Weakening Security Assumptions and Oblivious Transfer

(Abstract)

Claude Crépeau*
Department of Computer Science
MIT

Joe Kilian†
Mathematics Department
MIT

1 Introduction

Our work is motivated by a recent trend in cryptographic research. Protocol problems that have previously been solved subject to intractability assumptions are now being solved without these assumptions. Examples of this trend include a new completeness theorem for multiparty protocols[BGW,CCD], and a protocol for byzantine agreement using private channels[FM]. These breakthroughs illustrate both the strengths and the weaknesses of using the cryptographic model. Devising first a protocol that uses cryptographic assumptions can give powerful intuition that later allows one to create a protocol that works without assumptions. However, there is a danger that the cryptographic assumptions one uses can become inextricably bound up in the protocol. It may take years before these assumptions can be ironed out of the final protocol.

One way to keep a firm grasp on ones cryptographic assumptions is to compartmentalize them into a small set of relatively simple primitives. One then attempts to build protocols on top of these primitives, without using any cryptographic assumptions in the high level design. The problem of eliminating cryptographic assumptions from the protocol is then reduced to that of implementing the primitives without cryptography.

In this abstract, we explore a particularly useful set of primitives, known as *oblivious transfers*. First introduced by Rabin, oblivious transfer protocols are games in which one player, Sam(the sender), can impart some information to another player, Rachel(the receiver), without knowing precisely what information he has imparted.

*Supported in part by an NSERC Postgraduate Scholarship. Some of this research was performed while visiting Bell Communication Research.

†Research supported in part by a Fannie and John Hertz foundation fellowship, and NSF grant 865727-DCR. Some of this research was performed while visiting Bell Communication Research.

Oblivious transfers come in a wide variety of flavors, and are not obviously reducible to each other. Following the work of Brassard, Crépeau, Robert[BCR], and Crépeau[C], we develop techniques for establishing equivalences between a wide variety of oblivious transfers.

We also investigate the properties of an ordinary noisy channel. By a noisy channel, we mean a communication line in which a transmitted bit is flipped with a certain fixed probability. This model has been extensively studied in coding theory, but relatively little was previously known about its cryptographic capabilities. We show that a noisy channel can be used to implement two-party cryptographic protocol without any intractability assumptions. In the forthcoming [CK] we also study a transfer mechanism we refer to as quantum transfer. This mechanism abstractly models a transfer mechanism based on quantum mechanics.

Weaker variants of two of the more standard forms of oblivious transfer are also studied. We investigate scenarios in which the security properties guarenteed by these mechanisms may be almost completely violated. We show that in many of these scenarios, it is still possible to achieve the full power of ordinary oblivious transfer.

The purpose of this abstract is to introduce the reader to the terminology and the statement of our results. To get the actual reductions and more detail on the application of the techniques described in this abstract, the reader should consult [CK].

Main Results.

Our results may be summarized as follows. Before reading these theorems, we refer the reader to Section 2 of the paper, which provides the necessary terminology.

Theorem 1: α-1-2 slightly oblivious transfer is as powerful as 1-2 oblivious transfer.

Theorem 2: Noisy transfer is as powerful as 1-2 oblivious transfer.

Theorem 3: α-slightly oblivious transfer is as powerful as 1-2 oblivious transfer.

2 Definitions.

In this section, we describe the various forms of information transfer mechanisms we will be considering. We define the two standard mechanisms, two weakened versions of the standard forms of oblivious transfer, and our nonstandard transfer mechanism.

2.1 Standard forms of oblivious transfer.

There are two standard forms of oblivious transfer. We refer to these mechanisms as *oblivious transfer* and *1-2 oblivious transfer*.

Oblivious Transfer: In this protocol, Sam has a secret bit, b. At the end of the protocol, one of the following two events occurs, each with probability $\frac{1}{2}$.

1. Rachel learns the value of b.
2. Rachel gains no further information about the value of b (other than what Rachel knew before the protocol).

At the end of the protocol, Rachel knows which of these two events actually occurred, and Sam learns nothing.

Less formally, we can view this protocol as one in which Sam sends a letter to Rachel, which arrives exactly half the time.

1-2 Oblivious Transfer: In this protocol, Sam has two secret bits, b_0 and b_1. Rachel has a selection bit, s. At the end of the protocol, the following three conditions hold.

1. Rachel learns the value of b_s.
2. Rachel gains no further information about the value of b_{1-s}.
3. Sam learns nothing about the value of s.

Less formally, Sam has two secrets. Rachel can select exactly one of them, and Sam doesn't know which secret Rachel selected.

Dirtier Notions of Oblivious Transfer.

In describing oblivious transfers, we make two distinct specifications. First, we specify what information is being transferred. Second, we impose a set of security conditions, specifying what information each party is guaranteed *not* to know at the end of the protocol, and specifying that certain events cannot be controlled by either party. The definitions of oblivious transfer and 1-2 oblivious transfer are particularly stringent in their security conditions. In oblivious transfer, Sam has no control over whether Rachel receives b. In 1-2 oblivious transfer, Sam gains no information about Rachel's selection s. We would like to be able to handle cases in which a malicious Sam can, thorough some form of cheating, violate these security conditions. This motivates the following definitions.

α-Slightly Oblivious Transfer: This protocol is the same as oblivious transfer, except that instead of Rachel learning bit b with probability $\frac{1}{2}$, she learns it with probability p. If Sam is nonmalicious, $p = \frac{1}{2}$. If Sam is malicious, he may choose any value of p he wishes, subject to $1 - \alpha \leq p \leq \alpha$.

α-1-2 Slightly Oblivious Transfer: This protocol is the same as $1 - 2$ oblivious transfer, except that at the conclusion of the protocol, a malicious Sam can guess Rachel's selection bit s with probability α.

In both these definitions, the interesting range for α is $\frac{1}{2} \leq \alpha < 1$.

2.2 Nonstandard transfer mechanism.

We now consider our nonstandard transfer mechanism, motivated by coding theory.

Noisy Transfer: In this protocol. Sam has a secret bit, b. Rachel has no information about b. At the end of the protocol, Rachel receives a bit b'. With probability 3/4, $b' = b$, otherwise $b' = \overline{b}$. Sam learns nothing.

This protocol may be thought of as simulating a noisy communication channel, in which a bit is flipped with probability 1/4. We can parameterize the above definition by replacing the 3/4 with a probability ρ. We call this *ρ-noisy transfer.* In this paper, we only consider the "standard" noisy transfer, where $\rho = 3/4$.

Note that in these definitions, there is a careful distinction made between the powers of a malicious Sam verses the powers of a nonmalicious Sam. Since a malicious Sam is always more powerful than a nonmalicious Sam, it would at first seem natural to simply assume that Sam is malicious. However, we require that the protocols we build on top of these primitives meet the following two requirements: They must work when Sam is nonmalicious, and they must maintain their security conditions when Sam is malicious. So, for example, if one is building a protocol using a 3/4-slightly oblivious transfer subprotocol, one *cannot* require Sam to send 1000 bits, having at least 600 get through to Rachel. A malicious Sam could easily do this, but a nonmalicious Sam could not.

3 Making honest reductions more robust.

In this section we sketch the ideas behind the technique for strengthening some of our reductions. Using this technique, we can write simple reductions which depend on the receiver being honest, and in a fairly routine fashion, convert them to protocols which are robust against cheating by the receiver. This technique will be crucial in our reductions from 1-2 oblivious transfer to α-oblivious transfer and noisy transfer.

3.1 The general scenario.

We consider transfer mechanisms with the *verifiable obliteration* property. By this we mean that the transfer mechanism occasionally gives the receiver a value which is uncorrelated with the bit sent, and for which the receiver knows this fact. Two examples of such mechanisms are ordinary oblivious channel and α-oblivious transfer. Our intermediate goal is to implement some form or another of 1-2 oblivious transfer. Having accomplished this, we then try to apply the techniques leading to theorem 1 to implement standard 1-2 oblivious transfer.

For the complete description of this technique, consult [CK].

4 The power of noise.

In this section we consider the cryptographic power of an ordinary noisy communication channel, i.e. one which inverts a transmitted bit with some fixed probability. We sketch the proof that this family of transfer mechanisms can be used to implement 1-2 oblivious transfer, and hence a wide variety of secure two-party protocols.

4.1 A philosophical remark.

Noisy channels have been extensively studied in the field of coding theory, and it is interesting to see how our perspective differs from the more traditional one. Coding theory adopts the viewpoint that noise is a bad thing, to be eliminated as efficiently as possible. Given a noisy channel, a coding theorist tries to simulate a pristine, noiseless communication line.

From our point of view (following Wyner [W]), an ideal communication line is a sterile, cryptographically uninteresting entity. Noise, on the other hand, breeds disorder, uncertainty, and confusion. Thus, it is the cryptographer's natural ally. The question we consider is whether this primordial uncertainty can be sculpted into the more sophisticated uncertainty found in secure two-party protocols. The result outlined in this section answers this question in the affirmative.

4.2 An outline of our reduction.

Our reduction consists of four main parts. We first show how to use a noisy transfer channel to simulate a very dirty transfer channel which has the total obliteration property. This allows us to start applying the techniques of Section 3. Using these techniques, we can show how to implement a version of 1-2 oblivious transfer similar to α-1-2 slightly oblivious transfer. We can then use the proof of Theorem 1 to get an almost pure 1-2 oblivious transfer channel. This channel may be used to simulate a pure 1-2 oblivious transfer channel.

Please consult [CK] for the details of the reduction.

5 Acknowledgments.

We would like to acknowledge Gilles Brassard, Ernie Brickell, Ivan Damgård, Cynthia Dwork, Joan Feigenbaum, Shafi Goldwasser, and Silvio Micali for their valuable comments, ideas, and encouragement.

6 References

[**BCR**] Brassard, Gilles, Claude Crépeau, and Jean-Marc Robert. "Information Theoritic Reductions Among Disclosure Problems," *Proceedings of the* 27^{th} *FOCS*, IEEE, 1986, 168–173.

[**BGW**] Ben-Or, Michael, Shafi Goldwasser, and Avi Wigderson, "Completeness Theorems for Noncryptographic Fault-tolerant Distributed Computation," *Proceedings of the* 20^{th} *STOC*, ACM, 1988.

[**C**] Crépeau Claude, "Equivalence Between Two Flavours of Oblivious Transfer", *Proceedings of Crypto 87*, 1988,Springer-Verlag.

[**CCD**] Chaum David, Claude Crépeau and Ivan Damgård, "Multiparty unconditionally secure protocols," *Proceedings of the* 20^{th} *STOC*, ACM, 1988.

[**CK**] Crépeau Claude, and Joe Kilian, "Achieving Oblivious Transfer Using Weakened Security Assumptions," to appear in *Proceedings of the* 29^{th} *FOCS*, IEEE, 1988.

[**EGL**] Even S., Goldreich O., and A. Lempel, "A Randomized Protocol for Signing Contracts," *CACM*, vol. 28, no. 6, 1985, pp. 637-647.

[**FM**] Feldman, Paul, Silvio Micali. "Byzantine Agreement from Scratch," *Proceedings of the* 20^{th} *STOC*, ACM, 1988.

[**R**] Rabin, M., "How to exchange secrets by oblivious transfer," Tech. Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[**W**] Wyner, A. D., "The Wire Tap Channel," Bell System Journal, 54, 1981, pp. 1355-1387.