Reducing Oblivious String Transfer to Universal Oblivious Transfer

Stefan Wolf [1]

Abstract — **It is shown that oblivious transfer of strings can be reduced to the weakest version of oblivious bit transfer, where the receiver can choose to obtain arbitrary (but incomplete) information about the pair of bits sent. This solves an open problem posed by Brassard and Crépeau.**

I. Equivalence Between Oblivious Transfers

Important cryptographic primitives, such as secure message transmission, key agreement, or secure multi-party computation, can often be reduced to apparently much weaker primitives such as noisy communication channels or correlated randomness. In this note we present an information-theoretic reduction of so-called *1-out-of-2 oblivious string transfer* to a weak variant of oblivious bit transfer, called *universal oblivious transfer*. Oblivious-transfer primitives are of central importance for many cryptographic protocols. In principle, oblivious transfer allows for carrying out any secure two-party computation.

The standard *oblivious bit transfer* (bit OT) between two parties corresponds to a binary erasure channel with erasure probability $1/2$: The sender's input is a bit b, which the receiver learns with probability $1/2$, whereas otherwise, he obtains no information about b. The sender on the other hand does not learn whether the bit has been received or not.

In *1-out-of-2 bit OT* ($\binom{2}{1}$-OT for short) the sender sends two one-bit messages, exactly one of which the receiver can choose to read, remaining completely ignorant about the other one, such that the sender does not get any information about which message has been chosen. In *1-out-of-2 k-bit-string OT* ($\binom{2}{1}$-OT^k) the messages are k-bit strings instead of single bits.

The problem of reducing *string* OT to *bit* OT was studied by many authors (see [1] and the references therein). In [1], a reduction was presented based on so-called *privacy amplification* by hashing with linear functions. It was even shown that *$\binom{2}{1}$-OT^k with security s*, i.e., such that with probability at least $1-2^{-s}$, the receiver obtains no information at all about one of the transmitted strings, even when given the other, can be reduced to $n = O(k+s)$ realizations of *generalized OT (GOT)*, where the receiver can choose to learn any one-bit function (such as b_0, $b_0 \oplus b_1$, or $b_0 \wedge b_1$) about the two bits b_0 and b_1 sent. Protocol BC, which achieves this, works as follows. First, GOT is applied n times with random input bits (x_i, y_i). Then, the two k-bit messages m_0 and m_1 to be sent by $\binom{2}{1}$-OT^k are blinded by (i.e., xor-ed with) two k-bit strings $h_0(x_1, \ldots, x_n)$ and $h_1(y_1, \ldots, y_n)$, respectively, where h_0 and h_1 are two linear functions from n-bit to k-bit strings, chosen randomly and published by the sender.

It was stated as an open problem in [1] how this result generalizes to a primitive offering the receiver the possibility to obtain *arbitrary* (probabilistic) information about the pair (b_0, b_1). We show that the most optimistic answer is the correct one: Whenever the information the receiver obtains in such *universal OT (UOT)* does not completely determine (b_0, b_1), then string OT can be reduced to this primitive. The argument is based on the fact that among all types of an adversary's side information about a single bit with given error probability, there exists a "strictly worst case," namely information obtained from a symmetric erasure channel. This also allows for simplifying the proofs given in [1] and for improving the results with respect to the involved constants. Related results in models different from the one of [1] were shown in [2].

[1] Department of Computer Science, ETH Zürich, CH–8092 Zürich, Switzerland. E-mail: `wolf@inf.ethz.ch`

II. The Power of Universal OT

Definition 1. Let $\alpha > 0$. In *universal OT with parameter* α (α-UOT), the sender's input is a pair of bits (b_0, b_1). The receiver specifies a possibly probabilistic function Ω which must satisfy $H((b_0, b_1) \,|\, \Omega(b_0, b_1)) \geq \alpha$ if (b_0, b_1) is uniformly distributed. Then the receiver obtains $\Omega(b_0, b_1)$, but no additional information about (b_0, b_1). The sender on the other hand does not learn anything about Ω.

Theorem 1. *Protocol BC reduces $\binom{2}{1}$-OT^k with security s to at most $\lceil (s+2k)\ln 2/p_e \rceil$ realizations of α-UOT, where p_e is the unique solution ($\leq 1/2$) to the equation $h(2x) + 2x \log 3 = \alpha$.*

Lemma 2. *Let B be a symmetric binary random variable, and let U be a random variable such that B and U have joint distribution P_{BU}. Let p be the average error probability of guessing B when given U, using the optimal guessing strategy. Then there exists a random variable V with the following properties. First, $\mathcal{V} = \{0, 1, \Delta\}$ and $P_V(\Delta) = 2p$ hold, and for every $u \in \mathcal{U}$, we have $P_{B|U=u,V=\Delta}(0) = P_{B|U=u,V=\Delta}(1)$.*

Proof. Let $u \in \mathcal{U}$, and assume that $a = P_{B|U=u}(0) > P_{B|U=u}(1) = b$. Let V be defined by $P_{V|B=0,U=u}(0) = (a-b)/a$, $P_{V|B=0,U=u}(\Delta) = b/a$, and $P_{V|B=1,U=u}(\Delta) = 1$. Note that $P_{V|U=u}(\Delta) = 2b$, i.e., twice the error probability for guessing B when given $U = u$. □

The idea of the proof of Theorem 1 is as follows. By Fano's inequality, one can conclude that, when the pair (x_i, y_i) is sent by α-UOT, about at least two of the bits x_i, y_i, and $x_i \oplus y_i$, the receiver's error probability when guessing the bit with the optimal strategy is at least p_e. Because of Lemma 2, we can assume that with probability at least $2p_e$, the receiver has no information at all about such a bit. By construction, this implies that with overwhelming probability, the receiver cannot bias $g(h_0(x_1, \ldots, x_n), h_1(y_1, \ldots, y_n))$ for any linear function g with range $\{0, 1\}$ and depending non-trivially on both inputs. In this case, he has no information at all about one of the inputs, even when given the other.

References

[1] G. Brassard and C. Crépeau, "Oblivious transfers and privacy amplification," *Advances in Cryptography – EUROCRYPT' 97*, LNCS, Vol. 1233, pp. 334–345, Springer-Verlag, 1997.

[2] C. Cachin, "On the foundations of oblivious transfer," *Advances in Cryptography – EUROCRYPT' 98*, LNCS, Vol. 1403, pp. 361–374, Springer-Verlag, 1998.