# On oblivious transfer capacity

R. Ahlswede
Universität Bielefeld
Bielefeld, Germany

I. Csiszár
Alfréd Rényi Mathematical Institute
of Hung. Acad. of Sci.
Budapest, Hungary

***Abstract*— The concept of oblivious transfer capacity has been recently introduced by Nascimento and Winter. We give an upper bound to this capacity, both for source and channel models, and prove that it is tight for a class of channels. For other cases, lower bounds are provided. The tools include known results on secrecy capacity of simple source and channel models.**

## I. Introduction

Oblivious transfer (OT) is a fundamental concept in cryptography, see for example [4]. The term has been used with different meanings, including a simple transmission over a binary erasure channel. In this paper, unless stated otherwise, OT means "1-2 oblivious string transfer" [4]: Alice has two length-k binary strings $K_0$ and $K_1$ and Bob has a single bit $Z$ as inputs; an OT protocol should let Bob learn $K_Z$ while Alice remains ignorant of $Z$ and Bob of $K_{\bar{Z}}$ ($\bar{Z} = 1 - Z$). The Shannon-theoretic approach is used, thus ignorance means negligible amount of information; formal definitions are given in Section II.

Both source and channel models of OT are considered. In a source (or noisy correlations) model, a discrete memoryless multiple source (DMMS) with two component sources is given, whose outputs $X^n = (X_1, \ldots, X_n)$ and $Y^n = (Y_1, \ldots, Y_n)$ are available to Alice respectively Bob. In a channel model, a discrete memoryless channel (DMC) is given, Alice selects the inputs $X^n$ and Bob observes the outputs $Y^n$. In both models, Alice and Bob may use a public noiseless channel for unrestricted communication. The cost of OT is measured by the number $n$ of observed DMMS outputs or of DMC transmissions; the public channel use is considered free.

The OT capacity $C_{OT}$ of a DMMS of DMC is the limit as $n \to \infty$ of $\frac{1}{n}$ times the largest $k$ for which OT is possible with "cost" $n$. This concept has been introduced by Nascimento and Winter [7] who also proved $C_{OT} > 0$ under general conditions. For previous results, showing that a DMMS or DMC makes OT possible for any $k$ if $n$ is sufficiently large (but not that $\frac{k}{n}$ may be bounded away from 0 while the conditions (1)-(3) below are satisfied) see the references in [7]. A related concept of commitment capacity has been introduced and characterized in [8].

In the literature, much of the effort is devoted to designing OT protocols that prevent a dishonest Alice from learning about Bob's bit $Z$, or a dishonest Bob from obtaining information also about $K_{\bar{Z}}$, if they violate the agreed upon protocol. This issue is not addressed here, both Alice and Bob are assumed to honestly follow the protocol. This simplification facilitates gaining basic insights, expected to be relevant also in dealing with more practical but more difficult situations where protection against cheating is also required. Of course, upper bounds derived for the simpler case are even more valid in those situations.

We derive a general upper bound to $C_{OT}$ and show the tightness of this bound for a class of channels. For other cases, we give lower bounds to $C_{OT}$ which do not coincide with the upper bound. A necessary and sufficient condition for $C_{OT} > 0$ is also given which is similar to but not the same as the condition in [7]; the difference is due to our not dealing with "distrustful cryptography".

## II. Statement of results

An $(n, k)$ *protocol* for OT via a DMC is described as follows. Let $K_0, K_1, Z$, and $M, N$ be independent random variables (RVs), $K_0$ and $K_1$ uniformly distributed on $\{0,1\}^k$, and $Z$ on $\{0,1\}$, while $M$ and $N$ (serving for randomization for Alice resp. Bob) are arbitrary. At times $t = 1, \ldots, n$ Alice transmits a RV $X_t$ over the DMC, Bob receiving $Y_t$. Here $X_t$ is chosen as a function of $K_0, K_1, M$, and of the previous public communication $F^{t-1} = F_1 \ldots F_{t-1}$ where $F_i$ denotes the public communication in the time interval $(i, i+1)$ that may be interactive: $F_i$ is a sequence of messages sent alternatingly by Alice and Bob, those by Alice are functions of $K_0, K_1, M$, and of the messages previously received by her, those by Bob are functions of $Z, N$, and of the messages previously received by him, including $Y^i = Y_1 \ldots Y_i$. Finally, Bob produces an estimate $\hat{K}_Z$ of $K_Z$ where $\hat{K}_0$ and $\hat{K}_1$ are functions of $Y^n, N$, and of the total public communication $\mathbf{F} = F_1 \ldots F_n$.

An $(n, k)$ protocol for OT via a DMMS is similar but simpler: then $X^n, Y^n$ are the length-n outputs of the two component sources, independent of $K_0, K_1, Z, M, N$, and the public communication takes place after Alice and Bob have observed $X^n$ resp. $Y^n$, thus $\mathbf{F} = F_n$.

A positive number $R$ is an *achievable OT rate* for a DMMS of DMC if, for $n$ sufficiently large, there exist $(n, k)$ protocols with $\frac{k}{n} \to R$ letting Bob learn $K_Z$, that is

$$Pr\{\hat{K}_Z \neq K_Z\} \to 0 \tag{1}$$

while Alice remains ignorant of $Z$:

$$I(K_0 K_1 M X^n \mathbf{F} \wedge Z) \to 0 \tag{2}$$

and Bob learns nothing about $K_{\bar{Z}}$:

$$I(N Y^n \mathbf{F} \wedge K_{\bar{Z}} \mid Z) \to 0. \tag{3}$$

The dependence on $n$ of the RVs in (1)-(3) has been suppressed, to keep the notation transparent.

The *OT capacity* $C_{OT}$ of a DMMS or DMC is the largest achievable OT rate, or 0 if no $R > 0$ is achievable.

**Remark.** An alternative definition requires convergence with exponential speed in (1)-(3). The results in this paper hold also with that definition.

**Theorem 1.** *The OT capacity of a DMMS with generic RVs $X, Y$ is bounded above by*

$$\min\left[I(X \wedge Y), H(X \mid Y)\right]. \tag{4}$$

*The OT capacity of a DMC is bounded above by the maximum of (4) for RVs $X, Y$ connected by this DMC.*

**Remark.** This bound holds also for a weaker concept of OT, requiring Bob to learn or remain ignorant about a single length-$k$ string of Alice according as $Z$ equals 0 or 1, Alice remaining ignorant of $Z$. Also, the "strong secrecy" postulated in (3), see [5], could be relaxed to "weak secrecy", dividing the mutual information by $k$, see Section III.

**Theorem 2.** *For a binary erasure channel with erasure probability $p$*

$$C_{OT} = \min(1-p, p),$$

*thus the bound in Theorem 1 is tight.*

A DMC $\{W : \mathcal{X} \to \mathcal{Y}\}$ will be called a *generalized erasure channel* (GEC) if the output alphabet $\mathcal{Y}$ can be decomposed as $\mathcal{Y}_0 \cup \mathcal{Y}^*$ such that $W(y \mid x)$ does not depend on $x \in \mathcal{X}$ if $y \in \mathcal{Y}^*$. For a GEC, we denote $W_0(y \mid x) = \frac{1}{1-p^*} W(y \mid x)$, $x \in \mathcal{X}$, $y \in \mathcal{Y}_0$, where $p^*$ is the sum of $W(y \mid x)$ for $y \in \mathcal{Y}^*$ (not depending on $x$). The Shannon capacity of the DMC $\{W_0 : \mathcal{X} \to \mathcal{Y}_0\}$ is denoted by $C(W_0)$.

**Theorem 3.** *For a GEC, the bound in Theorem 1 is tight if $p^* \geq 1/2$, then $C_{OT} = (1-p^*)C(W_0)$. If $0 < p^* < 1/2$, a lower bound is $C_{OT} \geq p^* C(W_0)$.*

**Remark.** The latter bound is not tight in general, see Example 2 in Section IV.

**Theorem 4.** *The OT capacity of a DMMS or DMC is positive if and only if there exist $x'$ and $x"$ in $\mathcal{X}$ such that the joint probabilities $P_{XY}(x', y)$ and $P_{XY}(x", y)$, respectively the conditional probabilities $W(y \mid x')$ and $W(y \mid x")$, are not equal for all $y \in \mathcal{Y}$, and are simultaneously positive for some $y \in \mathcal{Y}$.*

**Remark.** Theorem 4 says that the positivity of the upper bound in Theorem 1, after merging identical rows (if any) of the matrix of joint respectively conditional probabilities, is necessary and sufficient for positive OT capacity, see Section III.

## III. Proof sketches

**Lemma 1.** *For arbitrary RVs $U, V, Z$ with values in finite sets $\mathcal{U}, \mathcal{V}, \mathcal{Z}$, and any $z_0, z_1$ in $\mathcal{Z}$ with $Pr\{Z = z_0\} = p > 0$, $Pr\{Z = z_1\} = q > 0$,*

$$|H(U \mid V, Z = z_0) - H(U \mid V, Z = z_1)|$$
$$\leq c\sqrt{I(UV \wedge Z)}\log_2 |\mathcal{U}| + h\left(\min\left[c\sqrt{I(UV \wedge Z)}, \frac{1}{2}\right]\right)$$

*where $h(t) = -t\log_2 t - (1-t)\log_2(1-t)$, and $c$ is a constant depending on $p$ and $q$.*

The proof, whose details are omitted, uses the Pinsker inequality to bound the variation distance of the two conditional distributions of $UV$, given $Z = z_0$ respectively $Z = z_1$. Then the conditional entropy difference is bounded as in [2]. Though the value of $c$ is not relevant here, by careful calculation (including an improvement of the bound in [2]) we have shown that $c = 3\sqrt{\frac{(p+q)\ln 2}{2pq}}$ suffices. Thus, for the case $p = q = 1/2$ used below, a suitable constant factor is $c = 3\sqrt{2\ln 2}$.

**Proof of Theorem 1.** Concentrating on channel models, we sketch the proof of the following stronger result: if there exist $(n, k)$ protocols with $\frac{k}{n} \to R$ and

$$Pr\{\hat{K}_0 \neq K_0 \mid Z = 0\} \to 0 \tag{5}$$

$$I(K_0 X^n \mathbf{F} \wedge Z) \to 0 \tag{6}$$

$$\frac{1}{k} I(NY^n \mathbf{F} \wedge K_0 \mid Z = 1) \to 0 \tag{7}$$

then $R$ does not exceed the maximum of (4).

Now, (6) implies by Lemma 1 that

$$H(K_0 \mid X^n \mathbf{F}, Z = 0) - H(K_0 \mid X^n \mathbf{F}, Z = 1) = o(k) \tag{8}$$

$$H(K_0 \mid \mathbf{F}, Z = 0) - H(K_0 \mid \mathbf{F}, Z = 1) = o(k). \tag{9}$$

From (9) and the consequence $I(\mathbf{F} \wedge K_0 \mid Z = 1) = o(k)$ of (7), it follows due to $H(K_1 \mid Z = 0) = H(K_1 \mid Z = 1) = k$ that

$$I(K_0 \wedge \mathbf{F} \mid Z = 0) = o(k). \tag{10}$$

If (5) and (10) held without conditioning on $Z = 0$ then $K_0$ would be a secret key for Alice and Bob, with (weak sense) security from an eavesdropper observing the public communication $\mathbf{F}$. The rate $\frac{k}{n}$ of such secret key is asymptotically bounded [5], [1] as

$$\frac{k}{n} \leq \frac{1}{n}\sum_{t=1}^{n} I(X_t \wedge Y_t) + \varepsilon_n\,, \quad \varepsilon_n \to 0. \tag{11}$$

The actual (5) and (10) imply the analogue of (11) with $I(X_t \wedge Y_t)$ replaced by $I(X_t \wedge Y_t \mid Z = 0)$. This replacement, however, has an asymptotically negligible effect since, due to the consequence $\max_t I(X_t \wedge Z) \to 0$ of (6), the conditional distribution of $X_t$ on the condition $Z = 0$ differs negligibly from the unconditional distribution. Thus, (5)-(7) imply (11).

It is not hard to show that $K_0 \to X^n \mathbf{F} \to NY^n \mathbf{F} Z$ is a Markov chain. This, (5), and Fano's inequality give

$$H(K_0 \mid X^n \mathbf{F}, Z = 0) \leq H(K_0 \mid NY^n \mathbf{F}, Z = 0) = o(k). \tag{12}$$

Then

$$k = H(K_0 \mid Z=1) \overset{(i)}{=} H(K_0 \mid NY^n\mathbf{F}, Z=1) + o(k)$$

$$\leq H(K_0 \mid X^nY^n\mathbf{F}, Z=1) + H(X^n \mid NY^n\mathbf{F}, Z=1) + o(k)$$

$$\overset{(ii)}{\leq} H(X^n \mid Y^n, Z=1) + o(k) \leq \sum_{t=1}^{n} H(X_t \mid Y_t, Z=1) + o(k)$$

where (i) follows from (7) and (ii) from (8) and (12). In the last sum, the conditioning on $Z=1$ has an asymptotically negligible effect as before, thus we have

$$\frac{k}{n} \leq \frac{1}{n}\sum_{t=1}^{n} H(X_t \mid Y_t) + \varepsilon_n, \quad \varepsilon \to 0. \tag{13}$$

Finally the main term in (11) is $\leq I(X_T \wedge Y_T)$ and the main term in (13) is $\leq H(X_T \mid Y_T)$ where $T$ is a RV uniformly distributed on $\{1,\ldots,n\}$, independent of the RVs $X_t, Y_t$. Hence, the claim follows from (11), (13).

**Proof of Theorem 2.** Theorem 1 gives the upper bound $C_{OT} \leq \min(1-p,p)$. The following protocol shows that each $R < \min(1-p,p)$ is an achievable OT rate.
(i) Alice transmits over the DMC $n$ independent equiprobable bits $X^n$.
(ii) Bob determines the set $G \subset \{1,\ldots,n\}$ of "good" positions where no erasure occurred, and selects from $G$ a random subset of size $k = nR$, and similarly from the "bad" set $G^c$. Denoting by $S_0$ the set of positions selected from $G$ or $G^c$ according as $Z=0$ or $Z=1$, and by $S_1$ the other set, Bob tells Alice $S_0$ and $S_1$, not leaking any information on $Z$.
(iii) Alice adds her strings $K_i$ to $\{X_t : t \in S_i\}$, $i=0,1$, bitwise mod 2, and she reports the sums to Bob.

As Bob knows $X_t$ for $t \in G$, he can recover $K_Z$, but remains ignorant of $K_{\bar{Z}}$, not knowing $X_t$ for $t \in G^c$.

**Proof of Theorem 3.** Due to Theorem 1, it suffices to show that $C_{OT} \geq \min(1-p^*,p^*)C(W_0)$, that is, that $R = R'R"$ is an achievable OT rate if $R' < \min(1-p^*,p^*)$, $R" < C(W_0)$. To this, a DMMS secrecy result [5] [1] will be used: Suppose Alice and Bob observe $l$ outputs of the component sources of a DMMs whose generic RVs have mutual information larger than $R$. Then, for $l$ sufficiently large, Alice can securely transmit $k = lR$ bits to Bob via sending a public message, with negligible probability of error and negligible leak of information to an eavesdropper who sees the public message alone.

Now, Alice transmits over the DMC $n$ i.i.d. RVs $X_t$ that achieve Shannon capacity (of both channels $W$ and $W_0$). Then Bob selects $l = nR$ positions at random from the good set $G = \{t : Y_t \in \mathcal{Y}_0\}$,as well as from the bad set $G^c = \{t : Y_t \in \mathcal{Y}^*\}$. Calling the resulting sets $S_0$ and $S_1$ as in the previous proof, Bob tells Alice $S_0$ and $S_1$, leaking no information on $Z$.

Under the condition $Z=0$, the RVs $\{(X_t,Y_t) : t \in S_0\}$ represent $l$ output pairs of a DMMS whose generic RVs have mutual information $C(W_0)$, while under the condition $Z=1$ these $X_t$ and $Y_t$ are independent. The joint distributions of $\{(X_t,Y_t) : t \in S_1\}$ under the same conditions coincide with those of $\{(X_t,Y_t) : t \in S_0\}$ as above, reversing $Z=0$ and $Z=1$. Hence, by the cited result and the assumption $R" < C(W_0)$, there exists a function $f$ on $\{0,1\}^k \times \mathcal{X}^l$, where $k = lR" = nR$, with the following properties: If Alice sends the public messages $f(K_0,\{X_t : t \in S_0\})$, $f(K_1,\{X_t : t \in S_1\})$ then, in case $Z=0$ when Bob knows $\{Y_t : t \in S_0\}$, Bob can recover $K_0$ but remains ignorant of $K_1$ regarding which he observes, in effect, the public message only. Similarly, in case $Z=1$ Bob can recover $K_1$ remaining ignorant of $K_0$.

**Proof of Theorem 4.** If some rows of the matrix of joint or conditional probabilities are equal then merging the corresponding elements of $\mathcal{X}$ does not change OT capacity. The necessity part of the assertion follows applying Theorem 1 after this merging. For sufficiency, concentrate on channel models. Consider the two-block extension of the given channel $\{W\}$ and restrict its input alphabet $\mathcal{X}^2$ to $\tilde{\mathcal{X}} = \{(x',x"),(x",x')\}$, for $x',x"$ in the hypothesis. It follows by that hypothesis and Theorem 3 that the so obtained channel $\{\tilde{W} : \tilde{\mathcal{X}} \to \mathcal{Y}^2\}$ which is a GEC, has positive OT capacity. Hence so does also the channel $\{W\}$.

## IV. Discussion, examples

The OT capacity of discrete memoryless source and channel models has been studied. A general upper bound, and a lower bound for generalized erasure channels were given, determining the OT capacity of binary erasure channels, and of any GEC with erasure probability $\geq 1/2$. For the general case, lower bounds were shown to follow from those for GECs. While in proving the upper bound very complex protocols were admitted, the achievability (lower bound) results use simple protocols. It remains open whether OT capacity can be achieved in general with protocols of comparable simplicity, similarly, for example, to multiterminal secrecy capacities [3].

Protection against cheating has not been addressed. Still, it is worth noting that while the protocols in Theorems 2 and 3 are vulnerable to cheating by Bob if the erasure probability is less than $1/2$ (when Bob, in addition to learning $K_Z$, can gain information about $K_{\bar{Z}}$ via dishonest choice of $S_{\bar{Z}}$), such cheating could be prevented by a modified protocol achieving the same OT rate. To this, sets $S_0$ and $S_1$ both of size $\frac{n}{2}$ are taken, with $S_Z \subset G$; then, as $S_{\bar{Z}}$ intersects $G$, a stronger DMMS secrecy result has to be invoked in which the eavesdropper knows more than the public message alone.

The approach in this paper easily extends to other versions of OT, one mentioned in connection with Theorem 1. For example, Alice may have $m$ stings $K_1,\ldots,K_m$ and Bob may chose either of them ("1 of $m$ OT") or any subset of them, while Bob has to remain ignorant of the other stings, and Alice of Bob's choice. Our reason for stating Lemma 1 for a not necessarily binary RV $Z$ has been to make it suitable to prove analogues of Theorem 1 for such OT problems, too.
We conclude by three examples.

**Example 1.** Consider a binary symmetric channel (BSC) with crossover probability $p$, and define a channel $\{\tilde{W} : \tilde{\mathcal{X}} \to \mathcal{Y}^2\}$ by restricting the input alphabet of the two-block

extension of this BSC to $\tilde{\mathcal{X}} = \{(0,1),(1,0)\}$.Then $\tilde{W}$ is a GEC with $\mathcal{Y}^* = \{(0,0),(1,1)\}$, and the corresponding $\tilde{W}_0$ is a BSC with crossover probability $p^2/(1-p^*)$ where $p^* = 2p(1-p) < 1/2$. Hence, Theorem 3 implies for the OT capacity of a BSC

$$C_{OT} \geq \frac{1}{2}p^* C(\tilde{W}_0) = p(1-p)\left(1 - h\left(\frac{p^2}{1-2p(1-p)}\right)\right).$$

**Example 2.** Consider the GEC with $\mathcal{X} = \{0,1\}, \mathcal{Y} = \{0,1,*\}$,

$$W = \begin{pmatrix} (1-p)(1-\varepsilon) & p(1-\varepsilon) & \varepsilon \\ p(1-\varepsilon) & (1-p)(1-\varepsilon) & \varepsilon \end{pmatrix}.$$

For its OT capacity, if $0 < \varepsilon < 1/2$, Theorem 3 gives $C_{OT} \geq \varepsilon C(W_0)$ where $W_0$ is the BSC with crossover probability $p$. Another lower bound in $C_{OT} \geq \frac{1}{2}p^* C(\tilde{W}_0)$ where $\{\tilde{W} : \tilde{\mathcal{X}} \to \mathcal{Y}^2\}$ is the GEC defined similarly as in Example 1, with $\mathcal{Y}^* = \{(0,0),(1,1),(**)\}$ and $p^* = 2p(1-p)(1-\varepsilon)^2 + \varepsilon^2$. If $\varepsilon \to 0$, the latter bound approaches that in Example 1, while the previous bound goes to 0. This shows that the lower bound in Theorem 3 is not tight, in general.

**Example 3.** Consider the additive DMC with $\mathcal{X} = \mathcal{Y} = \{0,1,2,3\}$, $Y = X + N$ (mod 4), $N$ binary $1/2 - 1/2$. This is not a GEC but the bound in Theorem 1 is tight for it, $C_{OT} = 1$. Indeed, the following simple $(1,1)$ protocol achieves perfect OT. (i) Alice transmits over the channel a uniformly distributed rv $X$. (ii) Bob receives $Y = X + N$ (mod4), and tells Alice $\phi = 0$ or 1 according as $Y + Z$ is even or odd. (iii) Alice reports the mod2 sums $K_0 + i_\phi(X)$ and $K_1 + i_{1-\phi}(X)$ were $i_0$ and $i_1$ are the indicator functions of the sets $\{1,2\}$ and $\{2,3\}$. This unambiguously tells Bob the bit $K_Z$, keeping him fully ignorant of $K_{\bar{Z}}$, because an even or odd value of $Y$ uniquely determines $i_0(X)$ respectively $i_1(X)$ but provides 0 information about $i_1(X)$ respectively $i_0(X)$.

## REFERENCES


[1] R. Alhswede, I. Csiszár, "Common Randomness in Information Theory and Cryptography, Part I." *IEEE Trans. Inf. Theory*, vol.39, pp.1121-1132, 1993.

[2] R. Alicki, M.Fannes, "Continuity of Quantum Conditonal Information" *J. Phys. A: Math. Gen.* vol. 37, pp.L55-L57, 2004.

[3] I. Csiszár, P. Narayan, "Secrecy Capacities for Multiterminal Channel Models", submitted to *IEEE Trans. Inf. Theory*, spec. issue on information theoretic secrecy.

[4] J. Kilian, "Founding Cryptography on Oblivious Transfer", *STOC 1998*, pp.20-31, 1988.

[5] U. Maurer, "Secret Key Agreement by Public Discussion", *IEEE Trans. Inf. Theory*, vol.39., pp.733-742, 1993.

[6] U. Maurer, "The Strong Secret Key Rate of Discrete Random Triples", *Communications and Cryptography: Two sides of One Tapestry*, R.E. Blahut et.al. Eds., pp.271-285, Kluwer 1994.

[7] A. Nascimento, A. Winter, "On the Oblivious Transfer Capacity of Noisy Correlations", *Proc. ISIT 2006, Seattle*, pp.1871-1875, 2006.

[8] A. Winter, A. Nascimento, H. Imai, "Commitment Capacity of Discrete Memoryless Channels", *Cryptography and Coding 2003*, LNCS 2898, pp.35-51, Springer 2003.