Notion Of Security

Dibyendu Mallik Sabyasachi Karati

February 18, 2009

1 Introduction.

In this chapter we compare the relative strengths of various notion of security for public key encryption. We want to understand which definition of security imply which others. We start by sorting out some the notion we will consider.

2 Notion.

A convenient way to organize definitions of secure encryption is by considering separately the various possible goals and various possible attack models.

2.1 Goals

2.1.1 Indistingushability

It formalizes an adversary's inability to learn any information about plaintext x underlying a challenge ciphertext y. In this notion the adversary cannot determine from which plaintext the challenge ciphertext came from.

2.1.2 Non-malleability

It formalizes an adversary's inability to find a ciphertext y_1,given a ciphertext y,such that the underlying plaintexts x_1 and x are related in some way,(eg. $x = x_1 + 1$)

2.2 Attack Models

2.2.1 Chosen Plaintext Attack(CPA).

2.2.2 Non-Adaptive Chosen Ciphertext Attack(CCA1)

Here the adversary has an access to decryption oracle O. But the adversary can use this oracle only before it gets the challenge ciphertext y, ie. the query to the oracle should not depend on the ciphertext y.

2.2.3 Adaptive Chosen Ciphertext Attack(CCA2)

Adversary has an access to the decryption oracle O and his query to the oracle may depend on the challenge ciphertext y. Only restriction is that the adversary cannot query the oracle to decrypt the y .(the challenge ciphertext).

3 Relations.

One can mix-and-match the goals {IND,NM} and attacks {CPA,CCA1,CCA2} in any combination,given rise to six notions of security.

- ***IND-Atk:*** IND-CPA,IND-CCA1,IND-CCA2.
- ***NM-Atk :*** NM-CPA,NM-CCA1,NM-CCA2.

For each pair of notion A,B belongs to IND-CPA,IND-CCA1,IND-CCA2,NM-CPA,NM-CCA1,NM-CCA2 we show one of the following :-

- $\boldsymbol{A \Rightarrow B}$: A proof that if PE is any encryption scheme meeting notion of security A then PE also meets the notion of security B.
- $\boldsymbol{A \not\Rightarrow B}$: There exists an encryption scheme A that meets the security notion of A but does no meet the notion of security of B.

4 Framework.

In formalizing both IND-Atk and NM-Atk we regard an adversary A as a pair of probabilistic polynomil time algorithm A=(A_1A_2). A runs in two stages. A_1 generates a message pair,encrypt one of them and send to A_2 as challenge ciphertext. We say A_2 is successful depending on its goal:

- ***Goal for IND-X sense :*** It has to tell $\frac{0}{1}$ which message is in encrypted form.
- ***Goal for NM-X sense :*** It has to return a ciphertext y_1 given y,where the underlying plaintexts are related.

5 Formal Definitions.

5.1 Indistinguishability:

A public key scheme *(E,D,G)* is (t,q,ϵ) secure in IND-Atk sense if for all pair of different messages of same length and any adversary A, that runs in time t and makes atmost q queries the oracle O, ϵ(n) denotes the advantage of the algorithm over a random guess.

$$\Pr_{(p_k,s_k)\leftarrow G(n)}[A^O(p_k, E_{p_k}, (m_1) = 1)] - \Pr_{(p_k,s_k)\leftarrow G(n)}[A^O(p_k, E_{p_k}, (m_0) = 1)] \leq \epsilon(n)$$

where the oracle is:

$$O = \begin{cases} - & \text{if IND-CPA} \\ D_{sk} & \text{if IND-CCA2} \end{cases}$$

and the adversary cannot query the decryption oracle at $E_{p_k}(m_i)$

5.2 Non-Malleability:

A public key scheme *(E,D,G)* is (t,q,ϵ) secure in NM-Atk sense if for all message distribution M,and all relation R:MxM → {0,1},and for every adversary A that runs in time t and makes at most q queries to the oracle O,then there exists another adversary A_1 which runs in poly(t),then the following holds.

$$\Pr_{(p_k,s_k)\leftarrow G(n),m}[R(m, D_{sk}(A^O(p_k, E_{p_k}(m)))] - \Pr_{(p_k,s_k)\leftarrow G(n),m}[R(m, D_{sk}(A'(p_k)))] \leq \epsilon(n)$$

where the oracle is:

$$O = \begin{cases} - & \text{if NM-CPA} \\ D_{sk} & \text{if NM-CCA2} \end{cases}$$

and the adversary cannot query the decryption oracle at $E_{p_k}(m)$

6 Relation NM-X ⇒ IND-X

If a public-key scheme is (t,q,ϵ)-secure in NM-X sense, then it is (t,q,2ϵ)-secure in IND-X sense.

Contradict that the scheme is (t,q,2ϵ)-secure in IND-X sense. Show that the scheme is also not (t,q,ϵ)-secure in NM-X sense.

Proof: Let us assume that the scheme is not IND-X secure.

There exists messages $m_0 = m_1$ and an adversary A^O , st :

$$\underset{(p_k,s_k)}{\Pr}[A^O(p_k, E_{p_k}(m_1)) = 1] - \underset{(p_k,s_k)}{\Pr}[A^O(p_k, E_{p_k}(m_1)) = 1] > 2\epsilon(n)$$

We need to prove that there exists B for which there exists a R, so that for all B':

$$\underset{(p_k,s_k),m}{\Pr}[R(m, D_{sk}(B^O(p_k, E_{p_k}(m)))] - \underset{(p_k,s_k),m}{\Pr}[R(m, D_{sk}(B'(p_k)))] > \epsilon(n)$$

Note:

$$\underset{(p_k,s_k),i\in\{0,1\}}{\Pr}[R(m_i, D_{sk}(B'(p_k)))] = \frac{1}{2}$$

$$Consider, R(u,v) = \begin{cases} 1 & \text{u = v} \\ 0 & \text{u} \neq \text{v} \end{cases}$$

and $B^O(p_k, c) = E_{p_k}(m_{A^O(p,c)})$

Thus,

$$\underset{(p_k,s_k),i\in\{0,1\}}{\Pr}[R(m_i, D_{sk}(B^O(p_k, E_{p_k}(m_i)))]$$

$$= \underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[m_i = D_{sk}(B^0(p_k, E_{p_k}(m_i)))]$$

$$= \underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^0(p_k, E_{p_k}(m_i)) = i]$$

$$= \frac{1}{2}\underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^0(p_k, E_{p_k}(m_0)) = 0] + \frac{1}{2}\underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^O(p_k, E_{p_k}(m_1)) = 1]$$

$$= \frac{1}{2}(1 - \underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^0(p_k, E_{p_k}(m_0)) = 1]) + \frac{1}{2}\underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^O(p_k, E_{p_k}(m_1)) = 1]$$

$$= \frac{1}{2} + (\underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^0(p_k, E_{p_k}(m_1)) = 1] - \underset{(p_k,s_k),m\in\{0,1\}}{\Pr}[A^0(p_k, E_{p_k}(m_0)) = 1])$$

$$= \frac{1}{2} + Adv[A^O]$$

Thus, LHS = Adv[A^O] > ϵ(n), by our assumption.

Thus the assumption leads to a successful adversary against the Encryption in the NM-X sense.

7 A Separation :

IND-CPA $\not\Rightarrow$ NM-CPA.

Suppose, we have (E,D,G) which satisfies IND-CPA.

Consider, $E'(p_k\ ) = 0 \parallel E_{p_k}(x)$.

Thus, $D'_{s_k}(b \parallel y) = D_{s_k}(y)$

(E', D', G) is also an IND-CPA scheme.

It may be shown that $(E', D'G)$ is not IND-NM.

Informally, the IND-NM adversary is provided with $0 \parallel y$ and is asked to produce another ciphertext, whose corresponding plaintext is related to the original plaintext. With probability 1, the adversary can make the first bit 1 and obtain $1 \parallel y$, whose corresponding plaintext is the the same as that corresponding to the challenge.

Thus adversary $A(p_k, E'_{p_k}(m))$ outputs $1 \parallel y$, where $y = E_{p_k}(m)$.

For an adversary A' who does not have access to $E'_{p_k}(m)$, its probability of guessing 0 or 1 is $\frac{1}{2}$.

Thus, $Adv[A^{NM-CPA}] = 1 - \frac{1}{2} = \frac{1}{2}$.