# Oblivious Transfer Is Symmetric

**Abstract**

We show that oblivious transfer of bits from $A$ to $B$ can be obtained from a single instance of the same primitive from $B$ to $A$. Our reduction is perfect and shows that oblivious transfer is in fact a symmetric functionality. This solves an open problem posed by Crépeau and Sántha in 1991.

## 1 Introduction and Motivation

### 1.1 Oblivious Transfer

Modern cryptography is an increasingly broad discipline and deals with many subjects besides the classical tasks of encryption or authentication. An example is *multi-party computation*, where two or more parties, mutually distrusting each other, want to coöperate in a secure way in order to achieve a common goal, for instance, to carry out an electronic election. Examples of specific multi-party computations are *secure function evaluation*—every party holds an input to a function, and the output should be computed in a way such that no party has to reveal unnecessary information about her input—or *broadcast*, i.e., *Byzantine agreement* [14].

A primitive of particular importance in the context of two- and multi-party computation is *oblivious transfer*. In classical *Rabin oblivious transfer* [18] or *Rabin OT* for short, one of the parties—*the sender*—sends a bit $b$ which reaches *the receiver* with probability 1/2; the sender hereby remains ignorant of about whether the message has arrived or not. In other words, Rabin OT is nothing else than a binary erasure channel.

Another variant of oblivious transfer is *chosen one-out-of-two oblivious transfer*—$\binom{2}{1}-$OT for short—, where the sender sends two bits $b_0$ and $b_1$ and the receiver's input is a choice bit $c$; the latter than learns $b_c$ but gets no information about the other bit $b_{1-c}$. As a black box, $\binom{2}{1}-$OT is represented in Figure 1.

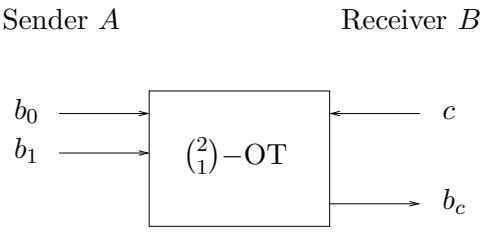



Figure 1: Chosen one-out-of-two oblivious transfer.

When the bits $b_0$ and $b_1$ in Figure 1 are replaced by $l$-bit strings $s_0$ and $s_1$, respectively, the resulting primitive is called *chosen one-out-of-two $l$-bit string oblivious transfer* or $\binom{2}{1}-\mathrm{OT}^l$ for short. (Note, however, that this notation is somewhat misleading since $\binom{2}{1}-\mathrm{OT}^l$ does *not* reduce in a trivial way to $l$ realizations of $\binom{2}{1}-$OT; but it *is* true that string OT *can* be reduced to bit OT in principle.)

Finally, (bit or string) oblivious transfer can be generalized to a primitive where the sender sends $n$ messages, $k$ of which the receiver can choose to read: *chosen $k$-out-of-$n$ oblivious transfer* or $\binom{n}{k}-\mathrm{OT}^l$ (see Figure 2).

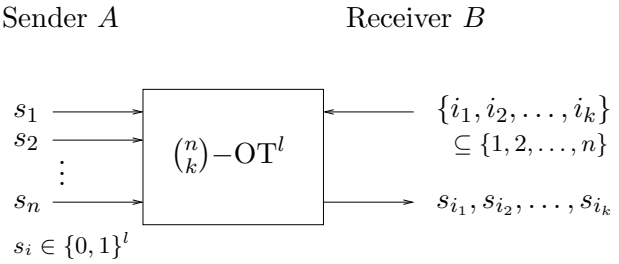



Figure 2: Chosen $k$-out-of-$n$ oblivious transfer.

The described variants of oblivious transfer have been shown equivalent to different extents. For instance, $\binom{2}{1}-\mathrm{OT}$ can be reduced to $m$ realizations of Rabin OT as long as a failure probability of $2^{-m}$ can be accepted [3]. (Here, *failure* means that either the sender obtains information about the receiver's choice, or that the receiver ends up with more information than just the bit of his choice—for instance, the XOR of the two bits.)

On the other hand, oblivious transfer of ($l$-bit) *strings* can be reduced to $\Theta(l)$ realizations of *bit* oblivious transfer—with or without failure probability, where the reduction can be made more efficient in terms of the hidden constant if a small probability of failure is tolerated [2]. In [2], it was also shown that $\binom{2}{1}-\mathrm{OT}^l$ can be reduced to a primitive offering only very weak protection of the sender, called *universal oblivious transfer* or *UOT*: Here, the receiver can choose to receive any kind and amount of information about the pair $(b_0, b_1)$ of bits sent under the sole condition that this information is incomplete.

$\binom{2}{1}-\mathrm{OT}$ from $A$ to $B$ was shown reducible to $\Theta(s)$ instances of *bit oblivious transfer from $B$ to $A$*—$\binom{2}{1}-\mathrm{TO}$ for short—, where a failure can occur with probability $2^{-s}$.

Finally, $\binom{n}{k}-\mathrm{OT}^l$ can be perfectly reduced to $\binom{2}{1}-\mathrm{OT}$; in fact, one reason for the importance of oblivious transfer is its *universality*, i.e., that it allows, in principle, for carrying out *any* two-party computation [13].

## 1.2 Unconditional Oblivious Transfer from Weak Primitives

Besides *computational* cryptographic security—based on the assumed hardness of certain computational problems and a limitation on the adversary's computing power—there also exists *unconditional* security—based on the fact that the *information* the potential adversary obtains is limited. This latter type of security, therefore, withstands attacks even by a computationally unlimited adversary, and it is, *a priori*, more desirable to realize cryptographic primitives—if possible—in such an unconditionally secure way.

Unfortunately, $\binom{2}{1}-\mathrm{OT}$ is impossible to achieve in an information-theoretically secure way from scratch, i.e., between parties connected by a noiseless channel—in fact, not even if this is a *quantum* channel over which the parties can exchange not only "classical" bits but quantum states [16].

The mentioned facts motivate the search for a way of realizing cryptographic primitives in an unconditionally secure way if not from scratch, so from weak and realistic primitives such as noisy channels or weakly correlated randomness. Reductions of this type have been studied by several authors, as the following table shows.

| from → ↑ | noisy channels | correlated randomness |
|---|---|---|
| confidentiality, key agreement | Wyner [24]; Csiszár, Körner [8] | Maurer [15] |
| oblivious transfer | Crépeau, Kilian [5]; Crépeau [4]; Crépeau, Morozov, Wolf [6]; Imai, Nascimento, Winter [12] | Imai, Nascimento, Winter [12]; Wolf, Wullschleger [23] |
| bit commitment | Crépeau, Kilian [5]; Crépeau [4]; Winter, Nascimento, Imai [22] | Imai, Müller-Quade, Nascimento, Winter [11]; Wolf, Wullschleger [23] |
| broadcast | Fitzi, Wolf, Wullschleger [10] | Fitzi, Wolf, Wullschleger [10] |

For instance, it was shown in [6] that any "non-trivial" noisy channel between $A$ and $B$ allows for efficiently realizing $\binom{2}{1}-\mathrm{OT}$ in an unconditionally secure way—where "trivial" channels are, roughly speaking, perfect or capacity-zero channels, or combinations thereof, from which oblivious transfer is obviously impossible to achieve.

Another group of results, which we discuss in some more detail, is concerned with realizing $\binom{2}{1}-\mathrm{OT}$ between parties $A$ and $B$ who have access to correlated pieces of information modeled by random variables $X$ and $Y$, respectively, with joint distribution $P_{XY}$ (see Figure 3).

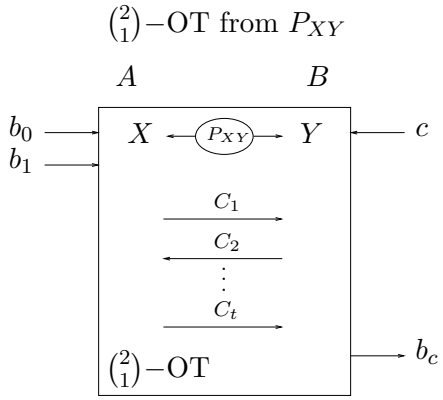



Figure 3: Oblivious transfer from correlated randomness.

In [12] and [23], a complete characterization is given of distributions $P_{XY}$ for which oblivious transfer, and also *bit commitment*, can be achieved in this scenario. In order to express this condition in a compact and intuitive way, the notions of *zero-error information* and *dependent part* have been introduced in [23] for a given distribution $P_{XY}$.

Intuitively, the *zero-error information* $I_0(X;Y)$ between two random variables $X$ and $Y$ is the entropy $H(X \wedge Y)$ of the "maximal" random variable $X \wedge Y$ that can be generated from $X$ as well as from $Y$. The quantity relates to Shannon's zero-error channel capacity [21] in exactly the same way as the "usual" mutual information to the channel capacity.

The *dependent part* $X \searrow Y$ of $X$ from $Y$, on the other hand, is the part of $X$ that is not independent from $Y$: $X \searrow Y$ is constructed from $X$ by identifying symbols $x, x' \in \mathcal{X}$ if $P_{Y|X=x} = P_{Y|X=x'}$. Roughly speaking, $I_0(X;Y)$ on one hand and $H(X \searrow Y)$ (as well as $H(Y \searrow X)$) on the other are "zero-error approximations" of the mutual information $I(X;Y)$ from below and above, respectively. When Yeung's graphical representation of the basic information-theoretic quantities [25] is extended by these new notions, then $H(XY)$ splits up into six disjoint regions as shown in Figure 4.

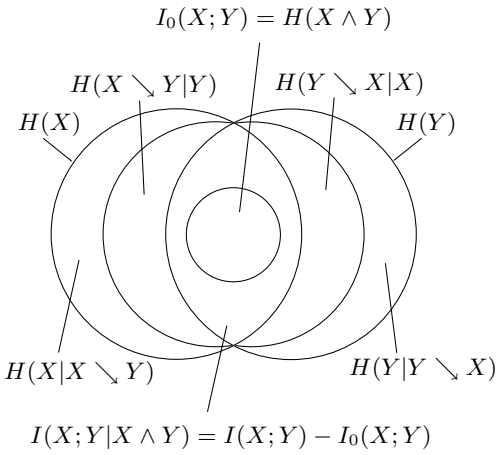



Figure 4: Zero-error information and dependent parts.

The main result of [23] is the following.

**Theorem 1. [23]** *For a probability distribution $P_{XY}$, the following conditions are equivalent.*

*(i) In the scenario where $A$ and $B$ have access to repeated realizations of $X$ and $Y$, respectively, and are connected by a noiseless channel, $\binom{2}{1}-$OT can be realized in an unconditionally secure way for both parties (with a failure probability exponentially small in the number of repetitions of the random experiment).*

*(ii) In the same scenario, bit commitment can be achieved.*

*(iii)* $I_0(X;Y) < I(X;Y)$.

*(iv)* $H(X \searrow Y \,|\, Y) > 0$.

*(v)* $H(Y \searrow X \,|\, X) > 0$.

Figure 5 shows the examples of a *local random bit* (known to $A$), a *common random bit*, and a *noisy shared bit* (which differs with probability $p > 0$).

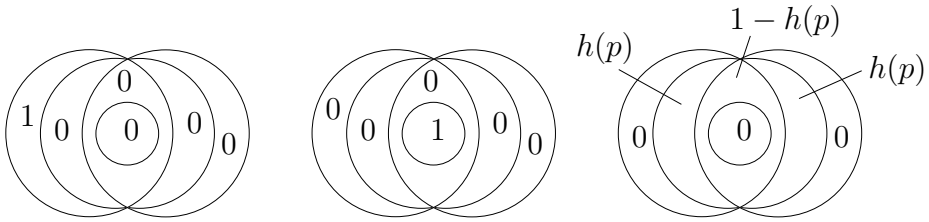



Figure 5: A local bit, a shared bit, and a noisy shared bit.

Hence, Theorem 1 implies that a sufficient number of noisy bits between $A$ and $B$ allows for unconditionally secure $\binom{2}{1}-$OT between the parties—which is not surprising given the mentioned result concerning oblivious transfer from noisy channels [4], [6].

In Section 2, we propose and discuss another particular distribution allowing for oblivious transfer. We show that in fact, *a single pair* of realizations of this random experiment is equivalent to oblivious transfer—it is, hence, fair to say that these pieces of information are an *oblivious transfer key* (just as a shared secret bit is an encryption key since it allows for perfectly encrypting a one-bit message).

## 2 How to Store Oblivious Transfer

Oblivious transfer protocols rely either on tools borrowed from public-key cryptography [18], [9] or on additional assumptions [1], [4], [19], [2], [23]. In the first case, we have to deal with relatively slow algorithms, which may be the bottleneck of the protocol execution. In the second case, one depends on these additional assumptions being present at the time of the execution of the protocol. In both cases, it is, therefore, desirable to carry out as much of the computation as possible *in advance*, and to make the actual execution of oblivious transfer as fast and simple as possible, based on this pre-computation. We will show that in fact, the *entire* computation can be done beforehand. More precisely, we present a specific probability distribution $P_{XY}^{n,k,l}$ with the property that one realization of $\binom{n}{k}-\mathrm{OT}^l$ allows for generating a sample of random variables distributed according to this distribution, and *vice versa*. A distributed pair $(X, Y)$ of realizations of these random variables is, hence, an $\binom{n}{k}-\mathrm{OT}^l$*-key* in very much the same sense as a shared secret bit is an encryption key; we will call the primitive distributing such a sample to $A$ and $B$ an *oblivious (transfer) key* or $\binom{n}{k}-\mathrm{OK}^l$ for short.

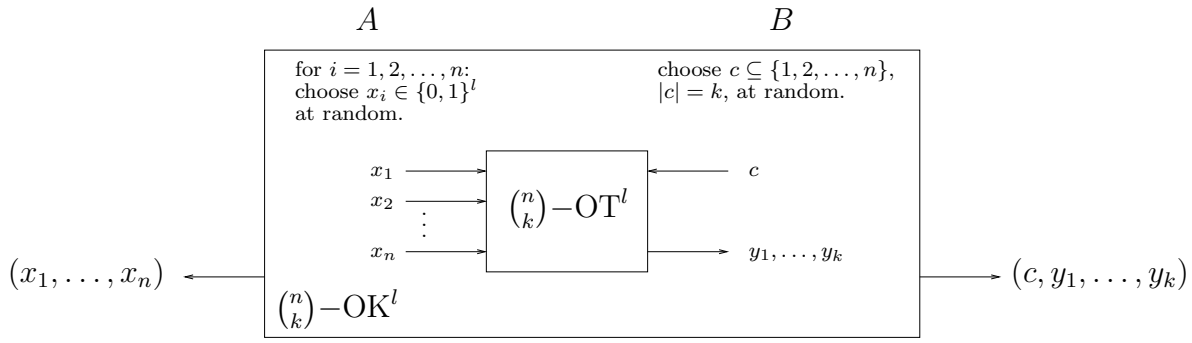
Intuitively speaking, $\binom{n}{k}-\mathrm{OK}^l$ is the distribution that arises when $A$ and $B$ choose, in $\binom{n}{k}-\mathrm{OT}^l$, their inputs at random. We give the precise definition of the distribution and show the perfect, *single-copy* reductions between $\binom{n}{k}-\mathrm{OT}^l$ and $\binom{n}{k}-\mathrm{OK}^l$.

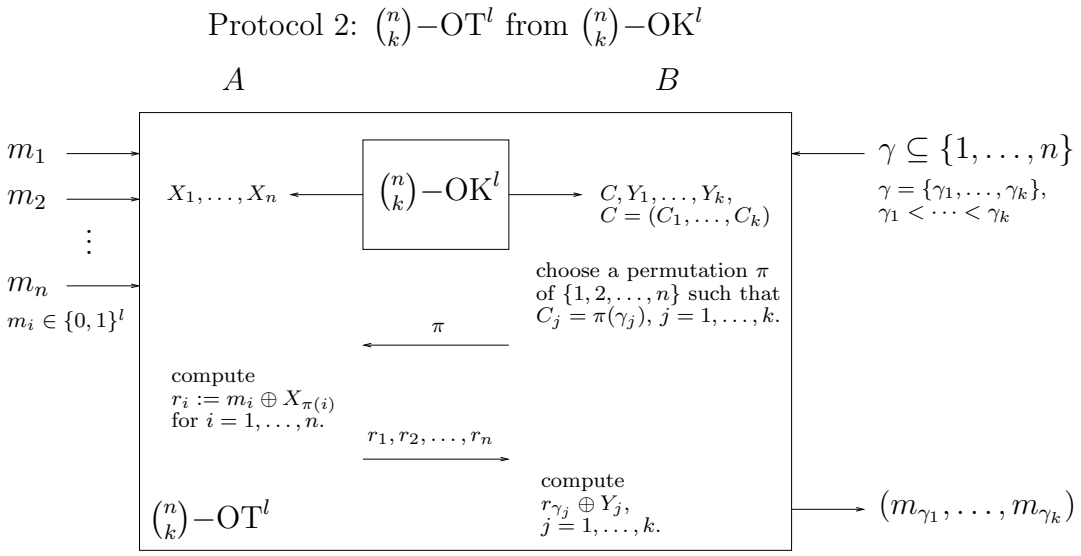
**Definition 1.** By $\binom{n}{k}-\mathrm{OK}^l$, we denote the primitive where a sample of two random variables $X$ and $Y$ is given to $A$ and $B$, respectively, where the distribution $P_{XY}$ is the one arising when the parties randomly choose their inputs in an execution of $\binom{n}{k}-\mathrm{OT}^l$. More precisely,

$$\begin{aligned} X &= (X_1, X_2, \ldots, X_n) \ , \\ Y &= (C, Y_1, Y_2, \ldots, Y_k) \ , \end{aligned}$$

where the $X_i$ are independently and uniformly distributed $l$-bit strings, $C = (C_1, C_2, \ldots, C_k)$ (where $1 \leq C_1 < C_2 < \cdots < C_k \leq n$) is a random subset of size $k$ of $\{1, 2, \ldots, n\}$, and where $Y_j = X_{C_j}$ holds for $1 \leq j \leq k$.

Protocol 1: $\binom{n}{k}-\mathrm{OK}^l$ from $\binom{n}{k}-\mathrm{OT}^l$






Protocol 2 is a straight-forward generalization of protocols proposed in [1] and [19]. It is easy to see that Protocols 1 and 2 provide *perfect single-copy* reductions between the primitives $\binom{n}{k}-\mathrm{OT}^l$ and $\binom{n}{k}-\mathrm{OK}^l$: If noiseless communication is available, the primitives are simply *equivalent*. This, together with the fact that $\binom{n}{k}-\mathrm{OK}^l$ is a *non-interactive* primitive, means that any sort of oblivious transfer can be *stored*: If an "oblivious transfer channel"—perfect or with failure probability or computationally secure—is available today, then oblivious transfer, with exactly the same security, can be carried out tomorrow. Note, hereby, that when the combination of Protocols 1 and 2 is used for delaying or storing $\binom{n}{k}-\mathrm{OT}^l$, then any active attack by one of the parties, i.e., non-random choice of the inputs in Protocol 1, can only harm the security of the misbehaving party, but not the honest party's.

## 3 How to Reverse Oblivious Transfer

We study the prominent special case of chosen one-out-of-two bit oblivious transfer $\binom{2}{1}$−OT and $\binom{2}{1}$−OK, which we will call *oblivious coin* or *OC* for short. Clearly, OC distributes a sample of a particular distribution satisfying the conditions of Theorem 1. In fact, we have $I(X;Y) - I_0(X;Y) = H(X \searrow Y \,|\, Y) = H(Y \searrow X \,|\, X) = 1$, whereas the three remaining "regions" of Figure 4 are zero. The distribution of OC is given and illustrated in Figure 6.

$$P_{XY}(x,y) = \begin{cases} 1/8 & \text{if } (x,y) \in \{((0,0),(0,0)),((0,0),(1,0)),((0,1),(0,0)),((0,1),(1,1)), \\ & \qquad ((1,0),(0,1)),((1,0),(1,0)),((1,1),(0,1)),((1,1),(1,1))\} \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

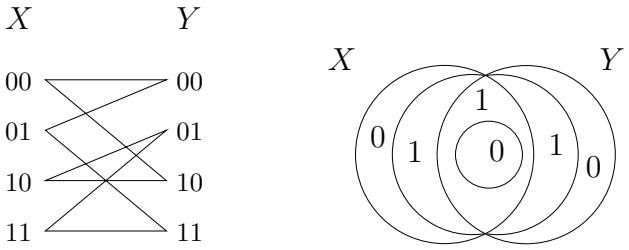



Figure 6: The distribution of an oblivious coin.

When the symbols of $X$ and $Y$ are renamed in a suitable way, the distribution corresponds to the one arising when Shannon's so-called *"noisy-typewriter channel"* [20] is used with random input (see Figure 7).

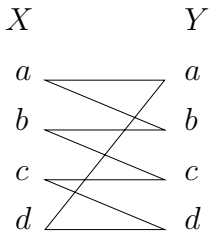



Figure 7: The distribution arising from the "noisy-typewriter channel."

Obviously, this distribution is *symmetric*. On the other hand, OC is equivalent to $\binom{2}{1}$−OT, which is, hence, symmetric as well: *A single* instance of $\binom{2}{1}$−TO allows for generating a realization of $\binom{2}{1}$−OT. The reduction is not only single-copy, but also *information-theoretically perfect*. This solves an open problem posed in [7] in an unexpectedly simple way.

**Theorem 2.** *One realization of* $\binom{2}{1}$−OT *can be perfectly reduced to a single instance of* $\binom{2}{1}$−TO.

Note that, as in the protocol for storing oblivious transfer, any active cheating in the protocol for reversing oblivious transfer can only harm the security of the misbehaving party, but not the honest party's security.

The reduction of $\binom{2}{1}$−OT to $\binom{2}{1}$−TO is of the strongest possible kind: *Any* protocol for $\binom{2}{1}$−OT—offering either computational or information-theoretic security for $A$ and $B$, respectively—can be transformed into a protocol for oblivious transfer from $B$ to $A$ having exactly the same security both for $A$ and $B$ as the original protocol; no additional failure can occur.

Another consequence of Theorem 2 is that the "security levels" in any $\binom{2}{1}$−OT protocol can be switched immediately: For instance, a protocol, based on RSA, say, the security offered by which is unconditional for the receiver but only computational for the sender can be transformed into an equally efficient and equally simple protocol that is unconditional for the sender and computational for the receiver.

**Lemma 3.** *Let $B_0$, $B_1$, $C$, and $Y$ be binary random variables. Then*

$$((B_0, B_1), (C, Y))$$

*is an OC if and only if*

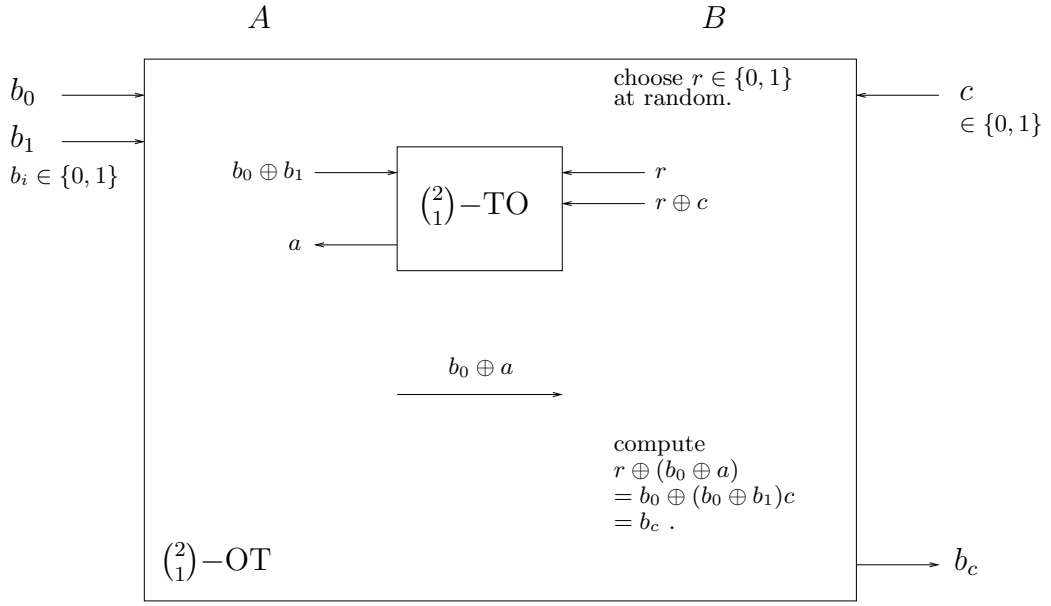
$$((\overline{B_0}, \overline{B_1}), (\overline{C}, \overline{Y})) := ((Y, C \oplus Y), (B_0 \oplus B_1, B_0))$$

*is an OC.*

*Proof.* We have $\overline{B_{\overline{C}}} = \overline{B_0} \oplus (\overline{B_0} \oplus \overline{B_1})\overline{C} = Y \oplus C(B_0 \oplus B_1) = B_C \oplus C(B_0 \oplus B_1) = B_0 = \overline{Y}$. □

One possibility of reducing $\binom{2}{1}$−OT to $\binom{2}{1}$−TO is via the generation of a sample of the—symmetric—distribution of OC. This protocol requires *three* bits of additional communication. Protocol 3 is even simpler, using only *one* bit of additional communication from $A$ to $B$. (Note that this is optimal since $\binom{2}{1}$−OT *does* allow for a bit of communication from $A$ to $B$.)

Protocol 3: $\binom{2}{1}$−OT from $\binom{2}{1}$−TO




It is obvious that $A$ cannot cheat in Protocol 3: Anything she could do just corresponds to correct behavior with respect to another pair of input bits. Bob, on the other hand, can try to cheat by not choosing $r$ randomly. This, however, only harms his own privacy.

# 4 Oblivious Linear-Function Evaluation

In contrast to OC, i.e., bit oblivious transfer, the oblivious key corresponding to *string* oblivious transfer is *not* symmetric. (However, string oblivious transfer into one direction can in principle be reduced to the same primitive into the other [2], but not in the perfect single-copy sense of Section 3.) In this section, we present another natural generalization of oblivious transfer to strings that *is* symmetric: *oblivious linear-function evaluation* or *OLFE* for short. Roughly speaking, the sender's input is a linear function, the receiver's input is an argument for which he then learns the evaluation of the function (see Figure 8). OLFE is a special case of oblivious polynomial evaluation [17].

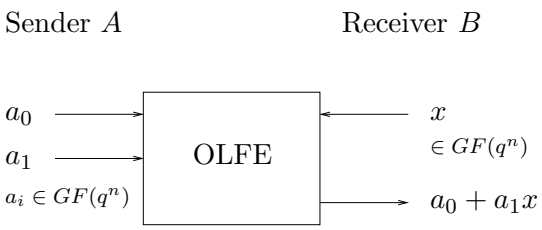
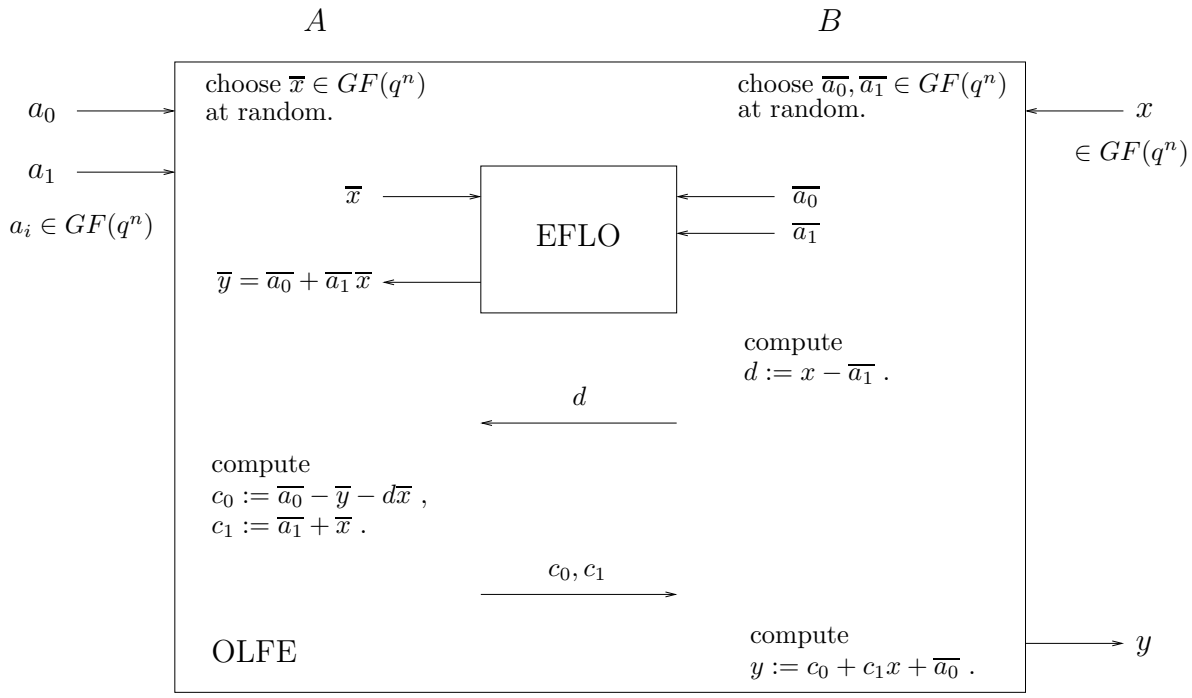



Figure 8: Oblivious linear-function evaluation.

OLFE is, as (string) oblivious transfer, equivalent to a non-interactive "OLFE key"—and can, therefore, be stored in the same sense. Moreover, this key is, as OC in the case of *bit* oblivious transfer, symmetric. Hence, OLFE from $A$ to $B$ can be reduced to OLFE from $B$ to $A$—*EFLO* for short—in a perfect and single-copy sense.

Protocol 4: OLFE from EFLO



**Lemma 4.** *Protocol 4 reduces OLFE to EFLO.*

*Proof.* We have $y = c_0 + c_1 x + \overline{a_0} = a_0 - \overline{a_0} - \overline{a_1}\,\overline{x} - (x - \overline{a_1})\overline{x} + (a_1 + \overline{x})x + \overline{a_0} = a_0 + a_1 x$. □

# 5 Concluding Remarks

The results of this paper are three-fold. First, we have shown that any variant of oblivious transfer is equivalent to a—non-interactive—primitive that distributes certain pieces of information to the two parties. This implies that (any kind of) oblivious transfer can be pre-computed and stored.

Secondly, we have shown that in the important special case of chosen one-out-of-two bit oblivious transfer, the distribution of these pieces of information is symmetric. Hence, bit oblivious transfer is: its orientation can be changed for free.

Thirdly, we have described an $n$-bit generalization of bit oblivious transfer—different from string oblivious transfer—that is symmetric as well: oblivious linear-function evaluation.

# References


[1] C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska, Practical quantum oblivious transfer, *Advances in Cryptology—Proceedings of EUROCRYPT '91*, LNCS, Vol. 576, pp. 351–366, Springer-Verlag, 1992.

[2] G. Brassard, C. Crépeau, and S. Wolf, Oblivious transfers and privacy amplification, *Journal of Cryptology*, Vol. 16, No. 4, pp. 219–237, 2003.

[3] C. Crépeau, *Correct and private reductions among oblivious transfers*, Ph. D. Thesis, Massachusetts Institute of Technology, 1990.

[4] C. Crépeau, Efficient cryptographic protocols based on noisy channels, *Advances in Cryptology—Proceedings of CRYPTO '97*, LNCS, Vol. 1233, pp. 306–317, Springer-Verlag, 1997.

[5] C. Crépeau and J. Kilian, Achieving oblivious transfer using weakened security assumptions, *Proceedings of the* $28^{th}$ *Symposium on Foundations of Computer Science (FOCS '88)*, pp. 42–52, IEEE, 1988.

[6] C. Crépeau, K. Morozov, and S. Wolf, Efficient unconditional oblivious transfer from almost any noisy channel, *Proceedings of Fourth Conference on Security in Communication Networks (SCN) '04*, LNCS, Springer-Verlag, 2004.

[7] C. Crépeau and M. Sántha, On the reversibility of oblivious transfer, *Advances in Cryptology—Proceedings of EUROCRYPT '91*, LNCS, Vol. 547, pp. 106–113, Springer-Verlag, 1991.

[8] I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. 24, pp. 339–348, 1978.

[9] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, *Communications of the ACM*, Vol. 28, No. 6, pp. 637–647, 1985.

[10] M. Fitzi, S. Wolf, and J. Wullschleger, Pseudo-signatures, broadcast, and multi-party computation from correlated randomness, *Advances in Cryptology—Proceedings of CRYPTO '04*, LNCS, Vol. 3152, Springer-Verlag, 2004.

[11] H. Imai, J. Müller-Quade, A. Nascimento, and A. Winter, Rates for bit commitment and coin tossing from noisy correlation, *Proceedings of the IEEE International Symposium on Information Theory (ISIT) '04*, IEEE, 2004.

[12] H. Imai, A. Nascimento, and A. Winter, *Oblivious transfer from any genuine noise*, unpublished manuscript, 2004.

[13] J. Kilian, Founding cryptography on oblivious transfer, *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88)*, pp. 20–31, 1988.

[14] L. Lamport, R. Shostak, and M. Pease, The Byzantine generals problem, *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, pp. 382–401, 1982.

[15] U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[16] D. Mayers, Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.*, Vol. 78, pp. 3414–3417, 1997.

[17] M. Naor and B. Pinkas. Oblivious transfer and polynomial evaluation, *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing (STOC '99)*, pp. 245-354, 1999.

[18] M. Rabin, *How to exchange secrets by oblivious transfer*, Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[19] R. L. Rivest, *Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer*, unpublished manuscript, 1999.

[20] C. E. Shannon, A mathematical theory of communication, *Bell System Technical Journal*, Vol. 27, pp. 379–423, 623–656, 1948.

[21] C. E. Shannon, The zero-error capacity of a noisy channel, *IEEE Transactions on Information Theory*, Vol. 2, pp. 8–19, 1956.

[22] A. Winter, A. Nascimento, and H. Imai, Commitment capacity of discrete memoryless channels, *Cryptography and Coding*, LNCS, Vol. 2898, pp. 35–51, Springer-Verlag, 2003.

[23] S. Wolf and J. Wullschleger, Zero-error information and applications in cryptography, *Information Theory Workshop (ITW) 2004*, IEEE, 2004.

[24] A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.

[25] R. W. Yeung, A new outlook on Shannon's information measures, *IEEE Transactions on Information Theory*, Vol. 37, No. 3, pp. 466–474, 1991.