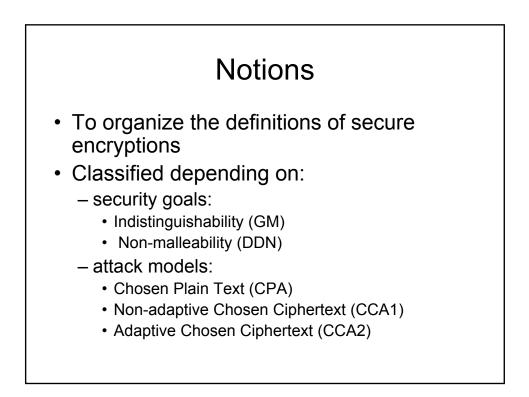
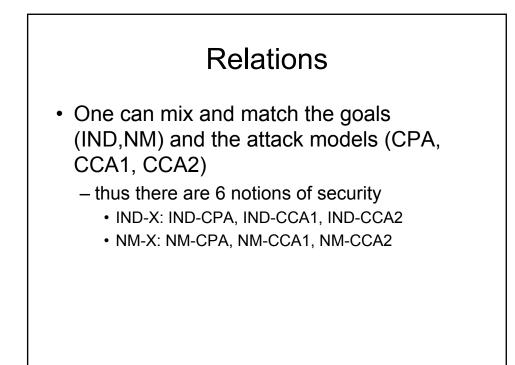
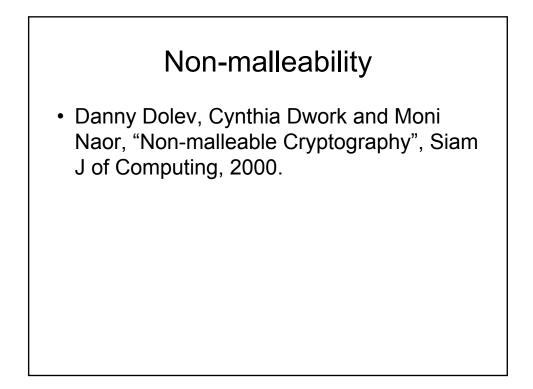
Relations Among Notions of Security for Public-Key Encryption Schemes

> Debdeep Mukhopadhyay IIT Kharagpur

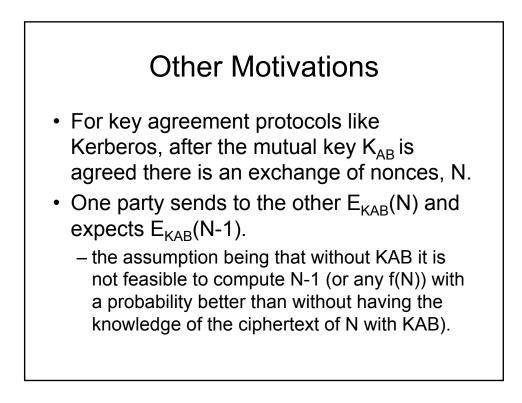






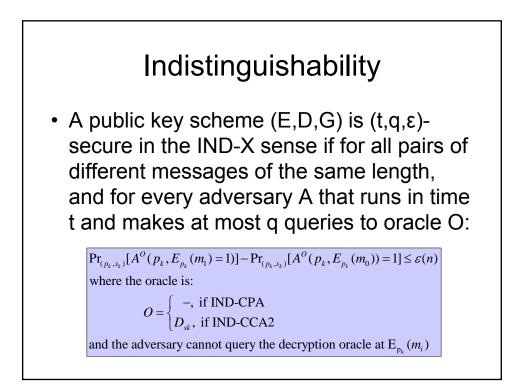
## Motivation

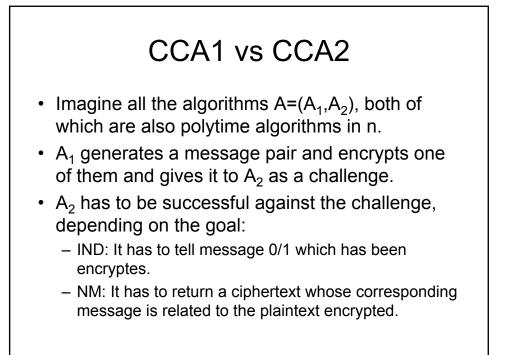
- Consider a bidding scheme.
- Company A gives a bit of say Rs 10,000.
- It communicates to the arbiter by using a Public Key Infrastructure (PKI), E(10000)
- Another company B, should not able to compute a bid value say E(x), st. x<10000 more likely than when B does not have a knowledge of E(10000).

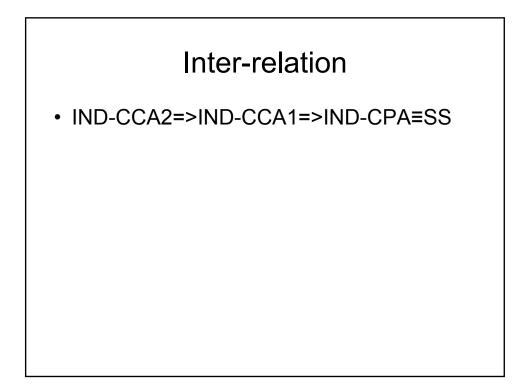


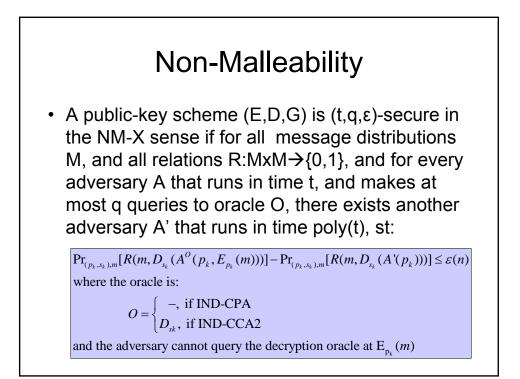
# Informally

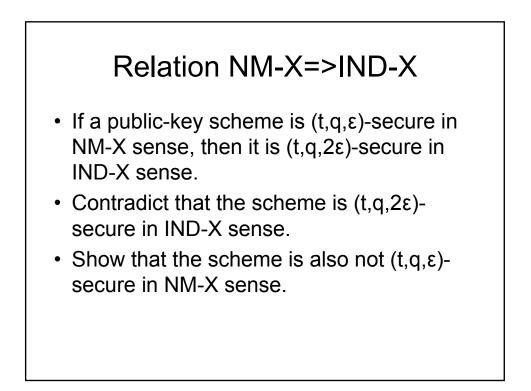
• Informally, given the CT it is no easier to generate a different CT, so that the corresponding PTs are related, than it is do with out the ciphertext.











Let us assume that the scheme is not IND-X secure.	
There exists messages $m_0 = m_1$ and an adversary $A^0$ , st :	
$\Pr_{(p_k,s_k)}[A^{\mathcal{O}}(p_k, E_{p_k}(m_1) = 1)] - \Pr_{(p_k,s_k)}[A^{\mathcal{O}}(p_k, E_{p_k}(m_0)) = 1] > 2\varepsilon(n)$	
We need to prove that there exists B for which there exists a R, so that	
for all B':	
$\Pr_{(p_k,s_k),m}[R(m, D_{s_k}(B^O(p_k, E_{p_k}(m)))] - \Pr_{(p_k,s_k),m}[R(m, D_{s_k}(B'(p_k)))] > \varepsilon(n)$	
<i>Note</i> : $\Pr_{(p_k, s_k), i \in \{0,1\}}[R(m_i, D_{s_k}(B'(p_k)))] = 1/2$	
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, $\Pr_{(p_k, s_k), i \in [0,1]}[R(m_i, D_{s_k}(B^O(p_k, E_{p_k}(m_i)))] =$	
$= \Pr_{(p_k, s_k), m \in [0,1]}[m_i = D_{s_k}(B^O(p_k, E_{p_k}(m_i)))]$	
$= \Pr_{(p_k, s_k), m \in [0,1]} [A^{o}(p_k, E_{p_k}(m_i)) = i]$	
$=\frac{1}{2}\mathrm{Pr}_{(p_{k},s_{k}),m\in[0,1]}[A^{o}(p_{k},E_{p_{k}}(m_{0}))=0]+\frac{1}{2}\mathrm{Pr}_{(p_{k},s_{k}),m\in[0,1]}[A^{o}(p_{k},E_{p_{k}}(m_{1}))=1]$	
$=\frac{1}{2}(1-\Pr_{(p_{k},s_{k}),m\in[0,1]}[A^{O}(p_{k},E_{p_{k}}(m_{0}))=1])+\frac{1}{2}\Pr_{(p_{k},s_{k}),m\in[0,1]}[A^{O}(p_{k},E_{p_{k}}(m_{1}))=1]$	
$= \frac{1}{2} + (\Pr_{(p_k, s_k), m \in [0,1]}[A^o(p_k, E_{p_k}(m_1)) = 1] - \Pr_{(p_k, s_k), m \in [0,1]}[A^o(p_k, E_{p_k}(m_0)) = 1])$	
$=\frac{1}{2}+Adv[A^{o}]$	
<i>Thus</i> , <i>LHS</i> = $Adv[A^o] > \varepsilon(n)$ , by our assumption. Thus the assumption leads	
to a successful adversary against the Encryption in the NM-X sense.	

	$IND - CPA \neq > NM - CPA$	
	Suppose, we have (E,D,G) which satisfies IND-CPA.	
	Consider, $E'(p_k) = 0 \parallel E_{p_k}(x)$	
	Thus, $D'_{s_k}(b \parallel y) = D_{s_k}(y)$	
A	(E',D',G) is also an IND-CPA scheme.	
Separation	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 $1 \parallel y$ , whose corresponding plaintext is the the same as	
	that corresponding to the challenge.	
	Thus adversary A( $p_k, E'_{p_k}(m)$ ) outputs 1  y, where y=E <sub><math>p_k(m)</math>.</sub>	
	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**

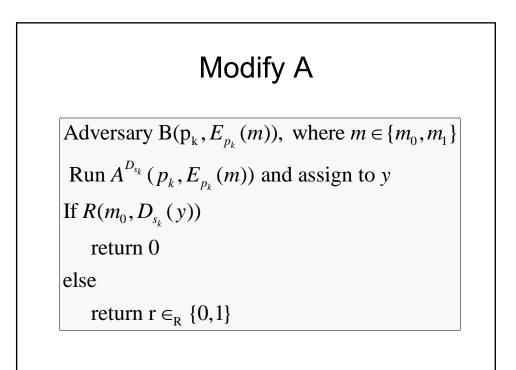
 $IND - CPA \neq > IND - CCA2$ 

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

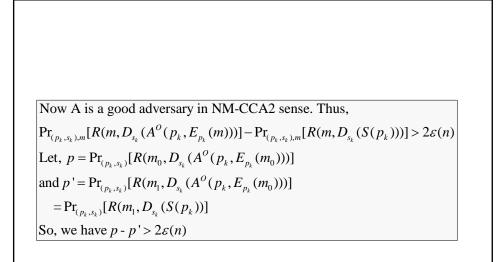
- We have proved NM-CCA2=>IND-CCA2
- We have to prove that IND-CCA2=>NM-CCA2
- We shall assume there is an adversary in the NM-CCA2 sense. We shall construct an adversary in the IND-CCA2 sense.

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  $R: M \times M \rightarrow \{0,1\}$  such that for all simulators *S* running in polynomial time *t*:  $\Pr[R(m, A(p_k, E_{p_k}(m))] - \Pr[R(m, S(p_k))] > 2\varepsilon(n)$ 



## Proof (contd.)

Simulator  $S(p_k)$ Generate  $m'' \leftarrow M$ Return  $A^{D_{s_k}}(p_k, E_{p_k}(m''))$ 



For IND-CCA2 we have an adversary B st.  $\begin{aligned} \Pr_{(p_{k},s_{k})}[B^{o}(p_{k},E_{p_{k}}(m_{1}))=0]-\Pr_{(p_{k},s_{k})}[B^{o}(p_{k},E_{p_{k}}(m_{0}))=0] &\leq \varepsilon(n) \\ \Pr_{(p_{k},s_{k})}[B^{o}(p_{k},E_{p_{k}}(m_{1}))=0]=\Pr_{(p_{k},s_{k})}[R(m_{0},D_{s_{k}}(A(p_{k_{i}},E_{p_{k}}(m_{1}))))] \\ &\quad +\frac{1}{2}\Pr_{(p_{k},s_{k})}[\operatorname{not} R(m_{0},D_{s_{k}}(A(p_{k_{i}},E_{p_{k}}(m_{1}))))] \\ &\quad =p'+\frac{1}{2}(1-p') \\ \Pr_{(p_{k},s_{k})}[B^{o}(p_{k},E_{p_{k}}(m_{0}))=0]=\Pr_{(p_{k},s_{k})}[R(m_{0},D_{s_{k}}(A(p_{k_{i}},E_{p_{k}}(m_{0}))))] \\ &\quad +\frac{1}{2}\Pr_{(p_{k},s_{k})}[\operatorname{not} R(m_{0},D_{s_{k}}(A(p_{k_{i}},E_{p_{k}}(m_{0}))))] \\ &\quad =p+\frac{1}{2}(1-p) \\ \\ \operatorname{Thus}, \operatorname{Adv}[\operatorname{B}^{o}(p_{k})]=p+\frac{1}{2}(1-p)-p'+\frac{1}{2}(1-p')=\frac{1}{2}(p-p') > \varepsilon(n) \\ \\ \operatorname{This completes the proof.} \end{aligned}$ 

