T-79.5502 Advanced Course in Cryptology

Lecture 7, April 6 , 2006

Formal and Strong Security Definitions 2 (Chapter 14)

Semantic security vs. IND-CPA

Property 14.1: (Semantic security) Whatever is efficiently computable about the plaintext given the ciphertext, is also efficiently computable without the ciphertext.

Definition (Sven, page 5): (Semantic security) A Public Key Cryptosystem is ε-secure if, given the ciphertext, the adversary's advantage in computing any efficiently computable predicate relative to the plaintext is less than ε.

Note: In Definition 14.1, Mao defines semantic security as equivalent to IND-CPA. We take Mao's Definition 14.1 as the definition for IND-CPA. Definition 14.1 is essentially equivalent to Sven's definition of IND-CPA, page 6. On page 9-10, Sven shows that IND-CPA implies Semantic security.

IND-CPA ⇒ Semantic security

In Sven's proof:

Cryptosystems that have IND-CPA are attacked by Malice.

Cryptosystems having semantic security are attacked by Charlie.

Sven shows that if Charlie has advantage $\mathrm{Adv}^{\mathrm{guess}}(\mathrm{Charlie})$, then Malice has advantage $\mathrm{Adv}(\mathrm{Malice}) = ½\, \mathrm{Adv}^{\mathrm{guess}}(\mathrm{Charlie})$. Idea of Sven's proof is as follows:

Malice is running his distinguishing game (Mao:Protocol 14.1, Sven: Slide 7). Charlie is good in computing predicates (solving decision problems). Malice makes use of Charlie by giving him a ciphertext. In Malice's world Exp_0, Charlie has some positive advantage in outputting $\pi(m_0)$. Similarly, in world Exp_1 Charlie would have some advantage in outputting $\pi(m_1)$, but no advantage at all in outputting $\pi(m_0)$!

(TBD) The converse also holds: Semantic security ⇒ IND-CPA

DDH ⇒ ElGamal is IND-CPA

The proof DDH ⇒ ElGamal is IND-CPA (Sven, slide 23) is using the same idea but the otherway round. Now Charlie, who wants to solve DDH problem, makes use of Malice, who is good at the ciphertext distinguishing game for ElGamal. Now Charlie has two worlds, Exp_0, where $z = g^{xk}$, and Exp_1, where $z = g^c$, and he has to guess in which world he is. Charlie asks Malice to help. In Exp_0 world, Malice plays his distinguishing game with some positive advantage, but in Exp_1 world Malice is completely lost. It is exactly this difference between the worlds Exp_0 and Exp_1 that Charlie is making use of!

IND-CPA is weak security

Chosen Ciphertext Attack on GM cryptosystem:

Malice has seen $c = E_{pk}(m)$, and wants to find out the bit m encrypted using Alice's public key. Alice has asked Malice a question and asked him to reply yes (=1) or no (=0). Malice prepares a ciphertext as follows: selects $m' = 0$ and encrypts it using Alice's public key, $x \leftarrow_{\mathrm{R}} \mathbf{Z}_N{}^*$, $E_{pk}(0) = (x)^2 \bmod N$, and creates ciphertext $c' = c(x')^2 \bmod N$, and sends it to Alice.

Then Malice will be able to decrypt based on Alice's reaction. Assume Alice says: "Why do you say no?" Then Malice knows that $m = 0$.

Alice could prevent this if she before decrypting can verify that the sender of the ciphertext knows everything about the plaintext.

Homomorphic encryption

Given ElGamal encryptions of m_1 and m_2 :

$(\alpha^{k_0}, \beta^{k_0} m_0)$ and $(\alpha^{k_1}, \beta^{k_1} m_1)$

one can generate valid ElGamal encryptions for $m_0 m_1$:

$$(\alpha^{k_0+k_1}, \beta^{k_0+k_1} m_0 m_1)$$

and and m_0 / m_1 :

$$(\alpha^{k_0-k_1}, \beta^{k_0-k_1} \frac{m_0}{m_1})$$

even without knowledge of the public key.

Vulnerable to CCA attacks, but has also some virtue: Can be used for oblivious transfer (OT).

One-out-of-Two Oblivious Transfer

Alice has two digital products m_0 and m_1. Bob wants to buy one of them, and Alice is willing to sell just one.

The protocol (Aiello et al, Eurocrypt 2001)

1. Alice and Bob agree on a group G where ElGamal cryptosystem is secure, and a generator $\alpha \in G$ of order n.
2. Bob generates a key pair $(a, \beta = \alpha^a)$ for ElGamal cryptosystem and selects the product m_b he wants to buy. He represents his choice as bit as $B = \alpha^b$ and computes an encryption of it: $C = (\alpha^k , \beta^k B)$. Bob sends C, β to Alice.
3. Alice verifies that β is a valid public key and C is a valid ciphertext (there are cryptographic methods for doing this.)

One-out-of-Two Oblivious Transfer (2)

4. Alice draws four integers $k_j, r_j, j = 0,1, 0 < k_j, r_j < n$, uniformly at random and computes encryptions of α^j , $j = 0,1$:

$$C_j = (\alpha^{k_j}, \beta^{k_j} \alpha^j),\ j = 0,1$$

and further encryptions of $\alpha^j /B = \alpha^{j - b}$ using homomorphic encryption. (Note that Alice does not know B but she knows the encryption C of it.)

$$(\frac{\alpha^{k_j}}{\alpha^k}, \frac{\beta^{k_j}\alpha^j}{\beta^k B}) = (\alpha^{k_j - k}, \beta^{k_j - k}\alpha^{j-b})$$

Then she raises both parts to power r_j and creates encryptions of $\alpha^{(j-b)rj}\ m_j$:

$$(\alpha^{(k_j - k)r_j}, \beta^{(k_j - k)r_j}\alpha^{(j-b)r_j} m_j),\ j = 0,1$$

and sends both encryptions to Bob.

One-out-of-Two Oblivious Transfer (3)

5. Bob takes the one with $j = b$, and is able to decrypt m_b as

$$(\alpha^{(k_b-k)r_b}, \beta^{(k_b-k)r_b}\alpha^{(b-b)r_b}m_b)$$

is a proper El Gamal encryption of m_b , since $\alpha^{b-b} = 1$.

If Bob selects $j \neq b$, and decrypts he gets $\alpha^{(j-b)\,rj}\, m_j = \alpha^{\pm rj}\, m_j$, which is random data.

Lunchtime Attack (Protocol 14.3)

Exp_0	Exp_1
1. $(pk,sk) \leftarrow$ G	1. $(pk,sk) \leftarrow$ G
2. $c \leftarrow \text{Malice}(pk)$	2. $c \leftarrow \text{Malice}(pk)$
3. $D_{sk}(c) \leftarrow$ O(c,sk)	3. $D_{\text{sk}}(c) \leftarrow$ O(c,sk)
4. $(m_0,m_1,\sigma) \leftarrow \text{Malice}$	4. $(m_0,m_1,\sigma) \leftarrow \text{Malice}$
5. $E_{pk}(m_0) \leftarrow$ O(coins, $m_0,m_1,pk)$	5. $E_{pk}(m_1) \leftarrow$ O(coins, $m_0,m_1,pk)$
6. guess $\leftarrow$ Malice$(\sigma, E_{pk}(m_0))$	6. guess $\leftarrow$ Malice$(\sigma, \text{E}_{\text{pk}}(\text{m}_1))$

$$\text{Adv(Malice)} = |\Pr[\text{guess} = 0 |\ \text{Exp}_0] - ½| \qquad (14.5.1)$$

$$= ½\ |\Pr[\text{guess} = 0|\ \text{Exp}_0] - \Pr[\text{guess} = 0|\text{Exp}_1]\ |$$

IND-CCA security

Definition 14.2: A cryptosystem with a security parameter k is said to be secure against an indistinguishable chosen-ciphertext attack (IND-CCA secure) if after the attack game in Protocol 14.3 being played with any polynomially bounded attacker, the advantage Adv is a negligible quantity in k.

Small-hours Attack (Protocol 14.4)

Exp_0	Exp_1
1. $(pk,sk) \leftarrow$ G	1. $(pk,sk) \leftarrow$ G
2. $c \leftarrow$Malice(pk) 3. $D_{sk}(c) \leftarrow$ O(c,sk)	*2.* $c \leftarrow$ Malice(pk) *3.* $D_{\mathrm{sk}}(c) \leftarrow$ O(c,sk)
4. $(m_0,m_1,\sigma) \leftarrow$ Malice 5. $E_{pk}(m_0) \leftarrow$ O(coins, m_0,m_1,pk)	4. $(m_0,m_1,\sigma) \leftarrow$ Malice 5. $E_{pk}(m_1) \leftarrow$ O(coins, m_0,m_1,pk)
6. $c' \leftarrow$Malice(pk) ($c' \neq E_{pk}(m_0)$) 7. $D_{sk}(c) \leftarrow$ O(c',sk)	6. $c' \leftarrow$Malice(pk) ($c' \neq E_{pk}(m_1)$) 7. $D_{sk}(c) \leftarrow$ O(c',sk)
8. guess $\leftarrow$ Malice(σ, $E_{pk}(m_0)$)	8. guess $\leftarrow$ Malice(σ, $\mathrm{E}_{\mathrm{pk}}(\mathrm{m}_1)$)

IND-CCA2 Security

Again:

Adv(Malice) = $|\Pr[\text{guess} = 0 \mid \text{Exp}_0] - ½|$ (14.5.2)

$= ½\ |\Pr[\text{guess} = 0 \mid \text{Exp}_0] - \Pr[\text{guess} = 0 \mid \text{Exp}_1]\ |$

Definition 14.3:A cryptosystem with a security parameter k is said to be secure against an indistinguishable chosen-ciphertext attack (IND-CCA2 secure) if after the attack game in Protocol 14.4 being played with any polynomially bounded attacker, the advantage Adv is a negligible quantity in k.

Malleability (Protocol 14.5)

1. $(pk,sk) \leftarrow$ G
2. **v,** desc(**v**) ← Malice(*pk),* desc(**v**) is a description of the distribution of the plaintexts in **v**
3. $c^* = E_{pk}(\alpha) \leftarrow$ O(**v**,desc(**v**),*sk*)
4. $(E_{pk}(\beta), \alpha \neq \beta, R, R(\alpha,\beta) = 1) \leftarrow$ Malice(**v**, desc(**v**),c^*)

NM-Adv =

|Pr[($E_{pk}(\beta)$,R) ← Malice(**v**, desc(**v**),c^*)] - Pr[(c,R) ← ZK-Sim]|

NM-CPA Security

Or: semantic security with respect to relations under chosen-plaintext attack

Property 14.2: A cryptosystem is said to be NM-CPA secure if attacker’s advantage to mount a malleability attack on the cryptosystem does not increase in any PPT discernible way from that to simulate the attack without the ciphertext.

NM-CPA Security implies IND-CPA Security.

Similarly NM-CCA and NM-CCA2.