CSA E0 235: Cryptography April 6, 2015

Lecture 9

Instructor: Arpita Patra *Submitted by: Bharath Kumar*

1 Public key encryption - Algorithms

A public key Encryption Π = (Gen,Enc_{pk},Dec_{sk}) contains three PPT algorithms as follows

- $Gen(1^n)$: Given a security parameter 1^n it generates two keys , viz Public Key pk and private key sk.
- $Enc_{pk}(m)$: Given a message m and a public key pk , produces a cipher text c by encrypting message m using pk.
- $Dec_{sk}(c)$ Given a cipher text c and a private key sk, decrypts the cipher text c to message m .

In public key encryption there is a requirement that the decryption of encrypted messages yield valid messages even under the condition that the keys for encryption and decryption are different, i.e. $Dec_{sk}(Enc_{pk}(m)) = m$.
The security definition of public key Encryption states that the adversary should not be able to find the password except with a probability negligibly better than $\frac{1}{2}$.

2 CO attack on public Key Encryption PKE Π

The CO attack game on public key Encryption Π is as follows

- The public key pk is given to the CO adversary .
- The adversary comes up with to message m_0 and m_1 which is given to the challenger.
- The challenger chooses a message m_b to be encrypted where b is randomly chosen to be 0 or 1.
- The encrypted message m_b in the form of c_b is forwarded to adversary.
- The adversary has to predict b with probability negligibly better than $\frac{1}{2}$ to win the game.

Π is COA-secure if for every PPT adversary A taking part in the above game, the probability that A wins the experiment is at most negligibly better than $\frac{1}{2}$

$$Pr[PubK^{COA}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(\cdot) \tag{1}$$

3 Difference between CO security of SKE and PKE

1. Unlike SKE the public key pk is given to adversary before the challenge in PKE.
2. This gives adversary, the power of encryption oracle Enc_{pk}(m) where he can encrypt enormous messages for his analysis.
3. The adversary can encrypt m_0 and m_1 which are challenge messages.
4. The challenger encrypts m_b with the same key pk which is already known to adversary.
5. Hence CO security of PKE encompasses CPA security.
6. So this scheme of encryption is not safe of small message space as adversary can maintain a table of encryption for messages to compare and find the encrypted message.

4 Multiple message CPA secuirty of PKE

Unlike the CPA security game of SKE , here, given a pair of message, { ($m_{0,1}$, $m_{1,1}$) ,($m_{0,2}$, $m_{1,2}$)...($m_{0,t}$, $m_{1,t}$)}, the challenger will encrypt $m_{b,i}$ for each $1 \leq i \leq t$ belonging to above tuple where b=0 or 1 and b is held to one and only one value through out the game . If b=0 then we say that the challenger is encrypting $m_{0,i}$ or using left oracle and if b=1 we say then the right oracle is used or message $m_{1,i}$ is encrypted . Let the encryption oracle be depicted by $LR_{pk,b}$. The Multi message CPA game is defined as follows:-

- The public key pk is given to the Multi message CPA adversary.
- The challenger randomly selects b to be 0 or 1 to choose the encryption oracle.
- The adversary now forwards ($m_{0,i}$, $m_{1,i}$) for each $1 \leq i \leq t$ to which the challenger encrypts $m_{b,i}$ based on b value . The cipher text $c_i = Enc_{pk}(m_{b,i})$ is sent to adversary .
- The game ends with adversary predicting b. If he guesses $b^{'}$= b then he wins or else he loses . Actually the adversary is trying to guess which of the oracle (left or right) was used by challenger to encrypt the message

Π is Multiple message CPA-secure if for every PPT adversary A taking part in the above game the probability that A wins the experiment is at most negligibly better than $\frac{1}{2}$

$$Pr[PubK_{A,\Pi}^{cpa-mult}(n) = 1] \leq \frac{1}{2} + negl(\cdot) \tag{2}$$

Theorem 1 If Π is CPA secure , then it is also CPA -Multi secure

5 Proof

Let $LR_{PK,0}$ denote left oracle which always encrypts message m_0 and $LR_{PK,1}$ denote right oracle which always encrypts message m_1. The attacker is given access to a left-to-right oracle $LR_{PK,b}$ that, on input a pair of equal length messages m_0,m_1, computes the cipher text c $\leftarrow Enc_{pk}(m_b)$ and returns c. Then we say that Π is CPA - Multi secure if the probability that the distinguisher distinguishes between $LR_{PK,0}$ and $LR_{PK,1}$ is negligible.

$$|Pr[A^{LR_{PK,0}}(n) = 1] - Pr[A^{LR_{PK,1}}(n) = 1]| \leq negl(n) \tag{3}$$

This can be proved by a hybrid argument . Let us define intermediate LR oracles which encrypt t message tuples ($m_{0,i}$ and $m_{1,i}$) for each $1 \leq i \leq t$ in following manner:-

- Let LR^0_{PK} define an oracle which encrypts upto 0 m_0 (left) messages and and t m_1 (right) messages.
- Let LR^1_{PK} define an oracle which encrypts upto 1 m_0 (left) messages and and t-1 (right) m_1 messages .
- Similarly Let LR^t_{PK} define an oracle which encrypts upto t m_0 (left) messages and and 0 m_1 (right) messages.
- Now we can define LR^i_{PK} as an oracle which encrypts upto i m_0 (left) messages and and t-i m_1 (right) messages.

Hence we have the probability of distinguishing between any two consecutive oracle given as

$$|Pr[A^{LR^i_{PK}}(n) = 1] - Pr[A^{LR^{i-1}_{PK}}(n) = 1]| \leq negl(n) for 1 \leq i \leq t \tag{4}$$

Since we have t such oracles we will have t such equations of (4) . Adding all t equations we get

$$|Pr[A^{LR^0_{PK}}(n) = 1] - Pr[A^{LR^t_{PK}}(n) = 1]| \leq t \cdot negl(n) \tag{5}$$

Now that we have concluded that the distinguish-ability between $LR_{PK,0}$ and $LR_{PK,1}$ should be negligible, we need to prove that by contradiction if this distinguish-ability is not negligible, i.e. Π is not CPA- Multi secure, then Π is not CPA secure. Following is the proof.
Lets assume that Π is not CPA-Multi secure. Then we can build a adversary $A^{'}$ to break CPA security of Π using A which breaks CPA-Multi security.
If Π is not CPA-Multi secure , then we have a adversary A such that for some i

$$|Pr[A^{LR^i_{PK}}(n) = 1] - Pr[A^{LR^{i-1}_{PK}}(n) = 1]| \geq negl(n) \tag{6}$$

We build adversary $A^{'}$ as follows:-

- 1 $A^{'}$, given pk, chooses a uniform index i = {1, . . . , t}.
- 2 $A^{'}$ runs A(pk), answering its j^{th} oracle query ($m_{0,j}$ and $m_{1,j}$) as follows:

- (a) For $j < i$, adversary $A^{'}$ computes $c_j = Enc_{pk}(m_{0,j})$ and returns c_j to A as the response from its oracle.
- (b) For j = i, adversary $A^{'}$ outputs ($m_{0,j}$ $m_{1,j}$) to challenger and receives back a challenge cipher text c_j. This is returned to A as the response from its oracle.
- (c) For $j > i$, adversary $A^{'}$ computes $c_j = Enc_{pk}(m_{1,j})$ and returns c_j to A as the response from its oracle.

- 3 $A^{'}$ outputs the bit $b^{'}$ that is output by A.

Clearly if challenger has encrypted $m_{0,j}$ message then $A^{'}$ predicts LR^{i}_{PK} as output oracle stating $b^{'}$=0 and if challenger has encrypted $m_{1,j}$ message then $A^{'}$ predicts LR^{i-1}_{PK} as output oracle stating $b^{'}$=1 and thus thereby breaking CPA security .
But this is a contradiction because we already know that Π is CPA secure .Hence Π is also CPA-Multi Secure. Hence we can conclude that if Π is CPA secure, then it is also CPA-Multi secure.

6 Comparison of SKE and PKE security

In SKE COA Security doesn't imply COA multi secuirty and COA multi security doesn't imply CPA secuirty.
But in PKE COA security implies COA multi security as well as CPA security and CPA security imply CPA- Multi security.
Hence Given CPA secure PKE scheme for small messages, we can construct CPA-secure PKE for a long message . This can be achieved by converting a long message M into vector of small messages such that M = (m_0,m_1 ,....,m_n). Following figure illustrates the same for a vector of 6 messages.

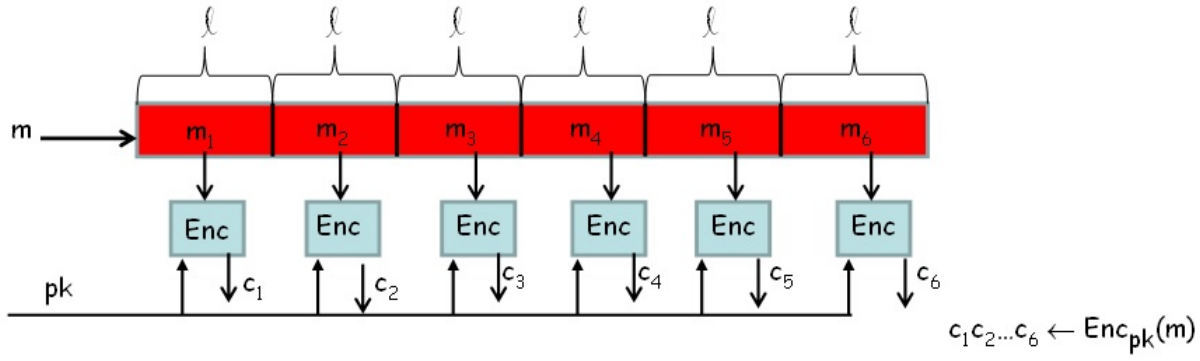

Fig: CPA secure PKE for long messages

It is necessary to note that if Π is CPA secure it doesn't necessarily be CCA secure.

7 EL Gamal public encryption scheme

Let G be a polynomial time aglorithm that takes an input 1^n and outputs a description of cyclic group , its order q and a generator g. Then El Gamal encryption scheme is described as follows.

- **Gen:** On input 1^n run G(1^n) to obtain ($\mathbb{G}$, q, g). The choose a uniform $x \in \mathbb{Z}_q$ and compute h := g^x. The public key is ($\mathbb{G}$, q, g,h) and the private key is ($\mathbb{G}$, q, g,x). The message space is $\mathbb{G}$.
- Enc_{pk}**(m):** On public key pk = ($\mathbb{G}$, q, g,h) and a message $m \in \mathbb{G}$, choose a uniform $y \in \mathbb{Z}_q$ and output the cipher text $(g^y, h^y \cdot m)$.
- $Dec_{sk}(c_1, c_2)$**:** On private key sk = ($\mathbb{G}$, q, g,x) and a cipher text c_1, c_2 , output $\hat{m} = c_2/c_1^x$.

Theorem 2 *If the DDH problem is hard relative to ($\mathbb{G}$, o), then El Gamal encryption scheme is CPA-secure*

In DH public encryption scheme given g^z to adversary he cannot distinguish k =g^{xy} when $\mathbb{G}$ is hard in DDH, where $\mathbb{G}$ is a cyclic group of prime order and g is a generator of $\mathbb{G}$. Here the key k perfectly masks message m through k $\cdot$ m mod q. Note that q is the order of $\mathbb{G}$.
The El Gamal encryption scheme extends this DDH protocol where given g^x , g^y and some random group element g^z , the adversary is unable to distinguish the mask g^{xy} .If an random element g^z was used for masking, then the encryption perfectly hides m . So even an unbounded powerful adversary will have no clue about the message

8 Security proof of EL Gamal public encryption scheme

Theorem 3 *If DDH is hard, then* Π *is a CPA-secure scheme.*

Proof : Assume by contradiction Π is not CPA-secure scheme.Then,

$$|Pr[D(\mathsf{DDH\ tuple}) = 1] - Pr[D(\mathsf{Non-DDH\ Tuple}) = 1]| \geq negl(n) \tag{7}$$

Let there exist an adversary A which can break CPA security with a probability more than $\frac{1}{2}$, i.e.

$$Pr[PubK^{CPA}_{A,\Pi}(n) = 1] \geq \frac{1}{2} + negl(n) \tag{8}$$

Note that For any z, Pr[$g^z \cdot$ m = $g^{z'}$] = 1/ $|G|$ when z is chosen uniformly from G , i.e.

$$Pr[PubK^{CPA}_{A,\Pi}(n) = 1] = \frac{1}{2} \tag{9}$$

Then we can build a adversary $A^{'}$ which can distinguish between a DDH and non DDH tuple as follows.

- Provide A with pk which contains $\{\mathbb{G}$,o,g, $g^x\}$.
- Receive two messages m_0 and m_1 from A , randomly select m_b where b can be 0 or 1 and forward this to challenger.
- The challenger masks message m_b with g^z and forwards $\{g^y, g^z \cdot m_b\}$ to adversary A', which is forwarded to A.
- At the end of the game A forwards $b^{'}$ to $A^{'}$. If b=$b^{'}$ the adversary $A^{'}$ has distinguished between DDH and non DDH tuple with a probability which is more than negligible or else otherwise.