protocol Bob receives U_c as his output, while Alice receives nothing. The protocol is said to be *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 cheating) defines random variables for all the messages exchanged and the 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 the corresponding random variable. 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 by the players Alice and Bob on inputs x_A and x_B which generates the outputs y_A and y_B by $[A,B](x_A,x_B) = (y_A,y_B)$. The event that a party receives no output is represented by $y = \Delta$.

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

$$\Pr\big\{[A,B]((U_0,U_1,\dots,U_{m-1}),c) \neq (\Delta,U_c)\big\} \le \epsilon$$

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

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

$$I(V_A;C) \le \epsilon$$

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).

It is *ϵ-private* for Alice if for any possible behavior of Bob, at most one of the m strings is not ϵ-invisible to Bob. Here, we say that the ith string is *ϵ-invisible* to Bob for a given strategy Σ he follows if there exists a random variable $\widetilde{V}$ (depending on $\Sigma, U_0, \dots, U_{i-1}, U_{i+1}, \dots, U_{m-1}$) taking values in views such that for all U_i,

$$\Pr\{V_B \neq \widetilde{V}\} \le \epsilon.$$

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

A protocol $[A,B](x_A,x_B) = (y_A,y_B)$ is said to be an ϵ-private, ϵ-correct 1-out-of-m string oblivious transfer *secure against honest-but-curious players* when in the above definitions the parties A and B follow the protocol but try to gather as much information as they can from their views of the protocol V_A and V_B, respectively.

As a genuine noise is considered an expensive resource, it is desirable to minimize as much as possible the use of the noisy channel/correlation when implementing string oblivious transfer. In order to measure how efficiently an OT protocol uses the noisy channel, we introduce the concept of *rate of an oblivious transfer protocol*. Let $[A,B](x_A,x_B) = (y_A,y_B)$ be a protocol implementing ϵ-private, ϵ-correct 1-out-of-m string oblivious transfer, 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 in this protocol.

[3]These communication are noiseless, the noisy channel is used, as well as in our case, $O(n)$ times where n is a security parameter.

Definition 2: The 1-*out-of-*m *oblivious transfer rate* of $[A,B](x_A,x_B)=(y_A,y_B)$ is defined as

$$R_m=\frac{k}{n}.$$

In our protocols, n will work as a security parameter. Thus, we are interested in the behavior of R_m when n approaches infinity.

A rate R^* is said to be *achievable* if for any $\epsilon,\gamma>0$, there exists a protocol $[A,B](x_A,x_B)=(y_A,y_B)$ implementing ϵ-private, ϵ-correct $\binom{m}{1}$-OT^k which, for sufficiently large n, has $R_m\geq R^*-\gamma$.

Definition 3: The supremum of all achievable rates is called the 1-*out-of-*m *OT capacity* of the channel W or of the correlation P, denoted respectively, $C_{\binom{m}{1}\text{-OT}}(W)$ or $C_{\binom{m}{1}\text{-OT}}(P)$.

We stress once more that these rates count only the use of the channel/correlation — protocols will also use error-free communication which we consider unlimited.

III. Lower Bound

In this work, we consider the case when Alice has two secrets as her input, i.e., $m=2$. We first give the protocol (adapted from [5], Protocol 4.2) which achieves the rate $R_2=1/4$ and is secure against fully malicious players. Let Alice's input strings be U_0 and U_1 and Bob's choice bit be c.

Protocol

1) Alice chooses a random binary string $r_1,\ldots,r_n$ of dimension n and sends it to Bob over the erasure channel.
2) After receiving the string, 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. Let $c\in\{0,1\}$ be Bob's input to the OT protocol. Bob chooses S_0 and S_1 so that, for any $i\in S_c$, r_i is not an erasure. Bob sends the sets S_0 and S_1 to Alice over the noiseless channel.
3) Denote the jth element of S_i by $S_i(j)$. After receiving S_0 and S_1, Alice generates a random matrix G of dimension $(1/2-\eta)n\times n/4$. She computes the vectors $A_0=\rho_0*G$ and $A_1=\rho_1*G$ where $\rho_0=[r_{S_0(1)},\ldots,r_{S_0(n)}]$ and $\rho_1=[r_{S_1(1)},\ldots,r_{S_1(n)}]$, "$*$" 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 bitwise exclusive-or. She sends G, B_0 and B_1 to Bob over the noiseless channel.
   Finally, Bob computes $A_c=\rho_c*G$ and obtains $U_c=A_c\oplus B_c$.

We first argue the security of this protocol.

Theorem 4: There exist $\epsilon>0$ and $0<\eta<1/2$ such that the above protocol is ϵ-correct and ϵ-private implementation of $\binom{m}{1}$-OT^k for sufficiently large n.

Proof (Sketch). Follows from the argument in Section 4 of [5].

For correctness, we note that if $0<\eta<1/2$ holds and the players behave honestly, then by the law of large numbers, Bob is almost certainly able to find enough of received bits to fill the vector ρ_c. Then, the correctness property can be easily verified by inspecting the steps of the protocol.

As for Alice's privacy, we note that in Step 2, the malicious Bob will not be able to fill both vectors ρ_0 and ρ_1 with bits, so at least in one of the vectors, there will appear a constant fraction of erasures. It is clear that on the average, the highest number of bits which can appear in either vector is n/4 independently of Bob's cheating strategy. Therefore, the choice of the dimension for matrix G allows us to use the privacy amplification result [2] which implies that Bob will have exponentially small (in n) information about at least one of U_0 or U_1, i.e. at least one of the bit strings U_0 or U_1 will be ϵ-invisible for Bob for any $\epsilon>0$.

Privacy for Bob follows from the fact that the sets S_0 and S_1 give Alice no information on c since the bits are erased by the channel independently. □

The next corollary follows immediately.

Corollary 5: $R_2=1/4$ for the case of malicious players.

At the same time, if the parties are honest-but-curious, a rate equal to $1/2$ can be obtained.

Corollary 6: $R_2=1/2$ for the case of honest-but-curious players.

Proof Sketch. It easy to see that when Bob follows the protocol, the privacy amplification is not needed because Bob will indeed put all the received bits in the subset ρ_c corresponding to his choice. Then, by the law of large numbers, ρ_{1-c} will contain only erasures.

Let us now modify our protocol such that Alice encrypts her secrets with ρ_0 and ρ_1 instead of A_0 and A_1. Clearly, this protocol is an ϵ-private, ϵ-correct 1-out-of-m string oblivious transfer secure against honest-but-curious players.

Note that this protocol has a rate R_2 approaching $1/2$ when n approaches infinity. The proof now follows. □

We prove the optimality of this rate in the following section.

IV. Capacity for Honest-But-Curios Case

Consider a protocol implementing $\binom{m}{1}$-OT^k based on the existence of an erasure channel with erasure probability 1/2. Let X^n and Y^n denote the n-dimensional random variables representing, respectively, an input and an output of the binary erasure channel. Denote the conversation over the noiseless channel by T. The set of m k-bit strings which constitute Alice's input to the protocol is represented here by U. Alice's and Bob's views after the protocol is completed are denoted by V_A and V_B, respectively.

Lemma 7: For any secure $\binom{2}{1}$-OT^k protocol based on the erasure channel, the rate $R_2=1/2$ is optimal.

Proof Sketch. ¿From Definition 1, we know that $H(U|V_B)=(m-1)k$ as Bob does not learn $m-1$ strings held by Alice after the protocol is finished. Furthermore, it is clear that, if Bob gets to know X^n, he should be able to completely break the security of the protocol, since otherwise, Alice must have some prior knowledge on Bob's choice. Thus, $H(U|V_BX^n)=0$.

We have that,

$$H(U|X^nV_B)=H(UX^n|V_B)-H(X^n|V_B),$$

therefore

$$H(X^nU|V_B)=H(X^n|V_B),$$

it follows that $H(X^n|V_B)\geq H(U|V_B)$.

Then, taking into account $V_B=TY^n$, we have

$$\begin{aligned}nH(X|Y)&\geq H(X^n|Y^n)\geq H(X^n|Y^nT)\\&=H(X^n|V_B)\geq H(U|V_B)=(m-1)k\end{aligned}$$

Thus, making $m = 2$ we obtain

$$R_2 = k/n \leq H(X|Y)$$

For the erasure channel, $H(X|Y) = 1/2$. □

Corollary 8: $C_{\binom{2}{1}\text{-OT}}(\text{erasure channel}) = 1/2$ for the case of honest-but-curious players.

Proof. Follows from Corollary 6 and Lemma 7. □

V. Conclusion and Open Question

In this work, we have introduced the concept of rate of oblivious transfer protocol and defined the OT capacity as the supremum of all achievable rates. We have also shown that the OT capacity of the erasure channel with erasure probability 1/2 is 1/2 (bits per instance) for the passive case and exposed the protocol whose rate is 1/4 for the fully malicious case.

The question of computing the OT capacity of general noisy channels/correlations is open.

References

[1] Y. Aumann, Y.Z. Ding, and M. O. Rabin, "Everlasting security in the bounded storage model," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1668–1680, 2002.

[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] G. Brassard, C. Crépeau, and S. Wolf, "Oblivious transfers and privacy amplification," *J. of Cryptol.*, vol. 16, no. 4, pp. 219–237, 2003.

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

[5] C. Crépeau, "Efficient Cryptographic Protocols Based on Noisy Channels," *Proc. EUROCRYPT '97*, LNCS, vol. 1233, pp. 306–317, 1997.

[6] C. Cachin, C. Crépeau, and J. Marcil, "Oblivious Transfer with a Memory-Bounded Receiver," *Proc. 39th IEEE FOCS*, pp. 493–502, 1998.

[7] C. Crépeau, J. Kilian, "Achieving oblivious transfer using weakened security assumptions," *Proc. 29th IEEE FOCS*, pp. 42–52, 1988.

[8] C. Crépeau, K. Morozov, S. Wolf, "Efficient Unconditional Oblivious Transfer from Almost any Noisy Channel," *Proc. SCN '04*, LNCS, vol. 3352, pp. 47-59, 2005.

[9] C. Crépeau, G. Savvides, "Optimal Reductions Between Oblivious Transfers Using Interactive Hashing," Appears in *Proc. EUROCRYPT '06*, LNCS, 2006.

[10] Y.Z. Ding, "Oblivious transfer in the bounded storage model," *CRYPTO '01*, LNCS, vol. 2139, pp. 155–170, 2001.

[11] I. Damgård, S. Fehr, K. Morozov, L. Salvail, "Unfair Noisy Channels and Oblivious Transfer," *Proc. TCC '04*, LNCS, vol. 2951, pp. 355–373, 2004. (Full version is available from: http://www.brics.dk/RS/03/36)

[12] I. Damgård, S. Fehr, R. Renner, L. Salvail, C. Schaffner, "A Tight High-Order Entropic Relation with Application in the Bounded Quantum-Storage Model", *Submitted to 47th IEEE FOCS*, 2006.

[13] I. Damgård, S. Fehr, L. Salvail, C. Schaffner, "Cryptography In the Bounded Quantum-Storage Model", *Proc. 46th IEEE FOCS*, pp. 449-458, 2005.

[14] Y.Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel, "Constant round oblivious transfer in the bounded storage model," *Proc. TCC '04*, LNCS, vol. 2951, pp. 446–472, 2004.

[15] I. Damgård, J. Kilian, L. Salvail, "On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions," *Proc. EUROCRYPT '99*, LNCS, vol. 1592, pp. 56–73, 1999.

[16] Y. Dodis, S. Micali, "Lower bounds for Oblivious Transfer Reduction," *EUROCRYPT '99*, LNCS, vol. 1592, pp. 42–54, 1999.

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

[18] O. Goldreich, S. Micali, A. Wigderson, "How to Play Any Mental Game, or: A completeness theorem for protocols with honest majority," *Proc. 19th ACM STOC*, pp. 218–229, 1987.

[19] D. Harnik and M. Naor, "On Everlasting Security in the Hybrid Bounded Storage Model", *To appear in ICALP 2006*.

[20] J. Kilian, "Founding Cryptography on Oblivious Transfer," *Proc. 20th ACM STOC*, pp. 20–31, 1988.

[21] A. C. A. Nascimento, A. Winter, "OT from any genuine noise," *Preprint*, 2004.

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

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

[24] R. L. Rivest, "Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer," *Manuscript*, 1999. Available at: http://theory.lcs.mit.edu/~rivest/Rivest-commitment.pdf

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

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