University of Michigan–Ann Arbor

Department of Electrical Engineering and Computer Science

EECS 475 **Introduction to Cryptography**, Winter 2023

Lecture 22: CPA security continued, El Gamal cryptosystem

March 29, 2023

Lecturer: Mahdi Cheraghchi

Scribe: Yi-Wen Tseng

1 CPA Security

In continuation of the previous class, we want to show that one-query CPA implies many-query CPA.

Image a many-query attacker A that makes up to q queries where $q \in poly(n)$. Consider the following worlds:

Hybrid 0 (Left World) : all queries (m_0, m_1) to the LR oracle are answered by $c \leftarrow Enc_{pk}(m_0)$.

Hybrid 1 : First query (m_0, m_1) to the LR oracle is answered by $c \leftarrow Enc_{pk}(m_1)$, then $c \leftarrow Enc_{pk}(m_0)$ thereafter.

Hybrid 2 : First 2 queries (m_0, m_1) to the LR oracle are answered by $c \leftarrow Enc_{pk}(m_1)$, then $c \leftarrow Enc_{pk}(m_0)$ thereafter.

$\vdots$

Hybrid q (Right World) : all queries (m_0, m_1) to the LR oracle are answered by $c \leftarrow Enc_{pk}(m_1)$.

Note here, the only difference between $Hybrid(i-1)$ and $Hybrid(i)$ is how the i^{th} query is answered.
Now, we build a "simulator" $S_i^{LR_{pk,b}(\cdot,\cdot)}(pk)$ that gets **one query** and simulates either $Hybrid(i-1)$ or $Hybrid(i)$ depending on b.

On j^{th} query of A (m_0^j, m_1^j):

- If $j < i$, S_i runs $c \leftarrow Enc_{pk}(m_1^j)$
- If $j > i$, S_i runs $c \leftarrow Enc_{pk}(m_0^j)$
- If $j = i$, S_i queries to LR oracle and gives the result to A

$$\begin{cases} S_i \text{ is in the left world } (b=0)\text{, then we perfectly simulate } Hybrid(i-1) \\ S_i \text{ is in the right world } (b=1)\text{, then we perfectly simulate } Hybrid(i) \end{cases} \tag{1}$$

By triangle inequality,

$$\begin{aligned} Adv_{\pi}^{CPA}(A) &= \left|Pr(A=1 \text{ in } Hybrid(0)) - Pr(A=1 \text{ in } Hybrid(q))\right| \\ &= \big|Pr(A=1 \text{ in } Hybrid(0)) - Pr(A=1 \text{ in } Hybrid(1)) + Pr(A=1 \text{ in } Hybrid(1)) \\ &\quad - Pr(A=1 \text{ in } Hybrid(2)) + Pr(A=1 \text{ in } Hybrid(2)) \cdots - Pr(A=1 \text{ in } Hybrid(q))\big| \\ &\le \sum_{i=1}^{q} Adv_{\pi}^{single-CPA}(S_i) = q\dot{n}egl(n) = negl(n) \end{aligned}$$

The theorem implies we can encrypt long messages bit-by-bit (or block-by-block) or broken up in any other many calls on "short" messages, which is acceptable by the theorem.

Theorem: Any public key encryption scheme wit deterministic $Enc_{pk}(.)$ can not be CPA secure **even for 1 query**.
Proof: query $c \leftarrow LR_{pk,b}(m_0, m_1)$ for any $m_0 \neq m_1$. Then, run $c' = Enc_{pk}(m_0)$. If $c = c'$ outputs 0, else 1. Because the adversary knows the query (m_0, m_1), the adversary has perfect advantage on distinguishing c and c'.

2 El Gamal Cryptosystem

El Gamal is the public key encryption version of Diffie Hellmen. It works as follows: