

CS6846 – Quantum Algorithms and Cryptography

Building Public Key Encryption



Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Public Key Encryption.

Security Parameter is λ .

Keygen/Setup (1^λ) \rightarrow PK, SK.
 $\in \mathcal{M}$ (msg space)

Encrypt (PK, m) \rightarrow CT.

Decrypt (CT, SK) \rightarrow m'

Correctness: If Keygen, Encrypt & Decrypt are run honestly, I should recover m .

$$\Pr \left(m' = m \mid \begin{array}{l} (PK, SK) \leftarrow \text{Keygen}(1^\lambda) \\ CT \leftarrow \text{Encrypt}(PK, m) \\ m' \leftarrow \text{Decrypt}(CT, SK) \end{array} \right) \geq 1 - \text{negl}(\lambda)$$

Security (IND-CPA): An Encryption scheme is said to be IND-CPA secure iff no PPT adversary \mathcal{A} has non-negligible advantage in the following game:

- 1). Challenger generates $(PK, SK) \leftarrow \text{Keygen}(1^\lambda)$ & gives PK to \mathcal{A} .
- 2). \mathcal{A} chooses M_0 & M_1 of same length.
- 3). Challenger chooses $b \in \{0, 1\}$ & gives $CT^* = \text{Encrypt}(PK, M_b)$ to \mathcal{A} .
- 4). \mathcal{A} outputs $b' \in \{0, 1\}$ & wins if $b' = b$.

The scheme is $\text{IND}_{\Delta}^{\text{CPA}}$ secure if \mathcal{A} cannot win the IND-CPA game with probability non-negligibly better than $1/2$.

$$\text{Adv}_{\mathcal{A}}(\lambda) = \left| \Pr(b' = b) - \frac{1}{2} \right|$$

Want $\text{Adv}_{\mathcal{A}}(\lambda)$ to be negligible in λ .

Decision Diffie-Hellman assumption (DDH): Let G be a cyclic group of prime order $q > 2^n$. The DDH assumption holds if the distributions

$$D_0 = \left\{ (g, g^a, g^b, g^{ab}) \mid a, b \xleftarrow{\text{sampled randomly}} \mathbb{Z}_q \right\}$$

$$\text{and } D_1 = \left\{ (g, g^a, g^b, g^c) \mid a, b, c \xleftarrow{\text{sampled randomly}} \mathbb{Z}_q \right\}.$$

are computationally indistinguishable (i.e. $\forall \text{PPT } \mathcal{A}$)

ElGamal Encryption:

Keygen(1^n) \rightarrow PK, SK

- Choose G of prime order q , with g as generator
- Sample $x \leftarrow \mathbb{Z}_q$. Compute $X = g^x$.
- PK = $(g, X = g^x)$ SK = (x) .

Encrypt(PK, M) \rightarrow CT

- $M \in G$.

- Choose $n \leftarrow \mathbb{Z}_q$.

- set $C = (\underline{C_1}, \underline{C_2})$ where $C_1 = g^n$, $C_2 = M \cdot X^n$.

$$\begin{aligned} X &= g^x \\ X^n &= g^{xn} \end{aligned}$$

\downarrow

Decrypt(SK, CT) \rightarrow M' .

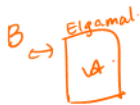
$$C_2 / C_1^n = \frac{M \cdot X^n}{(g^n)^n} = \frac{M \cdot g^{xn}}{g^{xn}} = M.$$

Correctness holds.

Security.

Theorem: The Elgamal Encryption scheme satisfies IND-CPA security iff the DDH assumption holds in group G .

Proof: Suppose A is an adversary with non-negligible advantage ϵ . We will construct a DDH distinguisher B . Here, B takes as input (g, g^a, g^b, T) where $a, b \stackrel{R}{\leftarrow} \mathbb{Z}_q$ and $T = g^{ab}$ or T is random in G .



- ① B chooses PK as $(g, x = g^a)$
- ② A outputs $M_0, M_1 \in G$.

- ③ B computes the ciphertext
 $C_1 = g^b, C_2 = M_b \cdot T.$

B receives
 g, g^a, g^b
 T

- ④ A guesses the bit, outputs b' .

- ⑤ If $b' = b$, then B says "real" (ie. $T = g^{ab}$)
else it says "random" (ie. $T = g^c$).
outputs 1.
outputs 0.

$$T \rightarrow g^{ab}$$

$$\rightarrow \underline{\underline{g^c}}$$

$$C_2 = M_b \cdot g^{ab}$$

$$C_2 = M_b \cdot \text{Random}$$

C_2 is itself random.

$$\Pr(B \rightarrow 1 \mid T = g^{ab}) = \Pr(b = b' \mid T = g^{ab})$$
$$= \frac{1}{2} + \epsilon.$$

On the other hand

$$\Pr(B \rightarrow 1 \mid T = g^c) = \frac{1}{2}.$$

So Advantage of B

$$\begin{aligned} \text{Adv}_B(\lambda) &= \left| \Pr[B \rightarrow 1 \mid T = g^{ab}] - \Pr[B \rightarrow 1 \mid T = g^c] \right| \\ &= \varepsilon. \end{aligned}$$

Advantage of A translates to Advantage of B.
