Efficient Oblivious Transfer From Any Non-Trivial Binary-Symmetric Channel

Douglas Stebila [1]

Stefan Wolf [2]

Abstract — **In 1997, Crépeau proved that the important cryptographic primitive of *oblivious transfer* can be efficiently realized by using a binary-symmetric channel with symbol-error probability less than 0.1982. We show that this restriction is unnecessary: Oblivious transfer can be realized as efficiently based on any non-trivial binary-symmetric channel between the involved parties.**

I. Cryptographic Primitives from Noisy Channels

Information-theoretic (or unconditional) security is the highest possible level of security in cryptography and withstands, in contrast to computational security, even attacks by a computationally unlimited adversary and is, in addition to this, not based on any unproven complexity-theoretic assumption. Unconditionally secure systems are, unlike computationally secure protocols, often impossible to realize from scratch, i.e., without any "information-theoretic primitive" to start from. This pessimism, however, is relativized by the fact that these starting points can be as simple as a noisy communication channel.

Wyner was the first to point out the cryptographic power of such channels in the context of confidentiality. It is a natural question whether other goals, such as secure two- or multi-party computations, can also be achieved from primitives as simple as that. In this context, so-called (chosen 1-out-of-2 bit) *oblivious transfer (OT)*, which allows a sender to transmit two bits, one of which can be chosen to be read by the receiver, leaving the sender ignorant about the receiver's choice, is crucial since it has been shown a universal two-party computation in the sense that any other can be reduced to it.

Crépeau and Kilian [3] showed that information-theoretically secure OT can be realized with a non-trivial binary-symmetric channel (BSC) by $\Omega((\log(1/\alpha))^{11})$ channel uses, where α is the failure probability of the protocol that has to be tolerated. Another example is given by Brassard *et. al.* [1], where OT is reduced to an arbitrarily weak variant of it, called *universal OT*: Here the receiver can choose to receive almost complete information about *both* message bits sent by the sender.

[1]Department of Combinatorics & Optimization, University of Waterloo, Waterloo, ON, Canada N2L 3G1. Email: dstebila@student.math.uwaterloo.ca. Supported by Canada's NSERC. Work carried out during an Undergraduate Research Assistantship in the Centre for Applied Cryptographic Research of the Department of Combinatorics & Optimization at the University of Waterloo.

[2]Département d'Informatique et R.O., Université de Montréal, Montréal, QC, Canada H3C 3J7. Email: wolf@iro.umontreal.ca. Supported by Canada's NSERC.

II. Efficient Oblivious Transfer from ANY Binary-Symmetric Channel

In [2], Crépeau presents a simpler and more efficient protocol than the one of [3] for realizing OT from a BSC that works, however, only if the BSC's error probability is less than 0.1982. It has been stated as an open problem in [2] whether this condition is necessary for the existence of a reduction with this efficiency, namely $O((\log(1/\alpha))^3)$ channel uses. In fact, this condition is unnecessary: OT can be realized, with the same asymptotic efficiency, from *any* non-trivial BSC.

Theorem 1 *Chosen 1-out-of-2 bit OT can be information-theoretically reduced to a BSC with bit-error probability φ, $0 < \varphi < 1/2$. The number of channel uses is $O(2^{(1/2-\varphi)^{-2}}(\log(1/\alpha))^3)$ if α is the failure probability of the reduction protocol.*

The new protocol is a generalization of Crépeau's three-stage construction of OT from a BSC. In the first stage, a standard OT (where only one bit is sent and reaches the receiver with some probability but is lost otherwise) is obtained by sending the corresponding bit over the BSC twice. Since this does not exclude that the bit is received incorrectly, error correction has to be done. The resulting "weak OT," however, does not yet protect against a cheating sender. It has to be repeated, and honesty metrics are used to detect cheating. Our protocol preserves this three-stage approach, but increases the number of times the bit is sent in the first stage. The analysis shows that the other stages can be modified and the honesty metrics redefined to achieve OT from any BSC. The complete protocol and the proof of Theorem 1 can be found in the full paper [4].

It is an interesting open question in this context which discrete noisy channels (not necessarily binary) between two parties can in principle be used to realize OT.

Acknowledgments

We thank Claude Crépeau, Serge Fehr, and Ueli Maurer for interesting discussions on the subject of this paper.

References

[1] G. Brassard, C. Crépeau, and S. Wolf, Oblivious transfers and privacy amplification, to appear in *Journal of Cryptology*, 2002.

[2] C. Crépeau, Efficient cryptographic protocols based on noisy channels, in *Proceedings of EUROCRYPT '97*, LNCS, Springer-Verlag, pp. 306–317, 1997.

[3] C. Crépeau and J. Kilian, Achieving oblivious transfer using weakened security assumptions, in *Proceedings of FOCS '88*, pp. 42–52, 1988.

[4] D. Stebila and S. Wolf, Efficient oblivious transfer from any binary-symmetric channel, in preparation, 2002.