Introduction to Modern Cryptography Recitation 7

Orit Moskovich
Tel Aviv University
December 14, 2016

Based on chapter 10.2.2 in Introduction to Modern Cryptography, Katz-Lindell

CPA Security

Adversarial indistinguishability experiment for A:

1. A random key (pk, sk) is generated using Gen
2. The adversary A is given pk and outputs a pair of messages m_0, m_1 of the same length
3. A random bit $b \leftarrow \{0,1\}$ is chosen
4. The ciphertext $c = Enc_{pk}(m_b)$ is computed and given to A
5. A outputs a bit b'

$$A \text{ wins} \Leftrightarrow b = b'$$

Definition. A PKE scheme (Gen, Enc, Dec) is **ε-CPA-secure** (chosen plaintext attack) if for every PPT adversary A it holds that $\Pr[A \text{ wins}] \leq \frac{1}{2} + \varepsilon$

Security for Multiple Encryptions

Adversarial indistinguishability experiment for A_{mult}:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_{mult} is given pk and outputs a pair of vectors $M_0 = (m_0^1, \dots, m_0^t)$ and $M_1 = (m_1^1, \dots, m_1^t)$, where $\forall i. |m_0^i| = |m_1^i|$
3. A random bit $b \leftarrow \{0,1\}$ is chosen
4. The vector $C = \left(Enc_{pk}(m_b^1), \dots, Enc_{pk}(m_b^t)\right)$ is given to A_{mult}
5. A_{mult} outputs a bit b'

$$A_{mult} \text{ wins} \Leftrightarrow b = b'$$

Definition. An encryption scheme is **ε-CPA-secure for multiple encryptions** if for every PPT adversary A_{mult} it holds that $\Pr[A_{mult} \text{ wins}] \leq \frac{1}{2} + \varepsilon$

Security for Multiple Encryptions

Theorem. If an encryption scheme is ε-CPA-secure, then it is ε_t-CPA-secure for multiple encryptions

- Proof – using hybrid arguments

Security for 2 Encryptions

- We'll start with the "easy" case

Theorem. If an encryption scheme is ε-CPA-secure, then it is ε'-CPA-secure for **2** encryptions

Security for Multiple Encryptions

- Let A_2 as follows:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_2 is given pk and outputs a pair of vectors $M_0 = (m_0^1, m_0^2)$ and $M_1 = (m_1^1, m_1^2)$
3. A random bit $b \leftarrow \{0,1\}$ is chosen
4. The vector $C = \left(Enc_{pk}\left(m_b^1\right), Enc_{pk}\left(m_b^2\right)\right)$ is given to A_2
5. A_2 outputs a bit b'

- We'll prove: $\Pr[A_2 \text{ wins}] \leq \frac{1}{2} + \varepsilon'$

Security for Multiple Encryptions – First Method

- Let A_1 as follows:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_1 is given pk runs A_2
3. A_2 outputs $M_0 = (m_0^1, \boldsymbol{m_0^2})$ and $M_1 = (m_1^1, \boldsymbol{m_1^2})$
4. A_1 outputs $\boldsymbol{m_0^2}, \boldsymbol{m_1^2}$
5. A random bit $b \leftarrow \{0,1\}$ is chosen
6. The ciphertext $c_2 = Enc_{pk}(\boldsymbol{m_b^2})$ is computed and given to A_1
7. A_1 encrypts $c_1 = Enc_{pk}(m_0^1)$ and sends (c_1, c_2) to A_2
8. A_1 outputs the bit b' that is output by A_2

Security for Multiple Encryptions – First Method

- We'll prove: $\Pr[A_2 \text{ wins}] \leq \frac{1}{2} + \varepsilon'$

$$\frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_0^2})\right)\right]\right]$$
$$+\frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_1^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$

Security for Multiple Encryptions – First Method

- We'll prove: $\Pr[A_2 \text{ wins}] \leq \frac{1}{2} + \varepsilon'$

- $\frac{1}{2} + \varepsilon \geq \Pr[A_1 \text{ wins}]$ (Enc is ε-CPA secure)

- $\Pr[A_1 \text{ wins}] = \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 1 \mid b = 1]$

$$= \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_0^2})\right)\right]\right]$$
$$+ \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\leq \frac{1}{2} + \varepsilon$$

Security for Multiple Encryptions – First Method

- We'll prove: $\Pr[A_2 \text{ wins}] \leq \frac{1}{2} + \varepsilon'$

- $\frac{1}{2} + \varepsilon \geq \Pr[A_1 \text{ wins}]$ (Enc is ε-CPA secure)

- $\Pr[A_1 \text{ wins}] = \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 1 \mid b = 1]$

$$= \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_0^2})\right)\right]\right]$$
$$+ \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\leq \frac{1}{2} + \varepsilon$$

Security for Multiple Encryptions – First Method

- We can do similar experiment, only changing the second encryption:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_1 is given pk runs A_2
3. A_2 outputs $M_0 = (m_0^1, \boldsymbol{m_0^2})$ and $M_1 = (m_1^1, \boldsymbol{m_1^2})$
4. A_1 outputs m_0^1, m_1^1
5. A random bit $b \leftarrow \{0,1\}$ is chosen
6. The ciphertext $c_1 = Enc_{pk}(m_b^1)$ is computed and given to A_1
7. A_1 encrypts $c_2 = Enc_{pk}(\boldsymbol{m_1^2})$ and sends (c_1, c_2) to A_2
8. A_1 outputs the bit b' that is output by A_2

Security for Multiple Encryptions – First Method

- Similarly:

- $\frac{1}{2} + \varepsilon \geq \Pr[A_1 \text{ wins}]$ (Enc is ε-CPA secure)

- $\Pr[A_1 \text{ wins}] = \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 1 \mid b = 1]$

$$= \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$+ \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_1^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\leq \frac{1}{2} + \varepsilon$$

Security for Multiple Encryptions – First Method

- Similarly:

- $\frac{1}{2} + \varepsilon \geq \Pr[A_1 \text{ wins}]$ (Enc is ε-CPA secure)

- $\Pr[A_1 \text{ wins}] = \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 1 \mid b = 1]$

$$= \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$+ \frac{1}{2} \cdot \left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_1^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\leq \frac{1}{2} + \varepsilon$$

Security for Multiple Encryptions – First Method

- Combine both results:

$$\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_0^2})\right)\right]\right]$$
$$+\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$+\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_1^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\leq 1 + 2\varepsilon$$

Security for Multiple Encryptions – First Method

- Combine both results:

$$\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_0^2})\right)\right]\right]$$
$$+\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 0 \text{ on } \left(Enc_{pk}(m_0^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$+\frac{1}{2}\cdot\left[\Pr\left[A_2 \text{ outputs } 1 \text{ on } \left(Enc_{pk}(m_1^1), Enc_{pk}(\boldsymbol{m_1^2})\right)\right]\right]$$
$$\leq 1 + 2\varepsilon$$

➔ $\Pr[A_2 \text{ wins}] \leq \frac{1}{2} + 2\varepsilon$

Security for Multiple Encryptions – Second Method

- Let A_1 as follows:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_1 is given pk runs A_2
3. A_2 outputs $M_0 = (m_0^1, m_0^2)$ and $M_1 = (m_1^1, m_1^2)$
4. A_1 chooses a random index $i \in \{1,2\}$ and outputs m_0^i, m_1^i
5. A random bit $b \leftarrow \{0,1\}$ is chosen
6. The ciphertext $c_i = Enc_{pk}(m_b^i)$ is computed and given to A_1
   - If $i = 1$: A_1 encrypts $c_2 = Enc_{pk}(m_1^2)$ and sends c_i, c_2 to A_2
   - If $i = 2$: A_1 encrypts $c_1 = Enc_{pk}(m_0^1)$ and sends c_1, c_i to A_2
7. The vector $C = (c_1, c_2)$ is given to A_2
8. A_1 outputs the bit b' that is output by A_2

Security for Multiple Encryptions – Second Method

- We'll prove: $\Pr[A_2 \text{ wins}] \leq \frac{1}{2} + \varepsilon'$
- $\frac{1}{2} + \varepsilon \geq \Pr[A_1 \text{ wins}]$ (Enc is ε-CPA secure)
- $\Pr[A_1 \text{ wins}] = \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[A_1 \text{ outputs } 1 \mid b = 1]$
- $$\begin{aligned}\Pr[A_1 \text{ outputs } 0 \mid b = 0] = {} & \Pr[A_1 \text{ outputs } 0 \mid b = 0 \wedge i = 1] \cdot \Pr[i = 1] \\ & + \Pr[A_1 \text{ outputs } 0 \mid b = 0 \wedge i = 2] \cdot \Pr[i = 2]\end{aligned}$$
- $$\begin{aligned}\Pr[A_1 \text{ outputs } 1 \mid b = 1] = {} & \Pr[A_1 \text{ outputs } 1 \mid b = 1 \wedge i = 1] \cdot \Pr[i = 1] \\ & + \Pr[A_1 \text{ outputs } 1 \mid b = 1 \wedge i = 2] \cdot \Pr[i = 2]\end{aligned}$$

Security for Multiple Encryptions

- How do we generalize this method to t encryptions?

- For a given public key pk and two vectors
  $M_0 = (m_0^1, \dots, m_0^t)$ and $M_1 = (m_1^1, \dots, m_1^t)$
  (the output of A_{mult})

- Define $C^i = \left(\underbrace{Enc_{pk}(m_0^1), \dots, Enc_{pk}\left(m_0^i\right)}, \underbrace{Enc_{pk}\left(m_1^{i+1}\right), \dots, Enc_{pk}(m_1^t)}\right)$

Security for Multiple Encryptions

- Let A_t as follows:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_t is given pk and outputs a pair of vectors $M_0 = (m_0^1, \dots, m_0^t)$ and $M_1 = (m_1^1, \dots, m_1^t)$, where $\forall i. \left|m_0^i\right| = \left|m_1^i\right|$
3. A random bit $b \leftarrow \{0,1\}$ is chosen
4. The vector $C = \left(Enc_{pk}(m_b^1), \dots, Enc_{pk}(m_b^t)\right)$ is given to A_t
5. A_t outputs a bit b'

- We'll prove: $\Pr[A_t \text{ wins}] \leq \frac{1}{2} + \varepsilon_t$

Security for Multiple (t) Encryptions – Second Method

- Let A_1 as follows:

1. A random key (pk, sk) is generated using Gen
2. The adversary A_1 is given pk runs A_t
3. A_t outputs $M_0 = (m_0^1, \dots, m_0^t)$ and $M_1 = (m_1^1, \dots, m_1^t)$
4. A_1 chooses a random index $i \in \{1, \dots, t\}$ and outputs m_0^i, m_1^i
5. A random bit $b \leftarrow \{0,1\}$ is chosen
6. The ciphertext $c_i = Enc_{pk}(m_b^i)$ is computed and given to A_1
   - For $j < i$: A_1 encrypts $c_j = Enc_{pk}(m_0^j)$
   - For $j > i$: A_1 encrypts $c_j = Enc_{pk}(m_1^j)$
7. The vector $C = (c_1, \dots, c_i, \dots, c_t)$ is given to A_t
8. A_1 outputs the bit b' that is output by A_t

Partially Homomorphic Encryption

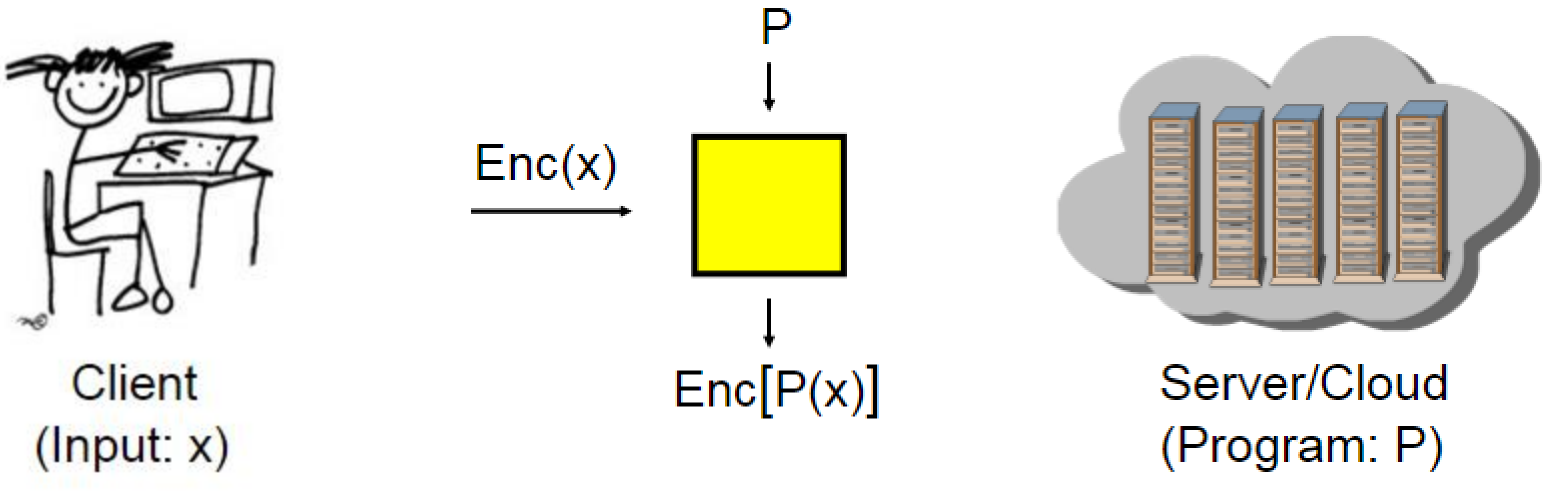
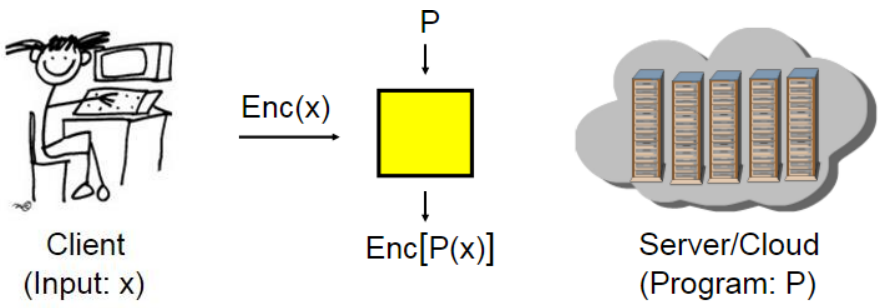


Image from: http://slideplayer.com/slide/236532/

Partially Homomorphic Encryption



Definition. A PKE scheme (Gen, Enc, Dec) is (partially) **homomorphic** if for all pk, sk and for all m_1, c_1, m_2, c_2:

$m_1 = Dec_{sk}(c_1)$ and $m_2 = Dec_{sk}(c_2)$ ➔

$$Dec_{sk}(c_1 \tilde{\odot} c_2) = m_1 \odot m_2$$

Partially Homomorphic Encryption

- El Gamal PKE scheme:
- $pk = (G, q, g, g^x = h)$
- $sk = x$

- $Enc_{pk}(m_1) = (g^y, h^y \cdot m_1) = c_1$
- $Enc_{pk}(m_2) = \left(g^{y'}, h^{y'} \cdot m_2\right) = c_2$

- $\Rightarrow$ $c_1 \cdot c_2 = \left(g^{y+y'}, h^{y+y'} \cdot (m_1 m_2)\right)$
- $\Rightarrow$ $Dec_{sk}(c_1 \cdot c_2) = m_1 m_2$

Partially Homomorphic Encryption

- El Gamal PKE scheme:
- $pk = (G, q, g, g^x = h)$
- $sk = x$

- $Enc_{pk}(m_1) = (g^y, h^y \cdot m_1) = c_1$
- $Enc_{pk}(m_2) = \left(g^{y'}, h^{y'} \cdot m_2\right) = c_2$

- ➔ $c_1 \cdot c_2 = \left(g^{y+y'}, h^{y+y'} \cdot (m_1 m_2)\right)$
- ➔ $Dec_{sk}(c_1 \cdot c_2) = m_1 m_2$