bla bla bla é ű á

Equivalence Between Two Flavours of Oblivious Transfers

Claude Crépeau†

Laboratory for Computer Science
M.I.T.
545 Technology Square
Cambridge Massachusetts 02139 USA

1. INTRODUCTION

The concept of oblivious transfer (O.T.) that was introduced by Halpern and Rabin [HR] turned out to be a very useful tool in designing cryptographic protocols. The related notion of "one-out-of-two oblivious transfer" was proposed by Even, Goldreich and Lempel in [EGL] together with some applications. Some more applications of this protocol can be found in recent papers [BCR], [GMW]. So far, the two notions where believed to be closely related but not known to be equivalent. This paper presents a proof that these two notions are computationally equivalent.

Essentially, we show a protocol for "one-out-of-two oblivious transfer", based on the existence of a protocol for the oblivious transfer problem. The reduction presented does not depend on any cryptographic assumption and works independently of the implementation of O.T.. The implications of this reduction are:

-there exists a protocol for ANDOS [BCR] if and only if there exists a protocol for O.T.
-the completeness theorem of [GMW] can be based on the existence of O.T.

2. DEFINITIONS

Let us first remind the reader the flavours of O.T. we are considering. The concept of oblivious transfer (O.T.) was first introduced by Halpern and Rabin in [HR]. Essentially the O.T. is a two-party protocol such that:

---

† Supported in part by an NSERC postgraduate scholarship.

Definition 1: (O.T.)

-Alice knows one bit b.
-Bob gets bit b from Alice with probability $\frac{1}{2}$.
-Bob knows whether he got b or not.
-Alice does not know whether Bob got b or not.

The related notion is the "one-out-of-two oblivious transfer" defined by Even, Goldreich and Lempel in [EGL]. This other protocol is:

Definition 2: (one-out-of-two O.T.)

-Alice knows two bits b_0 and b_1.
-Bob gets bit b_k and not $b_{\bar{k}}$ with $Pr(k=0) = Pr(k=1) = \frac{1}{2}$
-Bob knows which of b_0 or b_1 he got.
-Alice does not know which b_k Bob got.

In both these cases, the outcome of the transfer cannot be forced or influenced by either Alice or Bob. Although the structure of these protocols is extremely similar, so far nobody had proven their equivalence. Since the fact that O.T. can be achieved from one-out-of-two O.T. is trivial, the problem essentially is to show how to achieve one-out-of-two O.T. from O.T..

3. PROTOCOL

Before going into the explanation of the protocol, let us introduce a generalization of the O.T. protocol in the following way and consider the general case instead of the specific case. We define the p-O.T. to be a protocol such that:

Definition 3: (p-O.T.)

-Alice knows one bit b.
-Bob gets bit b from Alice with probability p.
-Bob knows whether he got b or not.
-Alice does not know whether Bob got b or not.

3.1. General idea

The general idea of the protocol is to use the p-O.T. protocol many times over random bits until it is very likely that it worked roughly pn times. The trick is to choose n large enough so that the p-O.T. protocol works at least $\frac{2}{3}pn$ of the time and not more than $\frac{4}{3}pn$ of the time. Then to get a bit, two disjoint subsets of size $\frac{2}{3}pn$ will be used, one of which will contain only indices of some p-O.T. that worked and the other will necessarily contain some indices of p-O.T. that did not work. Then the bits of each subset will be XORed together with one of the two bits to be disclosed.

3.2. Details of the protocol

Assume Alice owns b_0, b_1 two secret bits. To disclose one of them to Bob without knowing which one Bob gets, they can do the following for $p \leq \frac{3}{4}$:

Protocol for one-out-of-two O.T.

Alice and Bob agree on a security parameter s.
Alice chooses at random Ks bits $r_1, r_2, \cdots, r_{Ks}$ for some constant K to be later determined.
For each of these Ks bits Alice uses the p-O.T. protocol to disclose the bit r_i to Bob with probability p.
Bob selects $U=\{i_1, i_2, \cdots, i_{\alpha_s}\}$ and $V=\{i_{\alpha_s+1}, i_{\alpha_s+2}, \cdots, i_{2\alpha_s}\}$ where $\alpha_s = \left\lceil \frac{2Kps}{3} \right\rceil$ with $U \cap V = \phi$ and such that he knows r_{i_j} for each $i_j \in U$.
Bob sends $(X,Y)=(U,V)$ or $(X,Y)=(V,U)$ to Alice at random.
Alice computes $m_0 = \bigoplus_{x \in X} r_x$ and $m_1 = \bigoplus_{y \in Y} r_y$.
Alice returns to Bob k, $b_k \oplus m_0$ and $b_{\bar{k}} \oplus m_1$ for a random bit k.
Bob computes $\bigoplus_{u \in U} r_u \in \{m_0, m_1\}$ and uses it to get his secret bit.

If we have $p > \frac{3}{4}$ then they use the protocol for $p = \frac{3}{4}$ with a different value of K as suggested below.

4. ANALYSIS

We claim the following result about this protocol:

Theorem:
For an appropriately chosen constant K,

$$Pr(\text{Bob gets at least one of } b_0, b_1) \geq 1-2^{-s} \text{ and } Pr(\text{Bob gets more than one of } b_0, b_1) \leq 2^{-s}.$$

Proof:
Assume first that $p \leq \frac{3}{4}$. Name x_i the random variable such that

$$x_i = \begin{cases} 0 & \text{if Bob did not get } r_i \\ 1 & \text{if Bob did get } r_i \end{cases}$$

First notice that by definition $Pr(x_i=1) = 1-Pr(x_i=0) = p$. Consider the random variable

$X_i = \sum_{j=1}^{i} x_j$. Since the x_i's are independent random variables, then X_i is distributed with a binomial distribution. According to Bernshtein's Law of Large Numbers [Kr]

$$Pr\left(\left| \frac{X_i}{i} - p \right| \geq \varepsilon \right) \leq 2e^{-i\varepsilon^2}$$

for every ε such that $0 < \varepsilon \leq p(1-p)$. In particular if we set $i = Ks$ and $\varepsilon = \frac{p}{4}$ we get

$$0 < \varepsilon \leq p(1-p)$$

because $p \leq \frac{3}{4}$ and also we get

$$Pr\left(\left| \frac{X_{Ks}}{Ks} - p \right| \geq \frac{p}{4} \right) \leq 2e^{-\frac{Ksp^2}{16}} \leq 2^{-s}$$

for $K \geq \frac{12}{p^2}$. However, what we really are interrested in is

Pr(Bob gets at least one of b_0, b_1) and Pr(Bob gets more than one of b_0, b_1)

But we have that

$$\begin{aligned}
&Pr(\text{Bob gets at least one of } b_0, b_1)\\
&= 1 - Pr(\text{Bob gets none of } b_0, b_1)\\
&= 1 - Pr\left(X_{Ks} < \left\lceil \frac{2Kps}{3} \right\rceil\right)\\
&= 1 - Pr\left(p - \frac{X_{Ks}}{Ks} > \frac{p}{3} + \frac{\frac{2Kps}{3} - \left\lceil \frac{2Kps}{3} \right\rceil}{Ks}\right)\\
&\geq 1 - Pr\left(p - \frac{X_{Ks}}{Ks} > \frac{p}{3} - \frac{1}{Ks}\right)
\end{aligned}$$

Since $s \geq 1, K \geq \frac{12}{p^2}$ and $p^2 \leq p$ we get,

$$\begin{aligned}
&\geq 1 - Pr\left(p - \frac{X_{Ks}}{Ks} > \frac{p}{3} - \frac{p}{12}\right)\\
&\geq 1 - Pr\left(p - \frac{X_{Ks}}{Ks} > \frac{p}{4}\right)\\
&\geq 1 - Pr\left(\left| \frac{X_{Ks}}{Ks} - p \right| \geq \frac{p}{4} \right)\\
&\geq 1 - 2^{-s}
\end{aligned}$$

and

$$\begin{aligned}
&Pr(\text{Bob gets more than one of } b_0, b_1)\\
&= Pr\left(X_{Ks} \geq 2\left\lceil \frac{2Kps}{3} \right\rceil\right)\\
&\leq Pr\left(X_{Ks} \geq 2\frac{2Kps}{3}\right)\\
&= Pr\left(\frac{X_{Ks}}{Ks} - p \geq \frac{p}{3}\right)\\
&\leq Pr\left(\left| \frac{X_{Ks}}{Ks} - p \right| \geq \frac{p}{3} \right)\\
&\leq Pr\left(\left| \frac{X_{Ks}}{Ks} - p \right| \geq \frac{p}{4} \right)\\
&\leq 2^{-s}
\end{aligned}$$

Now, let's see the case $p > \frac{3}{4}$.

$$
\begin{aligned}
&Pr(\text{Bob gets at least one of } b_0, b_1)\\
&\geq Pr(\text{Bob gets at least one of } b_0, b_1 \mid p=\tfrac{3}{4})\\
&\qquad \geq 1-2^{-s}
\end{aligned}
$$

whenever $K \geq \frac{64}{3}$. And also

$$
\begin{aligned}
&Pr(\text{Bob gets more than one of } b_0, b_1)\\
&\qquad = Pr(X_{Ks} = Ks)\\
&\qquad = p^{Ks}\\
&\qquad \leq 2^{-s}
\end{aligned}
$$

for $K \geq \frac{1}{lg \frac{1}{p}}$. So $K \geq max(\frac{64}{3}, \frac{1}{lg \frac{1}{p}})$ is a sufficient condition for our purpose.

QED.

Essentially, this theorem is claiming that Bob will get one of the bits except with an exponentially small probability, and Alice knows that he cannot get more than one of them except also with an exponentially small probability. In other words, this protocol achieves the one-out-of-two O.T. requirements with probability $1-2^{-s}$.

5. APPLICATIONS

In [BCR] one can find a reduction between a problem named AN2BP (All or Nothing 2 Bits Problem) and a very general disclosure problem: ANDOS (All or Nothing Disclosure of Secrets). Essentially AN2BP is identical to one-out-of-two O.T. except that Bob choses the random bit k used by Alice to decide which bit he gets. So the protocol we describe above accomplishes AN2BP if k is supplied by Bob. This reduction leads to the conclusion that ANDOS can be achieved from any p-O.T., for any constant p. Some more generalizations of O.T. can also be used as basis for reductions and will be explored in a further paper.

In [GMW], a completeness theorem for interactive protocol is presented based on the existence of one-way functions and one-out-of-two O.T. protocols. This completeness theorem can now be based on the existence of p-O.T. and one-way functions. It seems possible that p-O.T. is easier to construct directly than one-out-of-two O.T., in general.

6. OPEN PROBLEMS

An interresting problem is to transform an O.T. in which Alice learns with probability q whether Bob got the bit b or not, or an O.T. in which Bob always learns a bias about b into a one-out-of-two O.T.. Also it would be very interresting to find a way of achieving one of these variations only using one-way functions.

7. ACKNOWLEDGEMENTS

I wish to thank Gilles Brassard, Joe Kilian and Silvio Micali for the discussions we had about the protocol. I want to thank Ernie Brickell for proof reading this version of the paper.

8. REFERENCES

[BCR] Brassard G., Crépeau C. and Robert J.-M., ''Information Theoretic Reductions Among Disclosure Problems'', *Proceedings of the 27th Annual IEEE Symposium on the Foundations of Computer Science*, 1986, pp. 168-173.

[EGL] Even S., Goldreich O. and Lempel A., ''A randomized Protocol for Signing Contracts'', *Communications of the ACM*, Vol. 28, No. 6, 1985, pp. 637-647.

[GMW] Goldreich O., Micali S. and Wigderson A., ''How To Play Any Mental Game or A Completeness Theorem for Protocols with Honest Majority'', *Proceedings of the 19th Annual ACM Symposium on the Theory of Computing*, 1987, pp. 218-229.

[HR] Halpern J. and Rabin M.O., ''A Logic to Reason about likehood'', *Proceedings of the 15th Annual ACM Symposium on the Theory of Computing*, 1983, pp. 310-319.

[Kr] Kranakis, E., ''Primality and Cryptography'', John Wiley & Sons, 1986.