MTAT.07.003 Cryptology II
Spring 2009 / Exercise session XIII

1. In the following, we are going to consider the simplified version of the oblivious transfer protocol that was proposed by Even, Goldreich and Lempel. As usual, let $\mathcal{P}_1$ be the receiver with input $b \in \{0,1\}$ and let $\mathcal{P}_2$ be the sender with input $x_0, x_1 \in \mathcal{M}$. Additionally, assume that participants can use oracle $\mathcal{O}_{\text{map}} : \mathcal{M} \to \mathcal{M}$ to evaluate a random permutation over $\mathcal{M}$ and the sender $\mathcal{P}_2$ can use the corresponding inversion oracle $\mathcal{O}_{\text{inv}}$:

$$\forall m \in \mathcal{M} : \quad \mathcal{O}_{\mathsf{inv}}(\mathcal{O}_{\text{map}}(m)) \equiv m \ .$$

To transfer the message x_b participants carry out the following steps:

1. $\mathcal{P}_1$ sends c_0, c_1 where $c_{1-b} \xleftarrow{u} \mathcal{M}$ and $c_b \leftarrow \mathcal{O}_{\text{map}}(r)$ for $r \xleftarrow{u} \mathcal{M}$.
2. $\mathcal{P}_2$ replies $d_0 \leftarrow \mathcal{O}_{\text{inv}}(c_0) \oplus x_0$ and $d_1 \leftarrow \mathcal{O}_{\text{inv}}(c_1) \oplus x_1$.
3. $\mathcal{P}_1$ reconstructs $x_b \leftarrow r \oplus d_b$.

Prove the protocol is secure in the semi-honest model.

(a) The protocol is functional and receiver indeed recovers x_b.

(b) Construct a simulator for semi-honest sender and show that the output distributions in the real an ideal world coincide.

(c) Construct a simulator for semi-honest receiver and show that the output distributions in the real an ideal world are computationally indistinguishable. More precisely, give the bound on distinguishing advantage in terms of $\mathcal{O}_{\text{map}}$ queries made by the distinguisher.

Hint: What is the distinguishing advantage if the distinguisher makes no calls to $\mathcal{O}_{\text{map}}$ and the receiver makes only a single $\mathcal{O}_{\text{map}}$ call?

($\star$) The full construction of the oblivious transfer proposed by Even, Goldreich and Lempel uses hard-core predicates. Let $\mathcal{F}_{\text{tp}}$ be a collection of trapdoor permutations and $\mathcal{P}_{\text{hc}}$ be the predicate collection with matching domain $\mathcal{M}_{\mathsf{pk}}$. Then the family $\mathcal{P}_{\text{hc}}$ forms a (t, ε)-hard-core predicate set with respect to $\mathcal{F}_{\text{tp}}$, if for any t-time algorithm $\mathcal{A}$ the corresponding advantage

$$\mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{\mathcal{F}_{\text{tp}} \bowtie \mathcal{P}_{\text{hc}}}(\mathcal{A}) = \left| \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] \right| \leq \varepsilon$$

where

$\mathcal{G}_0^{\mathcal{A}}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$m \xleftarrow{u} \mathcal{M}_{\mathsf{pk}}$
$b \xleftarrow{u} \{0,1\}$
return $\mathcal{A}(\mathsf{pk}, m, b)$

$\mathcal{G}_1^{\mathcal{A}}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$m \xleftarrow{u} \mathcal{M}_{\mathsf{pk}}$
$b \leftarrow \mathsf{Pred}_{\mathsf{pk}}(\text{Inv}_{\mathsf{sk}}(m))$
return $\mathcal{A}(\mathsf{pk}, m, b)$

Prove that the standard oblivious transfer protocols for 1-bit messages, where $d_i \leftarrow \mathsf{Pred}_{\mathsf{pk}}(\mathrm{Inv}_{\mathsf{sk}}(c_i)) \oplus x_b$, is secure in the standard model. Also, find a reference that shows that hard core predicates exist if one-way functions exist. Compute the corresponding security guarantees.

2. Recall that the Goldwasser-Micali cryptosystem is additively homomorphic over $\mathbb{Z}_2$ construct a corresponding oblivious transfer protocol based on the Aiello-Ishai-Reingold generic construction that was presented in the lecture. Additionally, assume that RSA modulus is correctly generated from two n-bit Blum primes such that the quadratic residuosity problem is (t, ε)-hard. That is, for all t-time adversaries $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{qrp}}_{\mathbb{P}_n}(\mathcal{A}) = |\Pr[\mathcal{Q}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{Q}_0^{\mathcal{A}} = 1]| \leq \varepsilon$$

where

$$\begin{array}{ll} \mathcal{Q}_0^{\mathcal{A}} & \mathcal{Q}_1^{\mathcal{A}} \\ \left[\begin{array}{l} p, q \xleftarrow{u} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow{u} QR_N \\ \textbf{return } \mathcal{A}(x) \end{array}\right. & \left[\begin{array}{l} p, q \xleftarrow{u} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow{u} J_N \setminus QR_N \\ \textbf{return } \mathcal{A}(x) \end{array}\right. \end{array}$$

Now prove the security of the corresponding oblivious transfer protocol directly from the indistinguishability property.

3. The construction of the one out of two oblivious transfer protocol proposed by Aiello, Ishai and Reingold can be extended in several ways.

   (a) Construct one out of n oblivious transfer protocol.
   Hint: Construct a protocol that reveals x only if $\mathsf{Dec}_{\mathsf{sk}}(c) = 2$.

   (b) Explain how to transfer long messages that do not fit into the message space of the homomorphic encryption by repeating the transfer phase. What happens with the security guarantees?

   (c) Explain how we can use the underlying principle of hybrid encryption and make the protocol more efficient for long strings. What happens with the security guarantees?

   (d) Describe how we can use the construction given above to implement pay-per-view system for sensitive content (satellite pictures).

4. Not all protocols used for one out of two oblivious transfer are perfect and therefore we need generic techniques for security amplification.

   (a) Consider a leaking ideal oblivious transfer protocol π for k-bit strings, where the trusted third party reveals with probability p both inputs x_0 and x_1 to receiver but with probability $1 - p$ reveals only x_b as desired. Describe a construction that uses several instances of π to securely implement one out of two oblivious transfer for k-bit strings.
   Hint: Use additive secret sharing to achieve all or nothing property.

(b) Consider a defective ideal oblivious transfer protocol π for k-bit strings, where trusted third party reveals x_b with probability p and otherwise halts the protocol prematurely. Describe a construction that uses several instances of π to securely implement one out of two oblivious transfer for k-bit strings.

Hint: What about error correction codes?

(c) Let π be an ideal oblivious transfer protocol for k-bit strings and let $f : \{0,1\}^k \to \{0,1\}^n$ be a (t, ε)-pseudorandom generator. Construct one out of two oblivious transfer protocol for n-bit strings.

5. Given a protocol π for ideal one out of two oblivious transfer, construct a commitment scheme by amplifying security properties of the following commitment scheme.

   1. To commit a bit x, a sender creates uniformly distributed pair x_0, x_1 such that $x_0 \oplus x_1 = x$. To get a commitment string c, the receiver chooses $b \xleftarrow{u} \{0,1\}$ and uses π to retrieve x_b.
   2. To open a commitment, the sender releases both values x_0 and x_1. The commitment is invalid if $c \neq x_b$.

   (a) Prove that the commitment scheme is perfectly hiding and $\frac{1}{2}$-binding.

   (b) Give a construction that is perfectly hiding and 2^{-k}-binding.

   (c) Extend the abovementioned construction for ℓ-bit strings.

   This result is important as Brassard, Chaum and Crépeau proved that everything is provable in zero knowledge provided that binding and hiding commitment schemes exists. More precisely, let the relation between a public parameter x and a secret witness w be encoded as a predicate

   $$\psi(x, w) = 1 \quad \Leftrightarrow \quad (x, w) \in R \ .$$

   Then the corresponding zero-knowledge proof can be computed in time $\Theta(\text{size}(\psi))$ where $\text{size}(\phi)$ is the the total number of wires, unary and binary logic gates in the circuit used to compute the formula ψ.

   (d) Conclude that one can implement zero knowledge proofs using only the implementations of ideal oblivious transfer. Is the latter formally sufficient to conclude that everything can be securely computed given a secure implementation of oblivious transfer?

6. Consider computations in the semi-honest model. Let π be a one out of two ideal oblivious transfer protocol for n-bit strings and let $f : \{0,1\}^n \to \{0,1\}^{2n}$ be a (t, ε)-secure pseudorandom generator. Construct an oblivious tree traversal protocol such that a receiver could retrieve all inputs stored in the arcs on the path selected by the receiver.

(a) Implement non-private but functional protocol, where receiver uses oblivious transfer to receive the input stored on the outgoing arc.

(b) Extend the tree protocol so that it preserves receiver-privacy, i.e., the server cannot detect which path the receiver chose.

(c) Use the inputs on the arc to encrypt the inputs of the following arcs. Conclude that the modified protocol is also computationally secure against semi-honest and malicious receivers.

(d) Conclude that any function can be computed by simultaneously executing enough oblivious transfer protocols. Is this protocol efficient for all functions?

($\star$) Let π be a one out of two oblivious transfer protocol that is secure against malicious receivers and semi-honest senders. Now consider the following simulator for malicious senders $\mathcal{P}_2^*$

$\mathcal{S}^{\mathcal{P}_2^*}$

$\omega_1 \xleftarrow{u} \Omega_1, \omega_2 \xleftarrow{u} \Omega_2$
Let $\hat{x}_0$ be the output of $\mathcal{P}_1(0;\omega_1)$ interacting with $\mathcal{P}_2(\omega_2)$.
Let $\hat{x}_1$ be the output of $\mathcal{P}_1(0;\omega_1)$ interacting with $\mathcal{P}_2(\omega_2)$.
Submit $\hat{x}_0$ and $\hat{x}_1$ to the trusted third party $\mathcal{T}$.
Output the end state of $\mathcal{P}_2(\omega_2)$ interaction with $\mathcal{P}_1(0;\omega_1)$.

where $\omega_1 \xleftarrow{u} \Omega_1$ is the randomness used by honest receiver $\mathcal{P}_1$ and $\omega_2 \xleftarrow{u} \Omega_2$ is the randomness used by malicious sender $\mathcal{P}_2^*$. Does this construction lead to joint output distribution that is computationally or statistically indistinguishable from the real world output distribution? Prove it or give a counter-example. Interpret the result.

Implicit assumption: We assume that receiver output always some output even if the sender halts or otherwise behaves illogically.

Hint: Consider first the protocol that has a perfect simulator for semi-honest sender.