0 Key Exchange

Write down the key-exchange experiment for a protocol Π with an adversary $\mathcal{A}$.

Let Σ be the key-exchange protocol. We have two players, Alice and Bob.
Key Exchange Experiment $KE^{eav}_{\mathcal{A},\Pi}(n)$

1. Alice and Bob execute Π to generate a key K and a transcript t of all messages sent between them.
2. A bit $b \in \{0,1\}$ is chosen. If $b = 0$: $\hat{K} = K$. Else if $b = 1$: $\hat{K} \leftarrow_{\$} \{0,1\}^n$.
3. $\mathcal{A}$ is given t and $\hat{K}$.
4. $\mathcal{A}$ outputs b'.

If $b' = b$, then $\mathcal{A}$ wins the game.

1 ElGamal

(a) Suppose you are given an ElGamal encryption for some unknown message $m \in \mathbb{G}$. Show how to construct a different ciphertext that decrypts to the same m.

(b) Show that, given two ElGamal encryptions for messages $m_1, m_2 \in \mathbb{G}$, how you can construct a ciphertext that decrypts to the product $m_1 \cdot m_2$.

a)
You are given $(c_1, c_2) = (g^y, h^y \cdot m)$ for some unknown m. Note that $\mathbb{G}, q, g, h$ are public.

$$c_1' = g \cdot c_1$$
$$c_2' = h \cdot c_2$$

Then $(c_1', c_2') = (g \cdot g^y, h \cdot h^y \cdot m)$, and thus $(c_1', c_2') = (g^{y+1}, h^{y+1} \cdot m)$.
b)
Upon $(c_1, c_2) = (g^y, h^y \cdot m_1)$ and $(b_1, b_2) = (g^z, h^z \cdot m_2)$ (with some unknown y and z):

$$(c_1 \cdot b_1, c_2 \cdot b_2) = (g^y \cdot g^z, h^y \cdot m_1 h^z \cdot m_2)$$
$$(c_1 \cdot b_2, c_2 \cdot b_2) = (g^{y+z}, h^{y+z} \cdot (m_1 \cdot m_2)$$

This is possible to do because $\mathbb{G}$ is a cyclic (thus, abelian) group.

2 PKE

11.3 Katz/Lindell (part b)
Say a public-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for n-bit messages is *one-way* if any PPT adversary $\mathcal{A}$ has a negligible probability of success in the following experiment:

- $\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk).
- A message $m \in \{0,1\}^n$ is chosen uniformly at random; a ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m)$ is computed.
- $\mathcal{A}$ is given pk and c, and outputs m'.
- If $m' = m$ then $\mathcal{A}$ succeeds.

Can a *deterministic* public-key encryption scheme be one-way? If not, prove impossibility; else, give a construction based on any of the assumptions introduced in this book.

Yes. Plain-RSA

1. $\mathsf{Gen}(1^n)$ for (N, e, d), the $pk = (N, e)$, $sk = (N, d)$.
2. Enc: for a message $m \in \mathbb{Z}_N^*$. $\mathsf{Enc}_{pk}(m) = m^e \mod N$.
3. Dec: On input $c \in \mathbb{Z}_N^*$: $\mathsf{Dec}_{sk}(c) = c^d \mod N$.

RSA-experiment $\mathsf{RSA} - \mathsf{inv}_{\mathcal{A},\mathsf{Gen}}(n)$

1. Run $\mathsf{Gen}(1^n)$ to obtain (N, e, d).
2. Choose a uniform $y \in \mathbb{Z}_N^*$.
3. $\mathcal{A}$ gets N, e, y and outputs $x \in \mathbb{Z}_N^*$.
4. $\mathcal{A}$ wins if $x^e = y \mod N$.

Theorem 1. *Plain-RSA is one-way.*

Proof. AFSOC that Plain-RSA is not one-way – there exists $\mathcal{A}_{ow}$ who can win the one-way experiment with non-negligible probability, but that $\mathsf{RSA} - \mathsf{inv}$ has only:

$$Pr[\mathsf{RSA} - \mathsf{inv}_{\mathcal{A},\mathsf{Gen}}(n) = 1 \leq \mathsf{negl}(n)$$

We construct an adversary $\mathcal{A}_{inv}$ against $\mathsf{RSA} - \mathsf{inv}$. Reduction

1. $\mathcal{A}_{inv}$ receives N, e, y from his challenger.
2. He forwards $pk = (N, e)$ to $\mathcal{A}_{ow}$ and also y.

3. $\mathcal{A}_{ow}$ outputs m'.

4. $\mathcal{A}_{inv}$ sends m' to his challenger.

From the view of $\mathcal{A}_{ow}$, choosing $y \in \mathbb{Z}_N^*$ is the same as choosing x and then calculating $y = \mathsf{Enc}_{pk}(x) = x^e \mod N$. The distribution of choices is equal because RSA encryption is a permutation.
We see if $\mathcal{A}_{ow}$ wins, then m' must be such that $c = \mathsf{Enc}_{pk}(m') = m'^e \mod N$. Then $\mathcal{A}_{inv}$ has found the correct m' as well. As we assumed that $\mathsf{RSA-inv}$ could be won with only a negligible probability, this is a contradiction.

$\square$

3 Key-Exchange Protocol

Consider the following key-exchange protocol:

1. Alice chooses uniform $k, r \leftarrow_\$ \{0,1\}^n$ and sends $s = k \oplus r$ to Bob.
2. Bob chooses $t \leftarrow_\$ \{0,1\}^n$ and sends $u = s \oplus t$ to Alice.
3. Alice computes $w = u \oplus r$ and sends w to Bob.
4. Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob have outputted the same key. Is this scheme secure? If yes, prove its security, otherwise show a concrete attack.

We show that Alice and Bob calculate the same key by showing that $w \oplus t = k$ using the definitions of all the values.

$$\begin{aligned} w \oplus t = (u \oplus r) \oplus t = \\ (s \oplus t \oplus r) \oplus t = \\ s \oplus r = \\ (k \oplus r) \oplus r = k \end{aligned}$$

Is this scheme secure? Let us say an eavesdropper, Eve, gets a transcript of s, u, w. Then:

$$\begin{aligned} s \oplus u = s \oplus (s \oplus t) = t \\ t \oplus w = k \end{aligned}$$

Thus, Eve can use the three values s, u, w to calculate k. This scheme is not secure.

4 CPA, key-agreement

Show that a 2-message key-agreement protocol exists iff CPA-secure public-key encryption exists.

I.e., show how to construct a CPA-secure encryption scheme from any 2-message KA protocol, and vice-versa. Prove the security of your constructions.

<u>2-message Key-agreement $\implies$ CPA-secure encryption scheme.</u>
A CPA-secure encryption scheme Π:
Let KA be a key-agreement scheme with 2 messages between Alice and Bob. Suppose in KA, Alice sends A and Bob sends B, and they are able to agree on a key K. We write a for any internal value Alice has for herself (to calculate A) and b for Bob (to calculate B).

Alice		**Bob**
a		
	$\xrightarrow{\quad A \quad}$	
		b
		$c \leftarrow \mathsf{Enc}_K(m)$
	$\xleftarrow{\quad B, c \quad}$	
$m \leftarrow \mathsf{Dec}_K(c)$		

In order to take KA and turn it into a CPA-secure scheme, Bob simply sends the value B that he normally sends for the key-agreement, along with his message encrypted under K (using a perfectly secret private-key encryption scheme, such as one time pad). Alice is able to recreate K using B, and decrypt c to learn Bob's message.

<u>2-message Key-agreement $\impliedby$ CPA-secure encryption scheme.</u>
A Key-agreement scheme KA: Here, let Π be a CPA-secure encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

Alice		**Bob**
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$		
	$\xrightarrow{pk}$	
		$c \leftarrow \mathsf{Enc}_{pk}(K)$
	$\xleftarrow{c}$	
$K \leftarrow \mathsf{Dec}_{sk}(c)$		

Alice sends her pk as usual, and Bob uses pk to encrypt the desired secret key K to c. Alice decrypts c to learn K.

SECURITY PROOF BY REDUCTION.

Theorem 2. *If* Π *is secure, then* KA *is secure.*

Proof. Assume for sake of contradiction that Π is CPA-secure, but KA is not secure under the key-exchange experiment (defined at 10.1 in Katz/Lindell).

Step 1.

Π is a CPA-secure scheme, meaning that for all PPT $\mathcal{A}$ there exists negl such that:

$$Pr[\mathcal{A} \text{ wins } \mathsf{Pub}^{\mathsf{cpa}}_{\mathcal{A},\Pi}] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

There exists a distinguisher for key-agreement D such that, for a non-negligible p:

$$Pr[D \text{ wins } \mathsf{KE}^{eav}_{D,\mathsf{KA}}] = \frac{1}{2} + p(\lambda)$$

The key-exchange experiment with KA is $\mathsf{KE}^{eav}_{D,\mathsf{KA}}$:

1. Alice and Bob execute KA to generate a key K and a transcript t of all messages sent between them, $t = pk, c$.
2. A bit $b \in \{0, 1\}$ is chosen. If $b = 0$: $\hat{K} \leftarrow_{\$} \{0, 1\}^n$, $b = 1$: $\hat{K} = K$.
3. D is given t and $\hat{K}$.
4. D outputs b'.

Say W_0 is the event that $b = 0$, and W_1 is the event that D sees the key per $b = 1$, where W_0 and W_1 happen uniformly at random. Then we can write:

$$\frac{1}{2} \cdot Pr[D = 0|W_0] + \frac{1}{2} \cdot Pr[D = 1|W_1] = \frac{1}{2} + p(\lambda)$$

Step 2. Reduction Then we build $\mathcal{A}$:

1. $\mathcal{A}$ receives pk.
2. $\mathcal{A}$ outputs 2 mesages k_0, k_1, which were selected uniformly at random from the keyspace.
3. $\mathcal{A}$ flips a bit to get $b' \in \{0, 1\}$.
4. Upon receipt of c^*, $\mathcal{A}$ forwards the transcript (pk, c^*) and $k_{b'}$ to D.
5. If D says 0, output $1 - b'$. Else b'.

Step 3. Analysis of Success probability of the reduction $\mathcal{A}$.
Case Analysis:

- Case 1: Here, $b' \neq b$. Suppose $c^* = \mathsf{Enc}_{pk}(k_b)$ and D is given (pk, c^*),and $k_{b'} = k_{1-b}$. Then as $k_{b'}$ is random,

  $$Pr[D \text{ wins } \mathsf{KE}^{eav}_{D,\mathsf{KA}}|(pk, \mathsf{Enc}_{pk}(k_b)), k_{1-b}] = Pr[D = 0|W_0]$$

  Then

  $$Pr[\mathcal{A} \text{ wins } \mathsf{Pub}^{\mathsf{cpa}}_{\mathcal{A},\Pi}|W_0] = Pr[D = 0|W_0]$$

- Case 2: Here, $b' = b$. Then $c^* = \mathsf{Enc}_{pk}(k_b)$ and D is given $(pk, c^*, k_{b'} = k_b$. As $k_{b'}$ is the agreed upon key,

  $$Pr[D \text{ wins } \mathsf{KE}^{eav}_{D,\mathsf{KA}}|(pk, \mathsf{Enc}_{pk}(k_b)), k_b] = Pr[D = 1|W_1] \implies Pr[\mathcal{A} \text{ wins } \mathsf{Pub}^{\mathsf{cpa}}_{\mathcal{A},\Pi}|W_1] = Pr[D = 1|W_1]$$

Using the assumption that

$$\frac{1}{2} \cdot Pr[D = 0|W_0] + \frac{1}{2} \cdot Pr[D = 1|W_1] = \frac{1}{2} + p(\lambda),$$

we can write

$$Pr[\mathcal{A} \text{ wins } \mathsf{Pub}^{\mathsf{cpa}}_{\mathcal{A},\Pi}] = \tfrac{1}{2} \cdot Pr[\mathcal{A} \text{ wins } \mathsf{Pub}^{\mathsf{cpa}}_{\mathcal{A},\Pi}|W_0] + \tfrac{1}{2} \cdot Pr[\mathcal{A} \text{ wins } \mathsf{Pub}^{\mathsf{cpa}}_{\mathcal{A},\Pi}|W_1]| = \tfrac{1}{2} + p(\lambda),$$

where $p(\lambda)$ is non-negligible. But as we assumed Π was CPA-secure, this is a contradiction. We conclude that KA must be secure in the presence of an eavesdropper. $\square$

Security Proof by Reduction.

Theorem 3. *If* KA *is secure under the key-exchange experiment, then* Π *is CPA-secure.*

Proof. We prove that Π has indistinguishable encryptions in the presence of an eavesdropper. Using Proposition 11.3 (Katz/Lindell), Π is then CPA-secure.

Step 1.

Let $\mathcal{A}$ be a PPT algorithm. Assume for sake of contradiction there is a non-negligible function such that

$$Pr[\mathcal{A} \text{ wins } \mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}] = \frac{1}{2} + p(\lambda).$$

(Using the experiment defined at Katz/Lindell 11.2). The eavesdropping indistinguishability experiment $\mathsf{PubK}^{eav}_{\mathcal{A},\Pi}$:

1. Gen run to obtain keys $(pk = A, sk = a)$.
2. $\mathcal{A}$ gets pk and outputs a pair of equal length messages m_0, m_1 in the message space.
3. Uniform $b \in \{0, 1\}$ is flipped and ciphertext B and $c^* \leftarrow \mathsf{Enc}_{pk}(m_b)$ given to $\mathcal{A}$.
4. $\mathcal{A}$ outputs b'. If $b' = b$ then $\mathcal{A}$ wins the experiment.

Step 2. Ideal scheme $\tilde{\Pi}$ Consider the "modified encryption" $\tilde{\Pi}$ where Gen is the same, but the encryption of the message m is done by choosing a uniform $\hat{K}$ and outputting $B, c \leftarrow \mathsf{Enc}_{\hat{K}}(m)$. $\tilde{Pi}$ is not actually an encryption scheme, but the experiment $\mathsf{Pub}^{\mathsf{cpa}}_{\tilde{\Pi},\mathcal{A}}$ is still well-defined.

1. Gen run to obtain keys $(pk = A, sk = a)$.
2. $\mathcal{A}$ gets pk and outputs a pair of equal length messages m_0, m_1 in the message space.
3. A random $\hat{pk}$ is chosen. Uniform $b \in \{0, 1\}$ is flipped and ciphertext B and $c^* \leftarrow \mathsf{Enc}_{\hat{pk}}(m_b)$ given to $\mathcal{A}$.
4. $\mathcal{A}$ outputs b'. If $b' = b$ then $\mathcal{A}$ wins the experiment.

We observe that, using a random key, because Enc is a perfectly secret encryption scheme, c is independent of m, and B is independent of m.

Step 3. Reduction

Then we construct $\underline{D}$

- Receives A, B and K'.
- Forwards $pk = A$ to $\mathcal{A}$.
- $\mathcal{A}$ outputs m_0, m_1.
- D flips a bit b'. Then does $c^* \leftarrow \mathsf{Enc}_{K'}(m_{b'})$. Returns B, c^* to $\mathcal{A}$.
- If $\mathcal{A}$ correct return 1. Else 0.

Step 4. Analysis of Success probability of the reduction A.

Say W_0 is the event that D sees a random key, and W_1 is the event that D sees the key agreed upon by the parties, where W_0 and W_1 happen uniformly at random.

- Case 1: If K' is a random key, then $\mathcal{A}$ receives $pk = A$ and then the encryption $B, c^* \leftarrow \mathsf{Enc}_{K'}(m_b)$. B is chosen independently of m_b, and thus gives away no information about m_b. Since c^* is constructed with a random key K' (so B is unrelated to K' here), and Enc is perfectly secret, it also gives no information about m_b. Thus

$$Pr[\mathcal{A} \text{ wins } \mathsf{PubK}^{\mathsf{eav}}_{\tilde{\Pi},\mathcal{A}}] = \frac{1}{2} \implies$$
$$Pr[D = 1|W_0] = Pr[\mathcal{A} \text{ wins } \mathsf{PubK}^{\mathsf{eav}}_{\tilde{\Pi},\mathcal{A}}] = \frac{1}{2}.$$

- Case 2: If K' is the real key, then $\mathcal{A}$ receives $pk = A$, and encryption B, c^* where $c^* \leftarrow \mathsf{Enc}_{K'}(m_b)$. This looks exactly as an instance of the eavesdropping game and by assumption:

$$Pr[\mathcal{A} \text{ wins } \mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}] = \frac{1}{2} + p(\lambda) \implies$$
$$Pr[D = 1|W_1] = Pr[\mathcal{A} \text{ wins } \mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}] = \frac{1}{2} + p(\lambda).$$

We see then that:

$$|Pr[D = 1|W_0] - Pr[D|W_1]| = p(\lambda),$$

but by assumption, KA is secure, meaning

$$|Pr[D = 1|W_0] - Pr[D = 1|W_1]| \leq \mathsf{negl}(\lambda)$$

We conclude that Π must have indistinguishable encryptions in the presence of an eavesdropper and thus be CPA-secure.

□