CMSC 858K — Introduction to Secure Computation September 11, 2013

Lecture 3

Lecturer: Jonathan Katz *Scribe(s): Aishwarya Thiruvengadam*

1 Summary

In this lecture, we introduce the primitive called Oblivious Transfer (OT). Oblivious transfer is a fundamental primitive from both a theoretical and practical standpoint. We give the definition of OT and present a protocol for 1-out-of-2 OT by Even-Goldreich-Lempel and prove that it is secure.

2 Oblivious Transfer

An oblivious transfer (OT) protocol allows a sender to transmit some of his inputs to the receiver with the guarantee that both parties do not learn more information than allowed (i..e.) the sender learns nothing about the choices of the receiver and the receiver learns no other inputs but those he chose to receive. In a 1-out-of-2 OT, the sender has two inputs x_0, x_1 and the receiver has a choice bit $b \in \{0,1\}$ and learns x_b at the end of the protocol while the sender learns nothing.

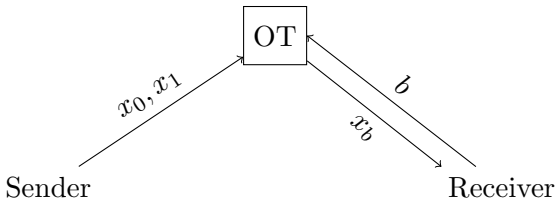


Figure 1: Oblivious Transfer

3 Oblivious Transfer Protocol

Here, we present a 1-out-of-2 OT protocol by Even-Goldreich-Lempel [EGL85]. The protocol uses a CPA-secure public key encryption scheme which we define below.

3.1 Public Key Encryption Scheme

A public key encryption scheme $\mathcal{E}$ consists of three probabilistic polynomial time algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where

- Gen is the key generation algorithm that on input 1^n, where n is the security parameter, outputs the public key pk and the secret key sk,

- Enc is the encryption algorithm that on input a message m and the public key pk outputs a ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m)$,
- Dec is the decryption algorithm that on input a ciphertext c and secret key sk outputs the message $m = \mathsf{Dec}_{sk}(c)$.

It is required that for every n, every $pk, sk \leftarrow \mathsf{Gen}(1^n)$ and every message m from the message space, it holds that $\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m$.

Definition 1[CPA security] Let $X_n(m) \stackrel{\text{def}}{=} \{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : (pk, \mathsf{Enc}_{pk}(m))\}$ and $Y_n(m) \stackrel{\text{def}}{=} \{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : (pk, \mathsf{Enc}_{pk}(0^{|m|}))\}$ for every m in the message space. A public key encryption scheme is secure against chosen plaintext attacks (CPA-secure) if the ensembles $\{X_n\}$ and $\{Y_n\}$ are computationally indistinguishable. $\diamondsuit$

For the security of the OT protocol, we also require that the encryption scheme have obliviously sampleable public keys. An encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has *obliviously sampleable* public keys if

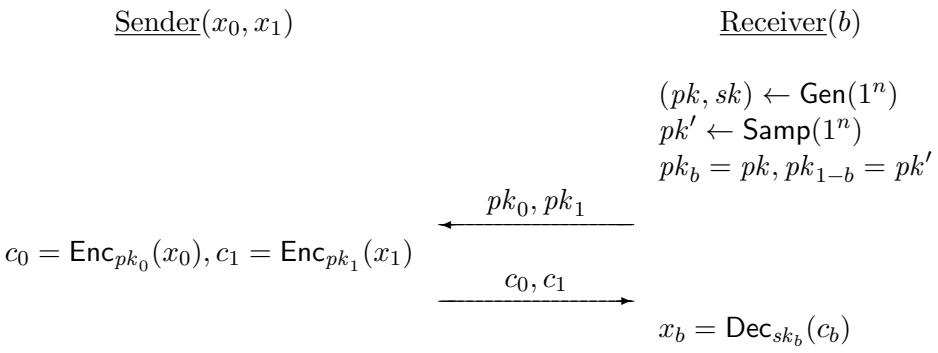
- there exists a polynomial time algorithm Samp such that $\{\mathsf{Samp}(1^n)\}$ is identically distributed to $\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : pk\}$ [1]
- there exists a polynomial time algorithm pkSim such that $\{r \leftarrow \{0,1\}^n; pk = \mathsf{Samp}(1^n; r) : (pk, r)\}$ and $\{(pk, sk) \leftarrow \mathsf{Gen}(1^n); r \leftarrow \mathsf{pkSim}(pk) : (pk, r))\}$ are computationally indistinguishable.

Note that standard El Gamal has obliviously sampleable public keys.

3.2 1-out-of-2 OT Protocol

Consider the following protocol π by Even-Goldreich-Lempel that requires a public key encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

OT Protocol



Theorem 1 *If the encryption scheme $\mathcal{E}$ is CPA-secure and has obliviously sampleable public keys, then protocol π 1-privately computes OT.*

[1] This condition alone is not sufficient as $\mathsf{Samp}(1^n)$ could be $\mathsf{Gen}(1^n)$.

Proof Let us first prove security against the sender. We need to show that there exists $\mathcal{S}$ such that $\{\mathcal{S}(1^n, x_0, x_1, z)\}$ and $\{\text{View}^{\pi}_{\text{sender}}(1^n, x_0, x_1, b, z)\}$ are computationally indistinguishable. Let us construct the following simulator $\mathcal{S}$ that runs as follows on input the security parameter n and strings x_0 and x_1.
$\underline{\mathcal{S}(1^n, x_0, x_1)}$:

1. Run $(pk_0, sk_0) \leftarrow \mathsf{Gen}(1^n)$ and $(pk_1, sk_1) \leftarrow \mathsf{Gen}(1^n)$
2. Choose randomness r_0, r_1 for the two encryptions.
3. Output $(pk_0, pk_1, r_0, r_1, x_0, x_1)$.

Consider the view of the sender in the protocol π. The sender has inputs $1^n, x_0, x_1$ and does not receive any output.
$\underline{\text{View}^{\pi}_{\text{sender}}(1^n, x_0, x_1)}$:

1. The sender receives $(pk_b, sk_b) \leftarrow \mathsf{Gen}(1^n)$ and $pk_{1-b} \leftarrow \mathsf{Samp}(1^n)$,
2. the randomness r_0, r_1 for the two encryptions.
3. Hence, the sender's view consists of $(pk_0, pk_1, r_0, r_1, x_0, x_1)$.

The public and the secret key pair (pk_b, sk_b) corresponding to the choice bit b is identically distributed in both cases above as they are both generated by running the key generation algorithm of the public key encryption scheme. Note also that pk_{1-b} is identically distributed in both cases as well. This is because of the fact that we assume that $\mathcal{E}$ is a public key encryption scheme that has obliviously sampleable public keys and hence $\mathsf{Samp}(1^n)$ and $\mathsf{Gen}(1^n)$ are identically distributed.

Let us now prove security against the receiver for the OT protocol. We construct the following simulator $\mathcal{S}$ that runs as follows on input the security parameter n, choice bit b and string x_b. (Note that the simulator receives both the input and the output of the receiver as its inputs.)
$\underline{\mathcal{S}(1^n, b, x_b)}$:

1. Choose randomness r_{Gen} and compute $(pk_b, sk_b) \leftarrow \mathsf{Gen}(1^n)$.
2. Run $(pk_{1-b}, sk_{1-b}) \leftarrow \mathsf{Gen}(1^n)$ and compute $r_{\text{Samp}} \leftarrow \mathsf{pkSim}(pk_{1-b})$.
3. Set $c_b \leftarrow \mathsf{Enc}_{pk_b}(x_b)$ and $c_{1-b} \leftarrow \mathsf{Enc}_{pk_{1-b}}(0^n)$.
4. Output $(r_{\text{Gen}}, r_{\text{Samp}}, c_0, c_1, b, x_b)$.

Consider the view of the receiver in the protocol π. The receiver has inputs $1^n, b$ and receives output x_b.
$\underline{\text{View}^{\pi}_{\text{receiver}}(1^n, b)}$:

1. The receiver chooses randomness $r_{\text{Gen}}, r_{\text{Samp}}$ and computes $(pk_b, sk_b) \leftarrow \mathsf{Gen}(1^n; r_{\text{Gen}})$ and $pk_{1-b} \leftarrow \mathsf{Samp}(1^n; r_{\text{Samp}})$.

2. The receiver receives $c_b = \mathsf{Enc}_{pk_b}(x_b), c_{1-b} = \mathsf{Enc}_{pk_{1-b}}(c_{1-b})$.

3. Hence, the receiver's view consists of $(r_{\text{Gen}}, r_{\text{Samp}}, c_0, c_1)$.

In order to prove security against the receiver, we have to show that $\mathcal{S}(1^n, b, x_b)$ and $\text{View}^{\pi}_{\text{receiver}}(1^n, b)$ are computationally indistinguishable. Consider the following hybrid:

Hybrid$(1^n, b)$:

1. Choose randomness r_{Gen} and compute $(pk_b, sk_b) \leftarrow \mathsf{Gen}(1^n; r_{\text{Gen}})$.

2. Compute $pk_{1-b} \leftarrow \mathsf{Gen}(1^n)$ and run pkSim to obtain $r_{\text{Samp}} \leftarrow \mathsf{pkSim}(pk_{1-b})$.

3. Receive ciphertexts $c_b = \mathsf{Enc}_{pk_b}(x_b), c_{1-b} = \mathsf{Enc}_{pk_{1-b}}(c_{1-b})$.

4. Output $(r_{\text{Gen}}, r_{\text{Samp}}, c_0, c_1)$.

By definition of the algorithm pkSim, the distributions $\text{View}^{\pi}_{\text{receiver}}(1^n, b)$ and Hybrid$(1^n, b)$ are identical. For distributions Hybrid$(1^n, b)$ and $\mathcal{S}(1^n, b, x_b)$, the difference is that we replaced the encryption of x_{1-b} with that of 0^n. The proof that these two distributions are computationally indistinguishable follows by reduction from the CPA security of the encryption scheme. We sketch the reduction below.

Fix some distinguisher D that can distinguish distributions Hybrid$(1^n, b)$ and $\mathcal{S}(1^n, b, x_b)$ with probability ε. Construct distinguisher $D'(1^n, b, x_0, x_1)$ for the CPA security of the encryption scheme as follows. When D' receives the public key pk and the challenge ciphertext c from the CPA security experiment where c is either the encryption of x_{1-b} or 0^n, D' does the following:

1. $(pk_b, sk_b) \leftarrow \mathsf{Gen}(1^n; r_{\text{Gen}})$

2. $r_{\text{Samp}} \leftarrow \mathsf{pkSim}(pk)$

3. $c_b = \mathsf{Enc}_{pk_b}(x_b); c_{1-b} = c$

4. Output $D(r_{\text{Gen}}, r_{\text{Samp}}, c_0, c_1)$

If $c = \mathsf{Enc}_{pk}(x_{1-b})$, then the view of D is distributed identically to Hybrid$(1^n, b)$. If $c = \mathsf{Enc}_{pk}(0^n)$, then the view of D is distributed identically to $\mathcal{S}(1^n, b, x_b)$. By the CPA security of the encryption scheme, we have that the probability of success for any distinguisher D' is negligible. This implies that the probability of success of D is negligible as the probability of success of D is exactly equal to the probability of success of D'. This implies that distributions Hybrid$(1^n, b)$ and $\mathcal{S}(1^n, b, x_b)$ are computationally indistinguishable. Hence, we have that distributions $\text{View}^{\pi}_{\text{receiver}}(1^n, b)$ and $\mathcal{S}(1^n, b, x_b)$ are computationally indistinguishable. ■

References

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, June 1985.