CSC 591 Cryptography 11/19/2018

Lecture 17 - Commitment Scheme

Lecturer: Alessandra Scafuro *Scribe: Rui Zhu*

Topic/Problem

In this lecture, we went through the formal definition of *Commitment Scheme*, along with two specific commitment schemes: *Naor's Commitment Scheme* (Bit Commitment) and *Pedersen Commitment Scheme* (String Commitment).

Defintion

Intuition: Nowadays, commitment scheme is used in confidential transactions. The idea is to hide the message for a while and open it later as is.
A commitment scheme is a pair of algorithms S (commiter), R (receiver) and consists of 2 phases (Commitment Phase, Opening Phase). It has two properties:

1. Hiding: At the end of the commitment phase, any adversarial receiver R^* should not learn anything about m.
2. Binding: Once the commitment phase was completed with transcript C, any malicious sender S^* should not be able to provide $(m_1, op_1), (m_2, op_2)$ such that both opening info can be accepted by the receiver.

The hiding experiment Hiding (A, Π, n)

1. The adversary R^* sends message m_0, m_1 to the challenger.
2. The challenger picks a bit b and execute the commitment phase of scheme Π on input m_b interacting with the adversary R^*.
3. At the end of the commitment phase, the adversary R^* outputs b'.
4. The adversary wins if $b = b'$.

A commitment scheme is hiding if for all PPT R^*,

$$Pr[R^* \text{wins hiding game}(\Pi, R^*, n)] \leq \frac{1}{2} + negl.(n)$$

For the binding part,

$$Pr[S^* \rightarrow (C, m_1, m_2, op_1, op_2) \wedge R^*(C, m_1, op_1) \wedge R^*(C, m_2, op_2)] \leq negl.(n)$$

A scheme can either be perfectly hiding and computationally binding or perfectly binding and computationally hiding.
The differences between encryption and commitments are that commitments can be interactive and are supposed to be used only one time.

Scheme

Naor's Commitment Scheme

Naor's Commitment Scheme is a bit commitment scheme, we can only commit to a bit 0 or 1.
In this scheme, we will use a PRG $G : \{0,1\}^n \to \{0,1\}^{3n}$.
In the commitment phase, the receiver R picks a random string $r \leftarrow \{0,1\}^{3n}$ and sends r to the sender S.
S picks a seed $s \leftarrow \{0,1\}^n$.
If the bit $b = 0$, compute $c = G(s)$; if $b = 1$, compute $c = G(s) \oplus r$.
c is sent back to R.
In the opening phase, S sends b, s.
R can check if $c = G(s) \oplus (b * r)$ is true. If true, R accepts and outputs 1, else outputs 0.

Pederson Commitment Scheme

Pederson Commitment Scheme works for group elements. Assume the public parameters G, g, q are known.
The sender S has a message $m \leftarrow Z_q$ for commitment.
In the commitment phase, the receiver R picks a random element $h \leftarrow G$ and sends h to S.
S picks a random $r \leftarrow Z_q$ and computes $c = g^r * h^m$. c is sent back to R.
In the opening phase, S sends r, m and R can check if $c = g^r * h^m$.

Security Proof

Naor's Commitment: Hiding

Any malicious R^* should not distinguish if c is a commitment of 0 or 1.
Intuition: The difference between commitments of 0 and 1 is that if $b = 0$, c is the output of a PRG, thus pseudorandom, while c is random if $b = 1$.

Proof

1. Towards a contradiction assume that there is an adversarial R^* that wins the hiding game with probability $\frac{1}{2} + p(n)$.
   Hiding Game instantiated with Naor's Scheme **Hiding** (A, Π_{Naor}, n)
   - R^* sends r
   - The challenger picks a bit b and then outputs $c = G(s) \oplus (b * r)$
   - R^* outputs b'
   - If $b = b'$ then R^* wins
2. Consider a mental experiment where the adversary has 0 advantage, i.e., the adversary wins with probability $\frac{1}{2} + 0$.
   Hiding Game instantiated with an ideal scheme **Hiding** $(A, \tilde{\Pi}_{Naor}, n)$
   - R^* sends r

- The challenger picks a bit b and then outputs $c = R(s) \oplus (b * r)$
- R^* outputs b'
- If $b = b'$ then R^* wins

3. Reduction to PRG security. Let D be a distinguisher for PRG G which has an input string y of length $3n$ bits and tries to distinguish if y is coming from PRG or a random function.
   Reduction $D(y)$
   - Activate R^*
   - Obtain r from R^*
   - Pick a bit b
   - Compute $c = y \oplus (b * r)$
   - When R^* outputs b', if $b = b'$ (R^* wins), output 1, else output 0.

4. Analysis
   - Case $y = G(s)$

$$Pr[D(y) \to 1] = Pr[R^* \text{wins Hiding}(A, \Pi_{Naor}, n)] = \frac{1}{2} + p(n)$$

   - Case $y = random$

$$Pr[D(y) \to 1] = Pr[R^* \text{wins Hiding}(A, \tilde{\Pi}_{Naor}, n)] = \frac{1}{2}$$

   The probability that D can distinguish if a string y is coming from a PRG or a truly random function is:

$$Pr_{y \leftarrow G}[D(y) \to 1] - Pr_{y \leftarrow R}[D(y) \to 1] = p(n),$$

   which should be negligible. Thus R^* can only win the hiding game with probability $\frac{1}{2} + negl.(n)$, proving the security of this scheme.

Pederson Commitment: Hiding

The Pederson Commitment Scheme is also perfectly hiding. We didn't prove this thoroughly in the lecture, but a brief intuition would be:
Consider an adversarial R^* trying to break the hiding game.
R^* picks two messages $m_0, m_1 \leftarrow Z_q$ and choose h.
After receiving c, R^* need to find out if c is a commitment of m_0 or m_1.
Knowing c, h, m, R^* can compute $y_0 = \frac{c}{h^{m_0}}$ and $y_1 = \frac{c}{h^{m_1}}$ to check which m is used. However, that leaves R^* with a Discrete Log number g^r where r is unknown. Given the security of Discrete Log Assumption (refer to lecture8), this commitment scheme is perfectly hiding.