Cryptography

Lecture 10

Arpita Patra

Quick Recall and Today's Roadmap

>> CPA & CPA-mult security

>> Equivalence of CPA and CPA-mult security

>> El Gamal Encryption Scheme

>> Hybrid Encryption (PKE from PKE + SKE with almost the same efficiency of SKE)

>> Key Encapsulation Mechanism (KEM): Little sister of PKE

CPA Security

>> CPA-secure KEM + COA-secure SKE => CPA-secure PKE

>> CPA-secure KEM from HDH Assumption (close relative of DDH assumption)

>> CCA Security for PKE

>> Single message CCA implies Multi message CCA

>> CCA KEM

>> CCA KEM + CCA SKE => CCA PKE (Hybrid encryption)

Two worlds: PKE, SKE

PKE	SKE
>> No assumption of sh >> Very expensive	umption needed nall computation/less ion)

Best of the Both Worlds

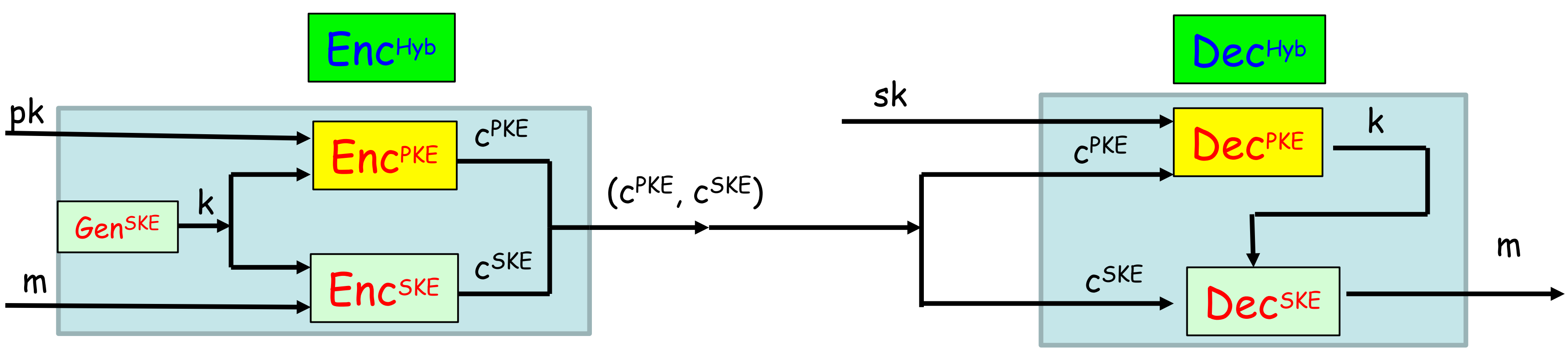
No shared-key assumption

Lightweight

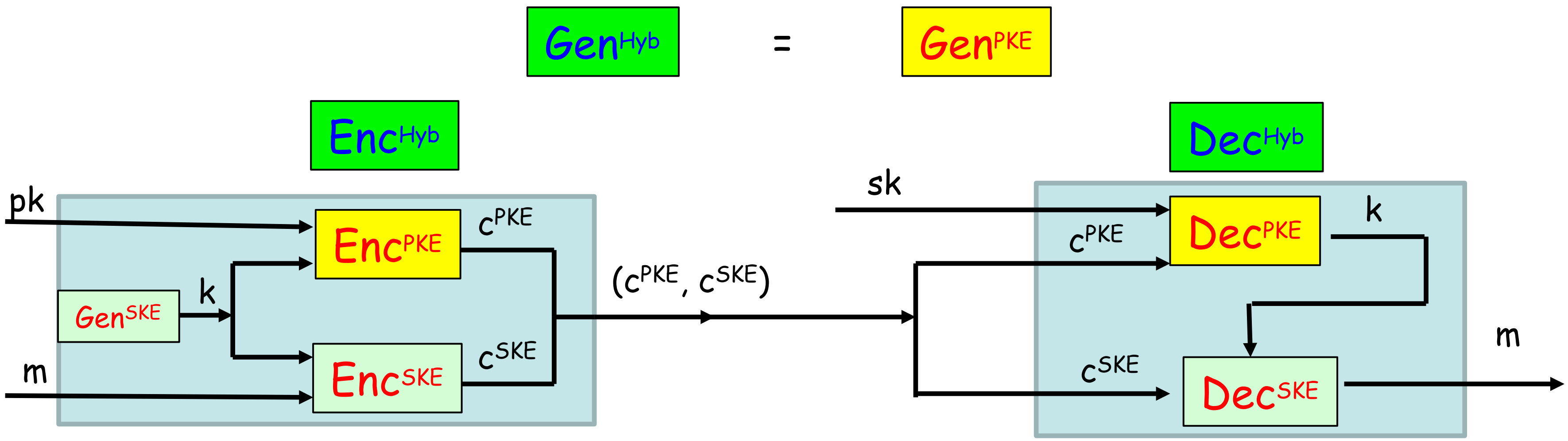
Hybrid Encryption= PKE + SKE

Gen^{PKE} Enc^{PKE} Dec^{PKE} Gen^{SKE} Enc^{SKE} Dec^{SKE}

Gen^{Hyb} = Gen^{PKE}



Advantage of Hybrid Encryption



|m|>>>>> |k| = n

α : Cost of encrypting 1 bit message using PKE
β : Cost of encrypting 1 bit message using SKE

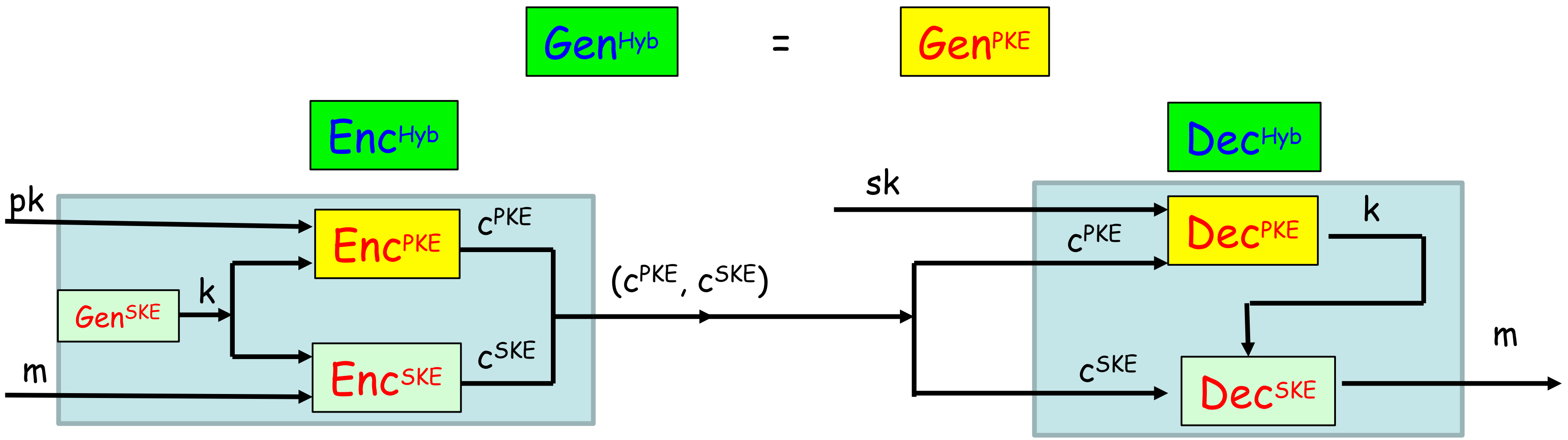
$$\alpha \approx \beta * 10^5$$

If PKE is used: α

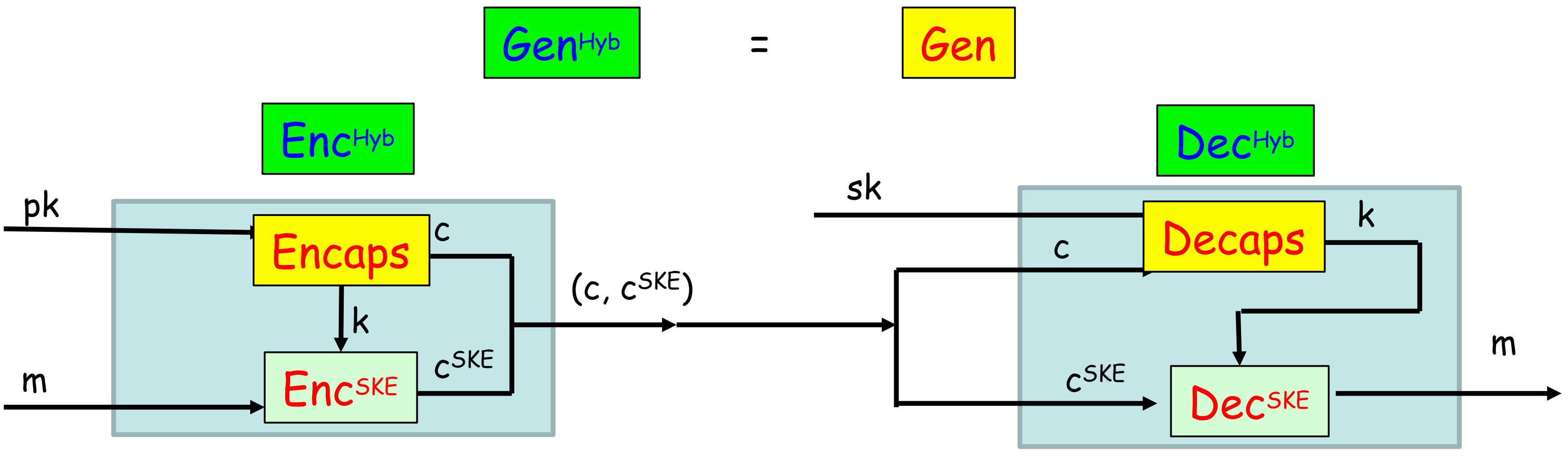
If Hybrid PKE is used: $\frac{n\alpha + |m|\beta}{|m|} = \frac{n\alpha}{|m|} + \beta$

Ciphertext Expansion??

Hybrid Encryption using KEM & DEM

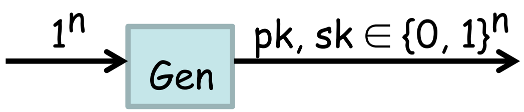


Hybrid Encryption using KEM & DEM



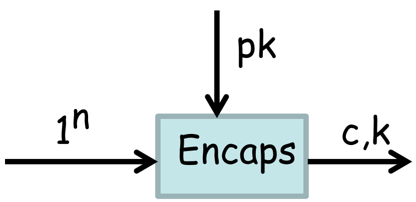
KEM: Syntax

- KEM is a collection of 3 PPT algorithms (Gen, Encaps, Decaps)



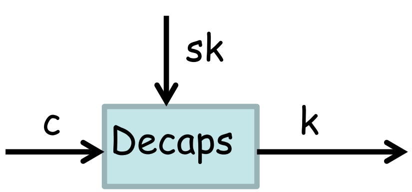
Syntax: $(pk, sk) \leftarrow Gen(1^n)$

Randomized Algo



Syntax: $(c,k) \leftarrow Encaps_{pk}(1^n)$

Randomized Algo



Syntax: $k := Dec_{sk}(c)$

Deterministic (w.l.o.g)

Except with a negligible probability over (pk, sk) output by $Gen(1^n)$, we require that if $Encaps(1^n)$ outputs (c,k) then

$Dec_{sk}(c) := k$

CPA Security for KEM

Indistinguishability experiment $KEM^{cpa}_{A,\Pi}(n)$

Π = (Gen, Encaps, Decaps)

PPT A

I can break Π

$(c,k) \leftarrow Encaps_{pk}(1^n)$

$k' \leftarrow k$ if b=0

$\leftarrow$ uniform random string, b =1

pk

(c,k')

b' $\in$ {0, 1}

b $\leftarrow$ {0, 1}

Let me verify $\leftarrow$ pk, sk $\leftarrow$ Gen(1^n)

(Attacker's guess about encapsulated key)

Game Output

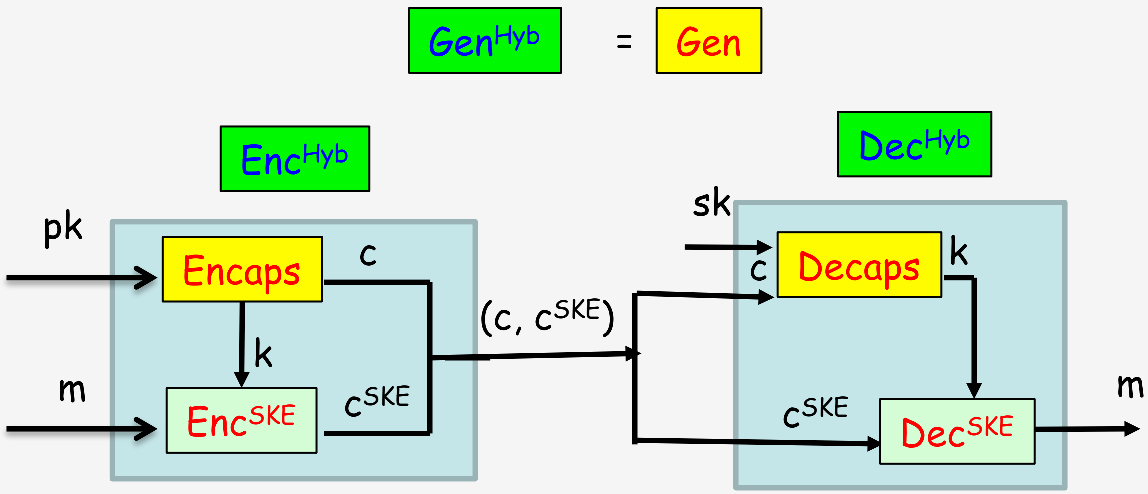
b = b' $\rightarrow$ 1 --- attacker won

b $\neq$ b' $\rightarrow$ 0 --- attacker lost

Π is CPA-secure if for every PPT attacker A, the probability that A wins the experiment is at most negligibly better than ½

$$\Pr\left[KEM^{cpa}_{A,\Pi}(n) = 1 \right] \leq \frac{1}{2} + negl(n)$$

CPA-Secure KEM + COA-Secure SKE -> CPA-secure PKE



Π = (Gen, Encaps, Decaps)

Π^{SKE} = (Gen^{SKE}, Enc^{SKE}, Dec^{SKE})

Π^{Hyb} = (Gen^{Hyb}, Enc^{Hyb}, Dec^{Hyb})

Theorem (Blum Goldwasser CRYPTO'84): Π is CPA-security KEM & Π^{SKE} is COA-secure SKE $\rightarrow$ Π^{Hyb} is CPA-secure PKE

Proof: Yet another Hybrid argument based Proof

$(pk, c, Enc_k^{SKE}(m_0))$

Indistinguishable due to CPA-security of KEM

$(pk, c, Enc_{k'}^{SKE}(m_0))$

Indistinguishable due to COA-security of SKE

$(pk, c, Enc_{k'}^{SKE}(m_1))$

Indistinguishable due to CPA-security of KEM

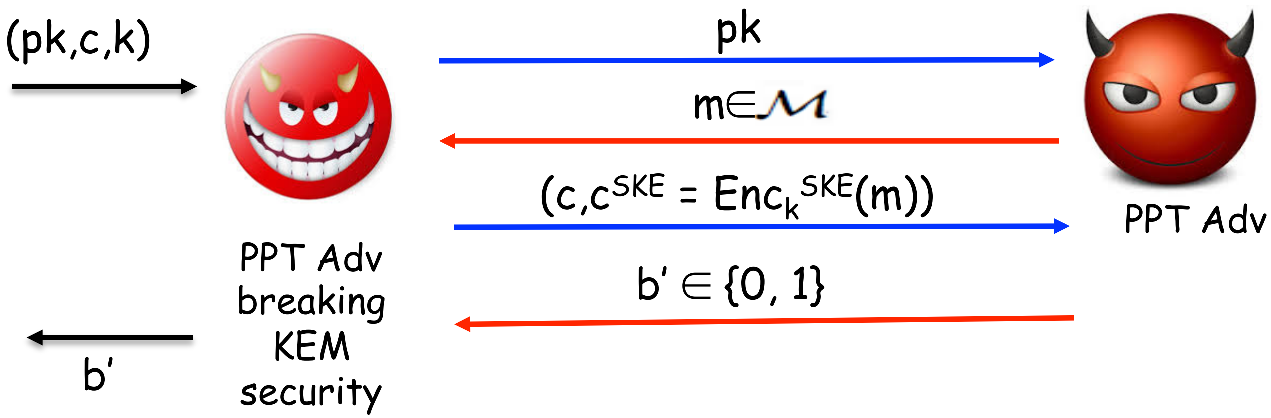
$(pk, c, Enc_k^{SKE}(m_1))$

CPA-Secure KEM + COA-Secure SKE -> CPA-secure PKE

Theorem: Π is CPA-security KEM & Π^{SKE} is COA-secure SKE $\rightarrow$ Π^{Hyb} is CPA-secure PKE

$(pk, c, Enc_k{}^{SKE}(m_0))$

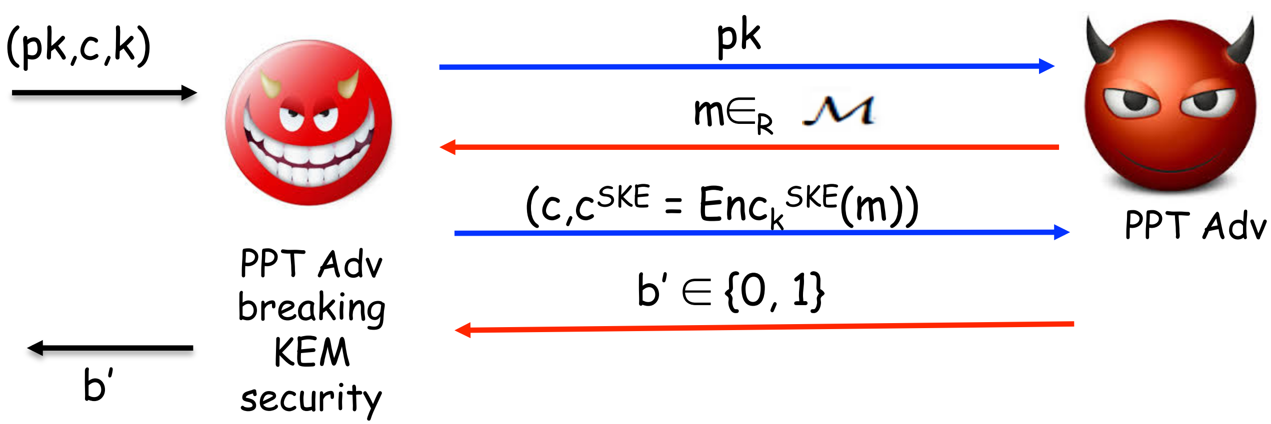
Encapsulated key or Random Key?



$(pk, c, Enc_{k'}{}^{SKE}(m_0))$

Encapsulated key or Random Key?

$(pk, c, Enc_{k'}{}^{SKE}(m_1))$



$(pk, c, Enc_k{}^{SKE}(m_1))$

CPA-Secure KEM + COA-Secure SKE -> CPA-secure PKE

Theorem: Π is CPA-security KEM & Π^{SKE} is COA-secure SKE $\rightarrow$ Π^{Hyb} is CPA-secure PKE

(pk,c, $Enc_k^{SKE}(m_0)$)

$$\left| \Pr[A(pk,c, Enc_k^{SKE}(m_0)) = 1] - \Pr[A(pk,c, Enc_{k'}^{SKE}(m_0)) = 1] \right| < negl(n)$$

$PrivK^{coa}_{A, \Pi^{SKE}}(n)$

$PubK^{cpa}_{A, \Pi}(n)$

Encyption of m_0 or m_1?

(pk,c, $Enc_{k'}^{SKE}(m_0)$)

m_0, m_1

c^{SKE}

b'

(pk,sk) <- Gen(1^n)

(c,k) <- $Encaps_{pk}(1^n)$

pk

$m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

(c,c^{SKE})

$b' \in \{0, 1\}$

PPT Adv

(pk,c, $Enc_{k'}^{SKE}(m_1)$)

$$\left| \Pr[A(pk,c, Enc_k^{SKE}(m_1)) = 1] - \Pr[A(pk,c, Enc_{k'}^{SKE}(m_1)) = 1] \right| < negl(n)$$

(pk,c, $Enc_k^{SKE}(m_1)$)

CPA-Secure KEM + COA-Secure SKE -> CPA-secure PKE

Theorem: Π is CPA-security KEM & Π^{SKE} is COA-secure SKE $\rightarrow$ Π^{Hyb} is CPA-secure PKE

$(pk, c, Enc_k^{SKE}(m_0))$

$$\left| \Pr[A(pk, c, Enc_k^{SKE}(m_0)) = 1] - \Pr[A(pk, c, Enc_{k'}^{SKE}(m_0)) = 1] \right| < negl(n)$$

$+$

$(pk, c, Enc_{k'}^{SKE}(m_0))$

$$\left| \Pr[A(pk, c, Enc_{k'}^{SKE}(m_0)) = 1] - \Pr[A(pk, c, Enc_{k'}^{SKE}(m_1)) = 1] \right| < negl'(n)$$

$(pk, c, Enc_{k'}^{SKE}(m_1))$

$+$

$$\left| \Pr[A(pk, c, Enc_{k'}^{SKE}(m_1)) = 1] - \Pr[A(pk, c, Enc_k^{SKE}(m_1)) = 1] \right| < negl(n)$$

$(pk, c, Enc_k^{SKE}(m_1))$

El Gamal like KEM

$\mathrm{Gen}(1^n)$

(G, o, q, g)

$h = g^x$. For random x

$pk = (G,o,q,g,h)$, $sk = x$

$\mathrm{Enc}_{pk}(m)$

$c_1 = g^y$ for random y

$c_2 = h^y . m$

$c = (c_1,c_2)$

$\mathrm{Dec}_{sk}(c)$

$c_2 / (c_1)^x = c_2 . [(c_1)^x]^{-1}$

$\mathrm{Gen}(1^n)$

(G, o, q, g)

$h = g^x$. For random x

$pk = (G,o,q,g,h)$, $sk = x$

$\mathrm{Encaps}_{pk}(1^n)$

$c = g^y$ for random y

$k = h^y = g^{xy}$.

(c,k)

$\mathrm{Dec}_{sk}(c)$

$k = c^x = g^{xy}$

El Gamal like KEM

Gen(1^n)

(G, o, q, g)

$h = g^x$. For random x

pk= (G,o,q,g,h), sk = x

Enc$_{pk}$(m)

$c_1 = g^y$ for random y

$c_2 = h^y . m$

$c = (c_1,c_2)$

- Need to choose m randomly
- Multiplication
- Ciphertext= 2 elements

Dec$_{sk}$(c)

$c_2 / (c_1)^x = c_2 . [(c_1)^x]^{-1}$

- Multiplication

Security: DDH Assumption

Gen(1^n)

(G, o, q, g)

$h = g^x$. For random x

pk= (G,o,q,g,h,H), sk = x

- No need of that
- No Multiplication, hashing
- Ciphertext= 1 element

Encaps$_{pk}$(1^n)

$c = g^y$ for random y

$k = H(h^y) = H(g^{xy})$

(c,k)

- No Multiplication, hashing

Dec$_{sk}$(c)

$k = H(c^x) = H(g^{xy})$

Security??

El Gamal like KEM

Gen(1^n)

(G, o, q, g)

h = g^x. For random x

pk= (G,o,q,g,h,H), sk = ·

CPA-secure KEM +
COA-secure SKE =>
CPA-secure PKE @
COA-secure SKE

Dec$_{sk}$(c)

k = $H(c^x) = H(g^{xy})$

HDH (Hash Diffie-Hellman) Assumption

HDH problem is hard relative to (G, o) and hash function H: G -> $\{0,1\}^m$ if for every PPT A (it is hard to distinguish $H(g^{xy})$ from a random string r from $\{0,1\}^m$ even given g^x, g^y)):

$$\left| \Pr[A(G, o, q, g, g^X, g^Y, H(g^{XY})) = 1] - \Pr[A(G, o, q, g, g^X, g^Y, r) = 1] \right| \leq negl()$$

HDH assumption is that there exists a group and hash function H so that HDH is hard relative to them

It is weaker than DDH but stronger than CDH when Hash function is implemented using known practical hash functions.

Theorem: HDH assumption holds → Π is a CPA-secure KEM

Proof: Easy

CCA Attacks in Public-key World

- CCA attacks --- attacker gets access to decryption oracle
  - More powerful than CPA attacks
- Launching CCA attacks in the public-key world is relatively easier
  - In the symmetric-key setting, a message encrypted with the (secret) key k can originate only from a source who has the key k
  - In the public-key world, an entity can receive encrypted messages from multiple sources who knows the public key for that entity

CCA Security

CCA experiment $\mathrm{PubK}^{cca}_{A,\Pi}(n)$

Encryption oracle does not need to be not explicitly provided

Π = (Gen, Enc, Dec)

PPT A

I can break Π

pk

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = \mathrm{Dec}_{sk}(C_i)$

$m_0, m_1, |m_0| = |m_1|$

$c^* \leftarrow \mathrm{Enc}_{pk}(m_b)$

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = \mathrm{Dec}_{sk}(C_i)$

$b' \in \{0, 1\}$

Let me verify

$b \leftarrow \{0, 1\}$

pk, sk

$\mathrm{Gen}(1^n)$

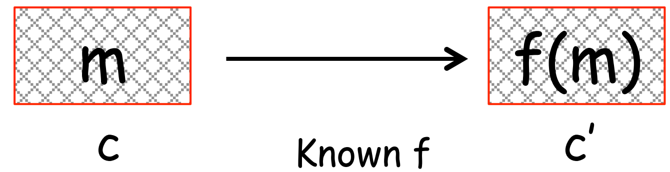
Game Output

$$\begin{cases} 1, \text{ if } b' = b \\ 0, \text{ otherwise} \end{cases}$$

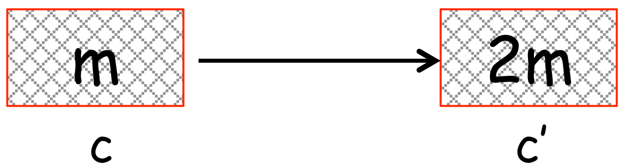
Π is CCA-secure if: $\Pr\left(\mathrm{PubK}^{cca}_{A,\Pi}(n) = 1\right) \leq \frac{1}{2} + \mathrm{negl}(n)$

Non-malleability : An Issue Related to CCA Attacks

- An encryption scheme (symmetric/asymmetric) is malleable if the following is possible:
  - Given an encryption c of an unknown message m
  - Possible to compute a ciphertext c′ from c which is an encryption of an unknown m′, but which is related to m in a known fashion



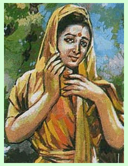
- Ex:



- If an encryption scheme is CCA-secure → it is non-malleable and vice versa
  - Otherwise an attacker in the CCA game on receiving challenge ciphertext $c^* \leftarrow Enc(m_b)$ can query the decryption oracle on $c' \leftarrow Enc(f(m_b))$ and obtain $f(m_b)$
- Malleability has both advantages as well as disadvantages
  - Disadvantage: consider an e-auction among two bidders.
    - A malicious bidder can always win without even knowing the other bid
  - Advantage ?
    - Think of it. Will see in the next course

El Gamal is malleable (NOT CCA-secure)

Public Key pk = $(G,o,q,g,h=g^x)$



$m, pk = (G,o,q,g,h=g^x)$

$Enc_{pk}(m)$

$c_1 = g^y$ for random y

$c_2 = h^y . m$

c

$c, sk=x$

$Dec_{sk}(c)$

$c_2 / (c_1)^x = c_2 . [(c_1)^x]^{-1}$

- Given El Gamal encryption (c_1, c_2) of m under the public key h, can you come up with an encryption of 2m ?
  - What will $(c_1, 2c_2)$ correspond to ?
- Can you compute a different ciphertext (c'_1, c'_2) for 2m, where $c_1 \neq c'_1$?

CCA Multi-message Security

CCA experiment $\mathrm{PubK}^{\text{cca-mult}}_{A,\Pi}(n)$

Π = (Gen, Enc, Dec)

$(m_{0,1}, m_{1,1})$ → $LR_{pk,b}$

$c^*_1 \leftarrow Enc_k(m_{b,1})$

$b \leftarrow \{0, 1\}$

PPT A

I can break Π

pk

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = Dec_{sk}(C_i)$

$(m_{0,1}, m_{1,1})$

$c^*_2 \leftarrow Enc_k(m_{b,1})$

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = Dec_{sk}(C_i)$

$b' \in \{0, 1\}$

Let me verify

pk, sk ← $Gen(1^n)$

Game Output

$$\begin{cases} 1, & \text{if } b' = b \\ 0, & \text{otherwise} \end{cases}$$

CCA Multi-message Security

CCA experiment $\mathrm{PubK}^{\text{cca-mult}}_{A,\Pi}(n)$

Π = (Gen, Enc, Dec)

PPT A

I can break Π

pk

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = \mathrm{Dec}_{sk}(C_i)$

$(m_{0,2}, m_{1,2})$

$c^*_2 \leftarrow \mathrm{Enc}_k(m_{b,2})$

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = \mathrm{Dec}_{sk}(C_i)$

$b' \in \{0, 1\}$

$(m_{0,2}, m_{1,2})$ → $\mathrm{LR}_{pk,b}$

$c^*_2 \leftarrow \mathrm{Enc}_k(m_{b,2})$

$b \leftarrow \{0, 1\}$

Let me verify

$\mathrm{Gen}(1^n)$ → pk, sk

Game Output

$$\begin{cases} 1, & \text{if } b' = b \\ 0, & \text{otherwise} \end{cases}$$

CCA Multi-message Security

CCA experiment $\mathrm{PubK}^{\text{cca-mult}}_{A,\Pi}(n)$

Π = (Gen, Enc, Dec)

PPT A

I can break Π

pk

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = \mathrm{Dec}_{sk}(C_i)$

$(m_{0,t}, m_{1,t})$

$c^*_t \leftarrow \mathrm{Enc}_k(m_{b,t})$

$C_1, C_2, \ldots, C_q$

$M_1, M_2, \ldots, M_q$ $\quad M_i = \mathrm{Dec}_{sk}(C_i)$

$b' \in \{0, 1\}$

Let me verify

$(m_{0,t}, m_{1,t}) \rightarrow \mathrm{LR}_{pk,b}$

$c^*_t \leftarrow \mathrm{Enc}_k(m_{b,t})$

$b \leftarrow \{0, 1\}$

$\mathrm{Gen}(1^n) \rightarrow$ pk, sk

Game Output

$$\begin{cases} 1, \text{ if } b' = b \\ 0, \text{ otherwise} \end{cases}$$

Π is CCA-secure if: $\Pr\left(\mathrm{PubK}^{\text{cca-mult}}_{A,\Pi}(n) = 1\right) \leq \frac{1}{2} + \mathrm{negl}(n)$

(Single vs Multi-message CCA Security)

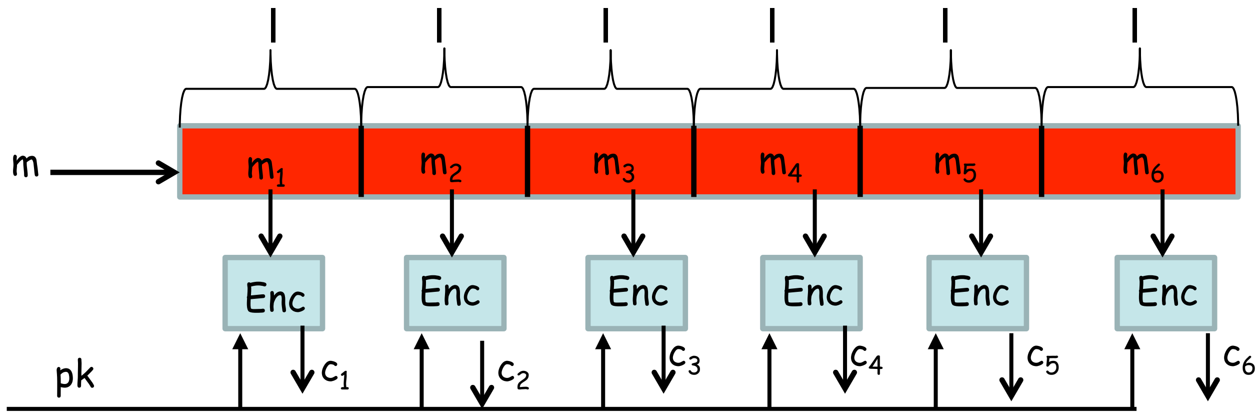
Theorem: single-message CCA security $\rightarrow$ multi-message CCA security.

Proof: The very same proof for CPA security using hybrid argument will work with minor necessary changes

PKE					SKE				
COA	$\approx$	CPA	$\not\rightarrow$	CCA	COA	$\not\rightarrow$	CPA	$\not\rightarrow$	CCA
$\approx$		$\approx$		$\approx$	$\not\rightarrow$		$\approx$		$\approx$
COA-mult		CPA-mult		CCA-mult	COA-mult		CPA-mult		CCA-mult

Implication of Single message Implies multi-message Security

- Given CCA secure scheme Π for bit/small messages, construct CCA-secure PKE for long message



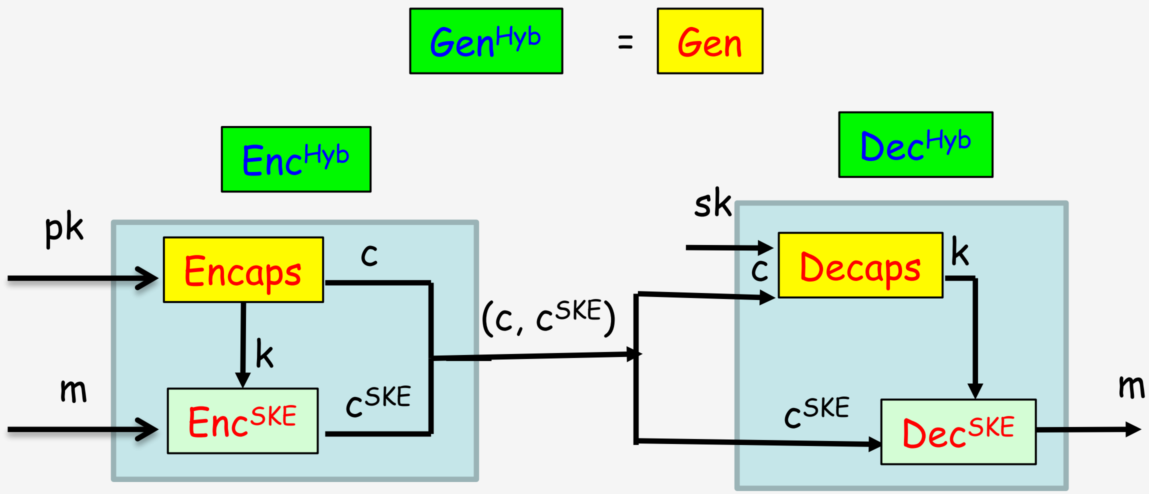
$c_1c_2\ldots c_6 \leftarrow \mathrm{Enc}_{pk}(m)$

- Is Π' CCA-secure ?
  - No! Truncate and take DO service

- CCA secure scheme Π for bit/small messages → CCA-secure PKE for long message- Very non-trivial construction

Term Paper: Steven Myers, Abhi Shelat: **Bit Encryption Is Complete.** FOCS 2009: 607-616

Hybrid Encryption using KEM



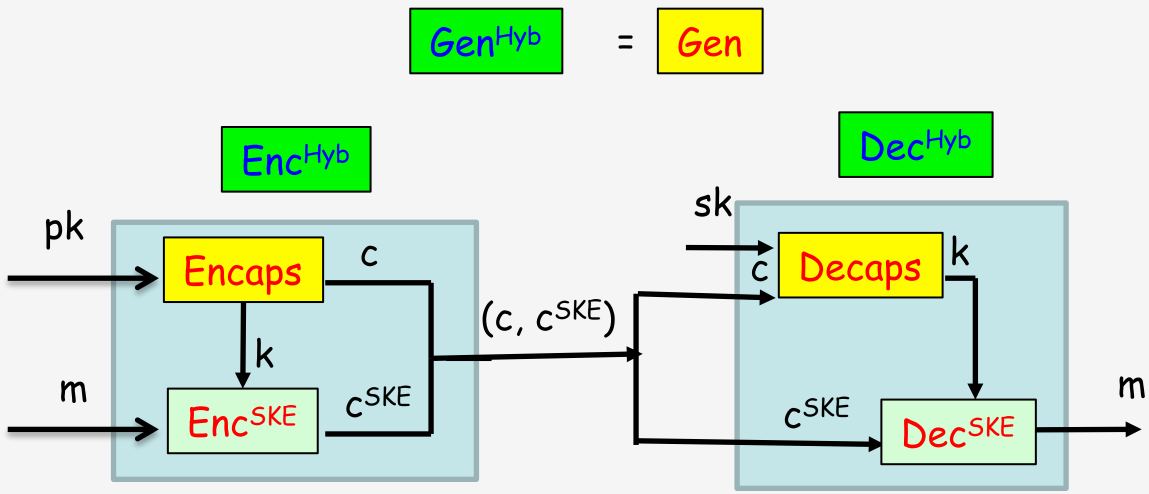
Π = (Gen, Encaps, Decaps)

Π^{SKE} = (Gen^{SKE}, Enc^{SKE}, Dec^{SKE})

Π^{Hyb} = (Gen^{Hyb}, Enc^{Hyb}, Dec^{Hyb})

CPA World	**CCA World**
Π CPA-secure Π^{SKE} COA-secure $\rightarrow$ Π^{Hyb} CPA-secure	If Π^{SKE} is malleable (think of PRG/PRF based schemes), then irrespective of Π, Π^{Hyb} is malleable too! (c (KEM ciphertext), G(k) + m (SKE ciphertext))

Hybrid Encryption using KEM



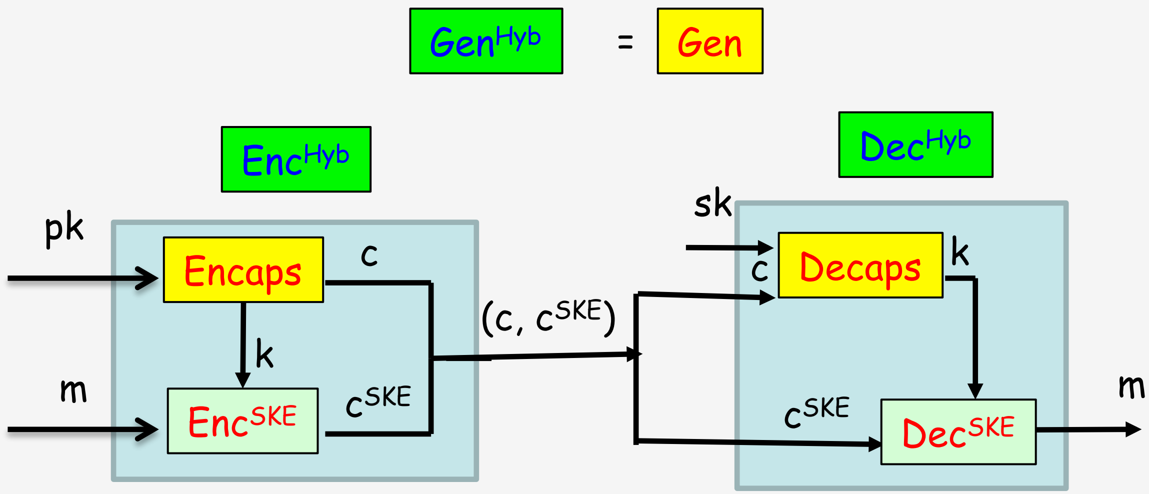
Π = (Gen, Encaps, Decaps)

Π^{SKE} = (Gen^{SKE}, Enc^{SKE}, Dec^{SKE})

Π^{Hyb} = (Gen^{Hyb}, Enc^{Hyb}, Dec^{Hyb})

CPA World	CCA World
Π CPA-secure Π^{SKE} COA-secure $\longrightarrow$ Π^{Hyb} CPA-secure	If Π is malleable, then Π^{Hyb} can malleable! (c (KEM ciphertext), G(k) + m (SKE ciphertext))

Hybrid Encryption using KEM



Π = (Gen, Encaps, Decaps)

Π^{SKE} = (Gen^{SKE}, Enc^{SKE}, Dec^{SKE})

Π^{Hyb} = (Gen^{Hyb}, Enc^{Hyb}, Dec^{Hyb})

CPA World	**CCA World**
Π CPA-secure, Π^{SKE} COA-secure $\rightarrow$ Π^{Hyb} CPA-secure	Π CCA-secure, Π^{SKE} CCA-secure $\rightarrow$ Π^{Hyb} CCA-secure

Sufficient but NOT necessary! In fact there are works proving this is true. Weaker than CCA-secure KEM + CCA SKE => CCA Hybrid encryption

Thank You!