600.641 Special Topics in Theoretical Cryptography 3/19/07

Lecture 13: Oblivious Transfer

Instructor: Susan Hohenberger *Scribe: Adam McKibben*

1 $\frac{1}{2}$-OT

Oblivious transfer (OT) was introduced by Michael Rabin in 1981. He invented a protocol with some curious properties and published it in a tech report. [Rab81] In this protocol a sender will send a message to the receiver with probability $\frac{1}{2}$. Rabin's scheme was later named $\frac{1}{2}$-OT because of this probability.

The scheme works as follows:

1. The sender (S) finds two large primes p, q (such that each prime is equal to $3 \mod 4$) and finds their product $n = pq$ and reveals n to the receiver (R).

2. R chooses a random $x \in \mathbb{Z}_n^*$ and sends $t = x^2 \mod n$ to S.

3. S computes $s = \sqrt{t}$ there will be four roots $x, -x, y, -y$. S can find these roots efficiently because he knows p and q. However, S has no way to know which of these roots was the actual x that R used to compute t. S chooses one of the roots at random and sends it to R.

4. If $s = \pm x$ then R learns nothing, if $s = \pm y$ then R can learn (p, q) by finding $GCD(x + s, n)$ or $GCD(x - s, n)$.

The case that S chooses $s = \pm x$ and the case that $s = \pm y$ are equally likely to occur, so R will learn (p, q) with probability $\frac{1}{2}$. S will not know if R learned the secret or learned nothing.

Some problems with this protocol were later discovered. R can cheat by choosing certain special values t such that R does not know any square roots of t. These special values will allow R to factor n when given *any* square root of t. This problem can be fixed by adding to the protocol a zero-knowledge proof of knowledge for the value of x. [GMR85]

Is this useful? Yes! We will see that this type of protocol, $\frac{1}{2}$-OT is *complete* for secure multi-party computation. That is, if we can securely realize OT, then we can securely realize almost any function. Let's summarize some of the fundamental results in OT.

- Even, Goldreich, and Lempel showed how to build $\binom{2}{1}$-OT from p-OT (where p is the probability that R learns the secret) [EGL85]. In $\binom{2}{1}$-OT, S knows two secrets and R may privately obtain one (and only one) of them. In Rabin's protocol, p=$\frac{1}{2}$.

- Brassard, Crépeau, and Robert showed how to build $\binom{n}{1}$-OT from $\binom{2}{1}$-OT [BCR86]. In $\binom{n}{1}$-OT, S knows n secrets and R may privately obtain one (and only one) of them. This is particularly useful because secure multiparty computation requires $\binom{4}{1}$-OT.

- Claude Crépeau showed how to build $\binom{2}{1}$-OT from $\frac{1}{2}$-OT. [Cre87].

Thus, the $\frac{1}{2}$-OT protocol that Rabin invented can be used to build secure multi party computation.

2 $\frac{1}{2}$-OT implies $\binom{2}{1}$-OT

We will now cover the result of Claude Crépeau, who showed how to build $\binom{2}{1}$-OT from $\frac{1}{2} - OT$ [Cre87]. This is a very nice result. (We present his protocol here with some slight modifications. The interested reader should have a look at the original paper.)

Suppose S knows two secret bits b_o, b_1.[1] Suppose a secure $\frac{1}{2}$-OT protocol exists, then S and R can execute a $\binom{2}{1}$-OT protocol as follows:

1. S and R agree on some security parameters m, n.
2. S chooses n random bits $r_1, ..., r_n$
3. For each $j = 1$ to n, S and R run $\frac{1}{2} - OT$ on r_j. Now R knows approximately half of the bits $r_1 ... R_n$ but S does not know which ones.
4. R picks two index sets $U = \{i_1, ..., i_m\}$ and $V = \{i_{m+1}, ..., i_{2m}\}$ such that $U \cap V = \emptyset$ and so that R knows r_i for all of the indices in U.
5. If R wishes to know b_0, it sends $(X, Y) = (U, V)$ to S. If R wishes to know b_1, it sends $(X, Y) = (V, U)$ to S.
6. S computes $z_0 = \bigoplus_{x \in X} r_x$ and $z_1 = \bigoplus_{y \in Y} r_y$ and sends $(w_1, w_2) = (b_0 \oplus z_0, b_1 \oplus z_1)$ to R.
7. R can now use the bits from U to find z_k. Using z_k, S can find $b_k = (z_k \oplus w_k)$.

Theorem 2.1 ([Cre87]) *For appropriately chosen values of n and m:*
Pr[R gets b_k]$\geq 1 - 2^{-m}$ and Pr[R gets both b_k and $b_{\overline{k}}$] $\leq 2^{-m}$.

The security of the above theorem depends on the selection of n and m. Intuitively, what we want here is that R is highly likely to learn *at least m* values r_j during step (3), so that R can gather the indices of these values together to form a valid set U in step (4) and then use these values to recover the selected bit in step (7). What we also want, however, is that R is highly likely *not* to learn $2m$ or greater values r_j during step (3), or this would allow R to fill both U and V with unique values in step (4) in such a way that R could recover *both* of the sender's bits in step (7). Setting them so that the following relationship holds $\frac{n}{m} \geq \frac{64}{3}$ should suffice.

Note, that this protocol *does* ensure that even a cheating sender cannot discover which bit R chose, but it *does not* ensure that the sender sends the "right" information, i.e., that the sender honestly creates z_k using some specific bit b_k. A cheating sender could return

[1] The protocol shown here is just for bits. Can you see how to generalize this protocol to the case where the secrets b_0 and b_1 are strings?

some random value for z_k and the receiver would not know. We must assume that the sender is willing to reveal the secret information to R, but that R does not want S to know which secret was received.

3 Recent developments in OT

We have seen that $\frac{1}{2}OT \to \binom{2}{1}OT \to \binom{n}{1}OT$. Other variants of OT have also been explored. One example is $\binom{n}{k}$-OT, where the sender has n values and the receiver wants to privately obtain k of them. We briefly mention a few other works.

- Naor and Pinkas introduced *adaptive* $\binom{n}{k}$-OT in [NP99], where instead of R choosing all k values at the beginning of the protocol (as is done in non-adaptive $\binom{n}{k}$-OT), R can privately obtain a value, look at it, and then choose another value up to k times. (Realizing this functionality is not as easy as just running $\binom{n}{1}$-OT k times. Can you think why?) The authors proved their protocol secure in a new half simulation model.
- Kalai showed that $\binom{2}{1}$-OT can be achieved from many different complexity assumptions in the half simulation model using smooth projective hashes [Kal05].
- Naor and Pinkas pointed out a potential security problem with the half simulation model (called the selective failure attack). Thus one might need to consider a stronger security model for OT.
- Recently, Camenisch, Neven and shelat show how to do adaptive $\binom{n}{k}$-OT in the *full* security model in [CNS07].

Using OT and anonymous digital cash it is possible to create a completely anonymous digital transaction. Digital cash can be used to protect the identity of the buyer and OT can be used to prevent the seller from knowing what has been purchased.

References

[BCR86] G. Brassard, C. Crepeau, and J.M. Robert. Information theoretic reductions among disclosure problems. *27th Annual Symposium on Foundations of Computer Science*, pages 168–173, 1986.

[CNS07] J. Camenisch, G. Neven, and A. Shelat. Adaptive Oblivious Transfer from Blind Signatures. *Advances in Cryptology-EUROCRYPT*, 2007.

[Cre87] Claude Crepeau. Equivalence between two flavours of oblivious transfers. In *CRYPTO*, pages 350–354, 1987.

[EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304, 1985.

[Kal05] Y.T. Kalai. Smooth Projective Hashing and Two-Message Oblivious Transfer. *Advances in Cryptology-EUROCRYPT*, pages 22–26, 2005.

[NP99] M. Naor and B. Pinkas. Oblivious transfer with adaptive queries. *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pages 573–590, 1999.

[Rab81] M. Rabin. How to exchange secrets by oblivious transfer. 1981.