CSA E0 235: Cryptography (01/04/2015)

Lecture #10

Instructor: Arpita Patra *Submitted by: Pradeep Kudikala(#11404)*

In previous lecture, we have seen the notion public-key encryption scheme, the equivalence between COA-Security(distinguishable encryptions in the presence of an eavesdropper) and CPA security and El Gamal Encryption Scheme for CPA-secure PKE. Today we see a more efficient notion of security called Hybrid Encryption, combination of Public key encryption(PKE) and private key encryption(SKE).

Outline

- Hybrid Encryption (PKE from PKE + SKE with almost the same efficiency of SKE)
- Key Encapsulation Mechanism (KEM) (Similar to PKE CPA Security)
- CPA-secure KEM + COA-secure SKE ⇒ CPA-secure PKE
- CPA-secure KEM from HDH Assumption (Similar to DDH assumption)
- CCA Security for PKE
- Single message CCA ⇒ Multi message CCA
- CCA KEM
- CCA KEM + CCA SKE ⇒ CCA PKE (Hybrid encryption)

1 Need for Hybrid Encryption

As we have seen PKE is computationally expensive and cipher text length is increased significantly. Whereas PKE is significantly faster and has lower cipher text expansion which asks for shared key assumption.
It is possible to construct a better efficient encryption scheme by using private-key encryption *in tandem with* public-key encryption.The resulting combination is called hybrid encryption and is used extensively in practice.
The basic **idea** (shown in Figure 1) is to use public-key encryption to obtain a shared key k, and then encrypt the message m using a private-key encryption scheme and key k. The receiver can use its private key to derive k, and then uses private-key decryption (with key k) to recover the plain message.

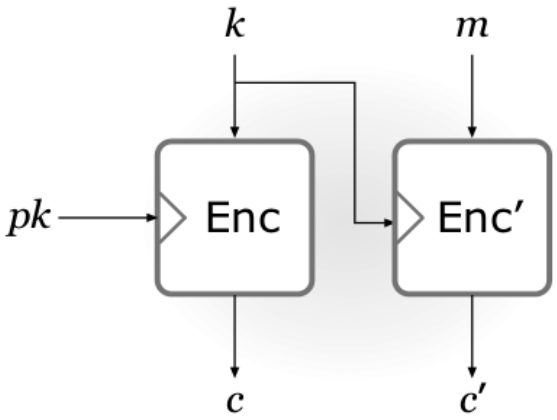

Figure 1. Hybrid encryption. Enc - PKE, $Enc^{'}$ - SKE

Advantage of Hybrid encryption
Let α, β be the cost of encrypting 1 bit message using PKE,SKE. α is orders of magnitude greater the β.
The cost of encrypting 1 bit message using Hybrid Encryption is

$$\frac{n\alpha + |m|\beta}{|m|} = \frac{n\alpha}{|m|} + \beta$$

where n is the key length and $|m|$ is message length. The above expression approaches β for sufficiently long m, same as the cost per bit of the private-key scheme. Hybrid encryption thus allows us to achieve the functionality of public-key encryption at the efficiency of private-key encryption, at least for sufficiently long messages.

2 Key-Encapsulation Mechanism

In the above implementation the sender would share k by

1. choosing a uniform value k
2. encrypting k using a public-key encryption scheme

Instead we can use a more direct approach called *key-encapsulation mechanism*(**KEM**) to accomplish both of these "*in one shot.*".
We define KEM as follows:

DEFINITION 1 A key-encapsulation mechanism (KEM) is a tuple of probabilistic polynomial-time algorithms (Gen, Encaps, Decaps) such that:

1. **Gen**: The *key-generation algorithm* takes input the security parameter 1^n and outputs a public-/private-key pair (pk, sk).

2. **Encaps:** The *encapsulation algorithm* input a public key pk, security parameter 1^n. It outputs a ciphertext c and a key $k \in \{0,1\}^n$ where *l(n)* is the key length. We write this as $(c, k) \leftarrow Encaps_{pk}(1^n)$.

3. **Decaps:** The *deterministic decapsulation algorithm* takes as input a private key sk and a ciphertext c, and outputs a uniform key k or a special symbol $\perp$ denoting failure. We write this as $k := Decaps_{sk}(c)$.

It is required that with all but negligible probability over (sk, pk) output by $Gen(1^n)$, if $Encaps_{pk}(1^n)$ outputs (c,k) then $Decaps_{sk}(c)$ outputs k.

Note****:** Any public-key encryption scheme trivially gives a KEM by choosing a random key k and encrypting it. However, construction KEMs can be more efficient.

2.1 Hybrid encryption using the KEM/DEM

As shown in the Figure 2 sender runs $Encaps_{pk}(1^n)$ to obtain c along with a key k; sender then uses a private-key encryption scheme(called *data-encapsulation mechanism* - **DEM** in this context) to encrypt its message m as c', using k as the key.

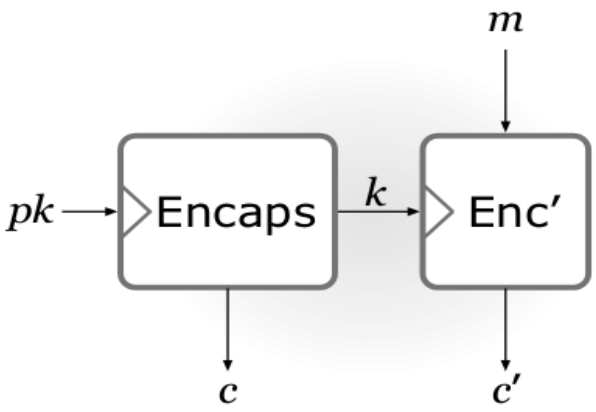

Figure 2. Hybrid encryption using KEM/DEM

The Decryption at the receiver end is followed in similar lines. Here we give the formal specification:

CONSTRUCTION 1
Let Π = (Gen, Encaps, Decaps) be a KEM with key length n, and let $\Pi^{pk} = (Gen^{pk}, Enc^{pk}, Dec^{pk})$ be a private-key encryption scheme. Construct a public-key encryption scheme $\Pi^{hy} = (Gen^{hy}, Enc^{hy}, Dec^{hy})$ as follows:

1. **Gen**^{hy}: on input 1^n run $Gen(1^n)$ and use the public and private keys (pk,sk) that are output.

2. **Enc**^{hy}: on input a public key pk and a message m 0, 1 do:

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

(b) Compute $c \leftarrow Enc_k^{pk}(m)$.

(c) Output the ciphertext $\langle c, c' \rangle$.

3. **Dec**^{hy}:on input a private key sk and a ciphertext $\langle c, c' \rangle$ do:

(a) Compute $k := Decaps_{sk}(c)$.

(b) Output the message $m := Dec_k^{pk}(c)$.

Security of Π^{hy}:

- Π is a CPA-secure KEM and Π^{pk} has indistinguishable encryptions in the presence of an eavesdropper, then Π^{hy} is a CPA-secure public-key encryption scheme. Here we only need weaker definition of security(indistinguishable encryptions). The reason is that a fresh, uniform key k is chosen each time a new message is encrypted. Since each key k is used only once, indistinguishability of a single encryption of Π^{pk} suffices for security of the hybrid scheme Π^{hy}.
- If Π is a CCA-secure KEM and Π^{pk} is a CCA-secure private-key encryption scheme, then Π^{hy} is a CCA-secure public-key encryption scheme.

3 CPA-Security in Public Key World

3.1 CPA-Security of KEM

Let $\Pi = (Gen, Encaps, Decaps)$ be a KEM and $\mathcal{A}$ an arbitrary adversary. **The CPA indistinguishability experiment $KEM_{\mathcal{A},\Pi}^{cpa}(n)$:**

- keys $= (pk, sk) \leftarrow Gen(1^n)$, Then $(c, k) \leftarrow Encaps_{pk}(1^n)$, $k \in \{0,1\}^n$
- A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ set $\hat{k} := k$. If $b = 1$ then chose a uniform $\hat{k} \in \{0,1\}^n$.
- Give $(pk, c, \hat{k})$ to $\mathcal{A}$, who outputs a bit b'. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

In the above experiment, $\mathcal{A}$ is given the ciphertext c and either the actual key k corresponding to c, or an independent, uniform key. The KEM is CPA-secure if no efficient adversary can distinguish between these possibilities.

DEFINITION 2: CPA-Security of KEM.
A key-encapsulation mechanism Π is CPA-secure if for all PPT adversaries $\mathcal{A}$ there exists a negligible function $negl(.)$ such that

$$Pr[KEM_{\mathcal{A},\Pi}^{cpa}(n) = 1] \leq \frac{1}{2} + negl(n).$$

3.2 CPA-Security Hybrid Encryption

Theorem 1. If Π is a CPA-secure KEM and Π^{pk} is a private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper, then Π^{hy} as in Construction 1 is a CPA-secure public-key encryption scheme.

Fix an arbitrary PPT adversary $\mathcal{A}^{hy}$, and consider experiment $PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n)$. Our goal is to prove that there is a negligible function negl such that Before proving the theorem, we recollect the proposition:

PROPOSITION 1 If a public-key encryption scheme has indistin- guishable encryptions in the presence of an eavesdropper, it is CPA-secure.

Proof We prove that Π^{hy} has indistinguishable encryptions in the presence of an eavesdropper; by above Proposition, this implies it is CPA-secure.

Fix an arbitrary ppt adversary $\mathcal{A}^{hy}$, and consider experiment $PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n)$. We prove that there is a negligible function $negl(.)$ such that

$$Pr[PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n) = 1] \leq \frac{1}{2} + negl(n).$$

By definition of the experiment, we have
$Pr[PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n) = 1]$

$$= \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps^{(1)}_{pk}(1^n), Enc'(m_0)) = 0] + \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps^{(1)}_{pk}(1^n), Enc'(m_1)) = 1] \quad \ldots [3.1]$$

where in each case k equals $Encaps^{(2)}_{pk}(1^n)$. Consider the following PPT adversary $\mathcal{A}^{\Pi}_1$ attacking Π. ($Encaps^{(1)}_{pk}(1^n), Encaps^{(2)}_{pk}(1^n)$ denote the ciphertext(resp., key) output by Encaps.)

Adversary $\mathcal{A}^{\Pi}_1$:

1. $\mathcal{A}^{\Pi}_1$ is given $(pk, c, \hat{k})$.
2. $\mathcal{A}^{\Pi}_1$ runs $\mathcal{A}^{hy}(pk)$ to obtain two messages m_o, m_1. Then $\mathcal{A}^{\Pi}_1$ computes $c' \leftarrow Enc'_{\hat{k}}(m_0)$, gives ciphertext $\langle c, c' \rangle$ $\mathcal{A}^{hy}$, and outputs the bit b' that $\mathcal{A}^{hy}$ outputs.

Consider the behavior of $\mathcal{A}^{\Pi}_1$ when attacking Π in experiment $KEM^{cpa}_{\mathcal{A}^{\Pi}_1,\Pi}(n)$.
When $b = 0$ in that experiment, then $\mathcal{A}^{\Pi}_1$ is given $(pk, c, \hat{k})$ where c and $\hat{k}$ were both outputs by $Encaps_{pk}(1^n)$. This means that $\mathcal{A}^{hy}$ is given a ciphertext of the form $\langle c, c' \rangle = \langle c, Enc'_k(m_0) \rangle$, where k is the key encapsulated by c. So,

$$Pr[\mathcal{A}^{\Pi}_1 \textit{ outputs } 0 | b = 0] = Pr[\mathcal{A}^{hy}(pk, Encaps^{(1)}_{pk}(1^n), Enc'_k(m_0)) = 0].$$

On the other hand, when $b = 1$ in experiment $KEM^{cpa}_{\mathcal{A}^{\Pi}_1,\Pi}$ then $\mathcal{A}^{\Pi}_1$ is given $(pk, c, \hat{k})$ with $\hat{k}$ uniform and independent of c. If we denote such a key by k', his means $\mathcal{A}^{hy}$ is given a

ciphertext of the form $\langle c, Enc'_{k'}(m_0)\rangle$, and

$$Pr[\mathcal{A}_1^{\Pi} \textit{ outputs } 1|b=1] = Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc'_{k'}(m_0)) = 1].$$

Since Π is a CPA-secure KEM, there is a negligible function $negl_1$ such that

$$\begin{aligned}
\tfrac{1}{2} + negl_1(n) &\geq Pr[KEM^{cpa}_{\mathcal{A}_1^{\Pi},\Pi}(n) = 1] \\
&= \tfrac{1}{2} \cdot Pr[\mathcal{A}_1^{\Pi} \textit{ outputs } 0|b=0] + \tfrac{1}{2} \cdot Pr[\mathcal{A}_1^{\Pi} \textit{ outputs } 1|b=1] \\
&= \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc'_{k}(m_0)) = 0] \\
&\quad + \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc'_{k'}(m_0)) = 1] \qquad \ldots [3.2]
\end{aligned}$$

where k is equal to $Encalps_{pk}^{(2)}(1^n)$ and k' is a uniform and independent key.

Next, consider the following PPT adversary $\mathcal{A}^{pk}$ that eavesdrops on a message encrypted using the private-key scheme Π^{pk} .
Adversary $\mathcal{A}^{pk}$:

1. $\mathcal{A}^{pk}(1^n)$ runs $Gen(1^n)$ on its own to generate keys (pk, sk). It also computes $c \leftarrow Encaps_{pk}^{(1)}(1^n)$.
2. $\mathcal{A}^{pk}$ runs $\mathcal{A}^{hy}(pk)$ to obtain two messages m_0, m_1. These are output by $\mathcal{A}^{pk}$, and it is given in return a ciphertext c'.
3. $\mathcal{A}^{pk}$ gives the ciphertext $\langle c, c'\rangle$ to $\mathcal{A}^{hy}$, and outputs the bit b' that $\mathcal{A}^{hy}$ outputs.

When $b=0$ in experiment $PrivK^{eav}_{\mathcal{A}^{pk},\Pi^{pk}}(n)$, adversary $\mathcal{A}^{pk}$ is given a ciphertext c' which is an encryption of m_0 using a key k' that is uniform and independent of anything else. So $\mathcal{A}^{hy}$ s given a ciphertext of the form $\langle c, Enc^{pk}_{k'}(m_0)\rangle$ where k' is uniform and independent of c, and

$$Pr[\mathcal{A}^{pk} \textit{ outputs } 0|b=0] = Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc'_{k'}(m_0)) = 0].$$

On the other hand, when $b=1$ in experiment $PrivK^{eav}_{\mathcal{A}^{pk},\Pi^{pk}}(n)$ then $\mathcal{A}^{pk}$ is given an encryption of m_1 using a uniform, independent key k' This means $\mathcal{A}^{hy}$ is given a ciphertext of the form $\langle c, Enc^{pk}_{k'}(m_1)\rangle$ and also

$$Pr[\mathcal{A}^{pk} \textit{ outputs } 1|b=1] = Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc'_{k'}(m_1)) = 1].$$

Since Π^{pk} has indistinguishable encryptions in the presence of an eavesdropper, there is a negligible function $negl^{pk}$ such that

$$\begin{aligned}
\tfrac{1}{2} + negl^{pk}(n) &\geq Pr[PrivK^{eav}_{\mathcal{A}^{pk},\Pi^{pk}}(n) = 1] \\
&= \tfrac{1}{2} \cdot Pr[\mathcal{A}^{pk} \textit{ outputs } 0|b=0] + \tfrac{1}{2} \cdot Pr[\mathcal{A}^{pk} \textit{ outputs } 1|b=1]
\end{aligned}$$

$$= \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc_{k'}^{'}(m_0)) = 0]$$

$$+ \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc_{k'}^{'}(m_0)) = 1] \quad \ldots [3.3]$$

Proceeding exactly as we did to prove Equation (3.2), we can show that there is a negligible function $negl_2$ such that

$$\tfrac{1}{2} + negl_2(n) \geq Pr[KEM^{cpa}_{\mathcal{A}_2^{\Pi},\Pi}(n) = 1]$$

$$= \tfrac{1}{2} \cdot Pr[\mathcal{A}_2^{\Pi} \; outputs \;\; 0 | b = 0] + \tfrac{1}{2} \cdot Pr[\mathcal{A}_2^{\Pi} \; outputs \;\; 1 | b = 1]$$

$$= \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc_{k}^{'}(m_0)) = 0]$$

$$+ \tfrac{1}{2} \cdot Pr[\mathcal{A}^{hy}(pk, Encaps_{pk}^{(1)}(1^n), Enc_{k'}^{'}(m_0)) = 1] \quad \ldots [3.4]$$

Summing Equations $[3.2] - [3.4]$ and using the fact that the sum of three negligible functions is negligible, we see there exists a negligible function $negl$ such that

$$\tfrac{3}{2} + negl(n) \geq$$

$$\tfrac{1}{2} \cdot (Pr[\mathcal{A}^{hy}(pk, c, Enc_{k}^{'}(m_0)) = 0] + Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_0)) = 1]$$

$$+ Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_0)) = 0] + Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_1)) = 1]$$

$$+ Pr[\mathcal{A}^{hy}(pk, c, Enc_{k}^{'}(m_1)) = 1] + Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_1)) = 0])$$

where $c = Encaps_{pk}^{(1)}(1^n)$ in all the above. Note that

$$Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_0)) = 1] + Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_0)) = 0] = 1,$$

since the probabilities of complementary events always sum to 1. Similarly,

$$Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_1)) = 1] + Pr[\mathcal{A}^{hy}(pk, c, Enc_{k'}^{'}(m_1)) = 0] = 1.$$

Therefore,

$$\tfrac{1}{2} + negl(n) \geq \tfrac{1}{2} \cdot (Pr[\mathcal{A}^{hy}(pk, c, Enc_{k}^{'}(m_0)) = 0] + Pr[\mathcal{A}^{hy}(pk, c, Enc_{k}^{'}(m_1)) = 1])$$

$$= Pr[PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(1^n) = 1]$$

(using Equation [3.1] for the last equality), proving the theorem. ■

4 "El Gamal-Like" KEM

El Gamal encryption discussed in earlier lectures can be used as part of a hybrid encryption scheme by simply encrypting a uniform group element m and using a hash of that element as a key.But this is not necessary! The proof of security for El Gamal encryption shows that c_1^x(where c_1 is the first component of the ciphertext, and x is the private key of the receiver) is already indistinguishable from a uniform group element, so the sender/receiver may as well use that. **Construction 2** illustrates the KEM that follows this approach. Note that the resulting encapsulation consists of just a single group element. In contrast, if we were to use El Gamal encryption of a uniform group element, the ciphertext would contain two group elements.

CONSTRUCTION 2 Let $\mathcal{G}$ be a polynomial-time algorithm that takes as input 1^n and (except possibly with negligible probability) outputs a description of a cyclic group $\mathbb{G}$, its order q (with $\|q\| = n$),and a generator g. Define a KEM as follows:

- **Gen:** on input 1^n run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$. choose a uniform $x \in \digamma_p$ and set $h := g^x$. Also specify hash function $H : \mathbb{G} \to \{0,1\}^m$. The public key is $\langle \mathbb{G}, q, g, h, H \rangle$ and The private key is $\langle \mathbb{G}, q, g, x \rangle$
- **Encaps:** on input a public key $pk = \langle \mathbb{G}, q, g, h, H \rangle$ choose a uniform $y \in \mathbb{Z}_p$ and output the ciphertext g^x and the key $H(h^y)$
- **Decaps:** and output the ciphertext $sk = \langle \mathbb{G}, q, g, x \rangle$ and a ciphertext $c \in \mathbb{G}$, output the key $H(c^x)$

HDH(Hash Diffie-Hellman) Assumtion

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

$$Pr[\mathcal{A}(\mathbb{G}, o, q, g, g^x, g^y, H(g^{xy})) = 1] - Pr[\mathcal{A}(\mathbb{G}, o, q, g, g^x, g^y, r) = 1] \leq negl()$$

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 2 If HDH assumption is hard the the scheme in construction 2 is CPA-Secure KEM.

5 CCA-Security in Public Key World

We had already seen the equivalence between CPA-Security and indistinguishability in presence of eavesdropper. Unlike the above two notions of security CCA attacks which have access to decryptio oracle are more powerfull than CPA attack

Launching the CCA Attacks in public key world is relatively easier than the private key world. In the symmetric-key setting, a message encrypted with the (secret) key k can originate only from a source who has the key k where as in the public-key world, an entity can receive encrypted messages from multiple sources who knows the public key for that entity

If the private-key encryption scheme Π^{pk} is not itself secure against chosen-ciphertext attacks, then (regardless of the KEM used) neither is the resulting hybrid encryption scheme Π^{hy} . If underlying Π^{pk} is not CCA-Secure then given $\langle c, c^{'} \rangle$ the output of Enc^{hy}, where $c^{'} \leftarrow Enc_k^{pk}(m)$ as shown in the construction 1, an attacker can modify $c^{'}$(which is an encryption of an unknown message) such that modified ciphertext. Attacker can now ask for decryption of modified cipher text which decrypts to $m^{'} = f(m)$. for some known function f. This is called Malleability.

Note** *If an encryption scheme is CCA-secure then its non-malleable and vice versa. El Gamal Encryption scheme is malleable, Given El Gamal encryption (c_1, c_2) of m under the public key h, an adversary can give encryption of 2m just by multiplying c_2 by 2.*

Hence we need a CCA-Secure private-key encryption scheme. But this is clearly not enough if the KEM is susceptible to chosen-ciphertext attacks. We now define the notion of security of KEM against cca attacks. In Definition 2 we defined the CPA-security of KEM. Now, we additionally allow the attacker to request decapsulation of ciphertexts of its choice.

Let $\Pi = (Gen, Encaps, Decaps)$ be a KEM with key length n and $\mathcal{A}$ an adversary, and consider the following experiment:

The CCA indistinguishability experiment $KEM^{cca}_{\mathcal{A},\Pi}(n)$:

1. $Gen(1^n)$ is run to obtain keys (pk, sk). Then $Encaps_{pk}(1^n)$ is run to generate (c, k) with $k \in \{0,1\}^n$.
2. A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ set $\hat{k} := k$. If $b = 1$ then choose a uniform $\hat{k} \in \{0,1\}^n$.
3. $\mathcal{A}$ is given $(pk, c, \hat{k})$ and access to an oracle $Decaps_{sk}(.)$, but may not request decapsulation of c itself.
4. $\mathcal{A}$ outputs a bit $b^{'}$. The output of the experiment is defined to be 1 if $b^{'} = b$, and 0 otherwise.

DEFINITION 3 A key-encapsulation mechanism Π is CCA-secure if for all PPT adversaries $\mathcal{A}$ there is a negligible function $negl$ such that

$$Pr[KEM^{cca}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

We can show that using a CCA-secure KEM in combination with a CCA-secure private-key encryption scheme results in a public-key encryption scheme secure against chosen-ciphertext attacks.

Theorem 3 If Π is a CCA-secure KEM and Π^{pk} is a CCA-secure private-key encryption scheme, then Π^{hy} as in Construction 1 is a CCA- secure public-key encryption scheme.

A proof can be obtained by suitable modification of the proof of Theorem 1.

Additional Points

1. **CCA Multi-message Security.** We can define an Experiment $PubK^{cca-multi}_{\mathcal{A},\Pi}$ by extending the $PubK^{cca}_{\mathcal{A},\Pi}$ in similar lines of $PrivK^{cca}_{\mathcal{A},\Pi^{pk}}$ which we have seen in the earlier lectures of this course. We define the scheme Π as CCA-Secure if for any PPT adversary $\mathcal{A}$ there exist negligible function $negl(n)$ such that

$$Pr[PubK^{cca-multi}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$

2. Any single message CCA-Secure scheme is also a multi-message CCA-Secure Encryption scheme and vice versa. To prove the above claim, we can use a variation of Hybrid arguments used in the proof of CPA security in this lecture.

3. Given CCA secure scheme Π for bit/small messages, construction of CCA-secure PKE for long message is possbile. A very non-trivial construction described in the paper Bit Encryption Is Complete. FOCS 2009: 607-616. by Steven Myers, Abhi Shelat.

4. CCA Security of KEM and CCA Security of Private Key Encryptions(SKE) scheme is Sufficient but not necessary for CCA Secure Hybrid Encryption scheme. In fact there are some constructions of CCA secure Hybrid Encryptions from weaker CCA-Secure KEM and CCA-secure SKE.

References:

1. Jonathan Katz, Yehuda Lindell : Introduction to Modern Cryptography, Second Edition