Relations Among Notions of Security for Public-Key Encryption Schemes

Debdeep Mukhopadhyay
IIT Kharagpur

Notions

- To organize the definitions of secure encryptions
- Classified depending on:
  - security goals:
    - Indistinguishability (GM) (Goldwasser-*Micali*)
    - Non-malleability (DDN), (*Dolev, Dwork, Naor*)
  - attack models:
    - Chosen Plain Text (CPA)
    - Non-adaptive Chosen Ciphertext (CCA1)
    - Adaptive Chosen Ciphertext (CCA2)

Relations

- One can mix and match the goals (IND,NM) and the attack models (CPA, CCA1, CCA2)
  - thus there are 6 notions of security
    - IND-X: IND-CPA, IND-CCA1, IND-CCA2
    - NM-X: NM-CPA, NM-CCA1, NM-CCA2

Non-malleability

- Danny Dolev, Cynthia Dwork and Moni Naor, “Non-malleable Cryptography”, Siam J of Computing, 2000.

Motivation

- Consider a bidding scheme.
- Company A gives a bid of say Rs 10,000.
- It communicates to the arbiter by using a Public Key Infrastructure (PKI), E(10000)
- Another company B, should not be able to compute a bid value say E(x), st. x<10000 more likely than when B does not have a knowledge of E(10000).

Other Motivations

- For key agreement protocols like Kerberos, after the mutual key K_{AB} is agreed there is an exchange of nonces, N.
- One party sends to the other $E_{KAB}(N)$ and expects $E_{KAB}(N-1)$.
  - the assumption being that without KAB it is not feasible to compute N-1 (or any f(N)) with a probability better than without having the knowledge of the ciphertext of N with KAB).

Informally

- Informally, given the CT it is no easier to generate a different CT, so that the corresponding PTs are related, than it is to do with out the ciphertext.

Indistinguishability

- A public key scheme (E,D,G) is (t,q,ε)-secure in the IND-X sense if for all pairs of different messages of the same length, and for every adversary A that runs in time t and makes at most q queries to oracle O:

$$\Pr_{(p_k,s_k)}[A^O(p_k, E_{p_k}(m_1)=1)] - \Pr_{(p_k,s_k)}[A^O(p_k, E_{p_k}(m_0))=1] \le \varepsilon(n)$$

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 $E_{p_k}(m_i)$

CCA1 vs CCA2

- Imagine all the algorithms $A=(A_1,A_2)$, both of which are also polytime algorithms in n.
- A_1 generates a message pair and encrypts one of them and gives it to A_2 as a challenge.
- A_2 has to be successful against the challenge, depending on the goal:
  - IND: It has to tell message 0/1 which has been encryptes.
  - NM: It has to return a ciphertext whose corresponding message is related to the plaintext encrypted.

Inter-relation

- IND-CCA2=>IND-CCA1=>IND-CPA≡SS

Non-Malleability

- A public-key scheme (E,D,G) is (t,q,ε)-secure in the NM-X sense if for all message distributions M, and all relations R:MxM→{0,1}, and for every adversary A that runs in time t, and makes at most q queries to oracle O, there exists another adversary A' that runs in time poly(t), st:

$$\Pr_{(p_k,s_k),m}[R(m, D_{s_k}(A^O(p_k, E_{p_k}(m)))] - \Pr_{(p_k,s_k),m}[R(m, D_{s_k}(A'(p_k)))] \le \varepsilon(n)$$

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 $E_{p_k}(m)$

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.

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

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

$\Pr_{(p_k,s_k)}[A^O(p_k, E_{p_k}(m_1) = 1)] - \Pr_{(p_k,s_k)}[A^O(p_k, E_{p_k}(m_0)) = 1] > 2\varepsilon(n)$

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

$\Pr_{(p_k,s_k),m}[R(m, D_{s_k}(B^O(p_k, E_{p_k}(m)))] - \Pr_{(p_k,s_k),m}[R(m, D_{s_k}(B'(p_k)))] > \varepsilon(n)$

$Note: \Pr_{(p_k,s_k),i\in\{0,1\}}[R(m_i, D_{s_k}(B'(p_k)))] = 1/2$

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

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

$Thus, \Pr_{(p_k,s_k),i\in\{0,1\}}[R(m_i, D_{s_k}(B^O(p_k, E_{p_k}(m_i)))] =$

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

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

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

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

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

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

$Thus, LHS = Adv[A^O] > \varepsilon(n),$ by our assumption. Thus the assumption leads to a successful adversary against the Encryption in the NM-X sense.

A Separation

$IND-CPA \neq> NM-CPA$

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

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

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

(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||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 $1\|y$, whose corresponding plaintext is the the same as that corresponding to the challenge.

Thus adversary $A(p_k, E'_{p_k}(m))$ outputs 1||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 1/2.

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

Another Separation

$IND-CPA \not=> IND-CCA2$

$Consider:\ \mathrm{E(m)=x^3(mod\ \ n)||s||x.s \oplus m}$

If the RSA function is a one-way function,

then E(x) is a IND-CPA scheme.

But, this is clearly not an IND-CCA2 scheme.

Why?

Equivalence of NM-CCA2 and IND-CCA2

- We have proved NM-CCA2=>IND-CCA2
- We have to prove that IND-CCA2=>NM-CCA2
- We shall assume there is an adversary in the NM-CCA2 sense. We shall construct an adversary in the IND-CCA2 sense.

Suppose there is an $(t,q,\varepsilon)-$adversary in the NM-CCA2 sense against the scheme E_{p_k}.

That is there exists a message distribution M and a relation $R: M \times M \to \{0,1\}$ such that for all simulators S running in polynomial time t:

$\Pr[R(m, A(p_k, E_{p_k}(m))] - \Pr[R(m, S(p_k))] > 2\varepsilon(n)$

Modify A

Adversary $B(p_k, E_{p_k}(m))$, where $m \in \{m_0, m_1\}$

Run $A^{D_{s_k}}(p_k, E_{p_k}(m))$ and assign to y

If $R(m_0, D_{s_k}(y))$

  return 0

else

  return $r \in_R \{0,1\}$

Proof (contd.)

Simulator $S(p_k)$

Generate $m'' \leftarrow M$

Return $\mathrm{A}^{\mathrm{D}_{s_k}}(p_k, E_{p_k}(m''))$

Now A is a good adversary in NM-CCA2 sense. Thus,

$\Pr_{(p_k,s_k),m}[R(m, D_{s_k}(A^O(p_k, E_{p_k}(m)))] - \Pr_{(p_k,s_k),m}[R(m, D_{s_k}(S(p_k)))] > 2\varepsilon(n)$

Let, $p = \Pr_{(p_k,s_k),m}[R(m, D_{s_k}(A^O(p_k, E_{p_k}(m)))]$

and $p' = \Pr_{(p_k,s_k),(m,m')}[R(m, D_{s_k}(A^O(p_k, E_{p_k}(m')))]$

$= \Pr_{(p_k,s_k),m}[R(m, D_{s_k}(S(p_k))]$

So, we have $p - p' > 2\varepsilon(n)$

Now, $\Pr_{p_k,s_k}[B(p_k, E_{p_k}(m_0)) = 0] = \Pr_{(p_k,s_k)}[R(m_0, D_{s_k}(A(p_{k_i}, E_{p_k}(m_0))))]$

$+\frac{1}{2}\Pr_{(p_k,s_k)}[\text{not } R(m_0, D_{s_k}(A(p_{k_i}, E_{p_k}(m_0))))$

$= p + \frac{1}{2}(1-p)$

$\Pr_{p_k,s_k}[B(p_k, E_{p_k}(m_1)) = 0] = \Pr_{(p_k,s_k)}[R(m_0, D_{s_k}(A(p_{k_i}, E_{p_k}(m_1))))]$

$+\frac{1}{2}\Pr_{(p_k,s_k)}[\text{not } R(m_0, D_{s_k}(A(p_{k_i}, E_{p_k}(m_1))))$

$= p' + \frac{1}{2}(1-p')$

Thus, $\text{Adv}[\text{B}^{\text{O}}(p_k)] = \text{p} + \frac{1}{2}(1-p) - \text{p}' + \frac{1}{2}(1-p') = \frac{1}{2}(p-p') > \varepsilon(n)$

This completes the proof.

Inter-relationship