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 $(1^\lambda) \rightarrow PK, SK$.

Encrypt $(PK, m) \rightarrow CT$ $\in \mathcal{M}$ (msg space)

Decrypt $(CT, SK) \rightarrow m'$

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

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

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 $b \leftarrow \{0,1\}$ & 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 IND-CPA secure if $\mathcal{A}$ cannot win the IND-CPA game with probability non-negligibly better than 1/2.

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

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

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

sampled randomly

$$D_0 = \{ (g, g^a, g^b, g^{ab}) \mid a, b \xleftarrow{R} \mathbb{Z}_q \}$$

and

$$D_1 = \{ (g, g^a, g^b, g^c) \mid a, b, c \xleftarrow{R} \mathbb{Z}_q \}.$$

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

ElGamal Encryption:

Keygen$(1^\lambda) \to PK, SK$

- 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$(PK, M) \to CT$

$X = g^x$
$X^r = g^{xr}$

- $M \in G$.
- Choose $r \xleftarrow{R} \mathbb{Z}_q$.
- set $C = (C_1, C_2)$ where $C_1 = g^r$, $C_2 = M \cdot X^r$.

Decrypt$(SK, CT) \to M'$.

$$C_2 / C_1^x = \frac{M \circ X^r}{(g^r)^x} = \frac{M \circ g^{xr}}{g^{xr}} = M.$$

Correctness holds.

Security.

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

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

$B \leftrightarrow$ Elgamal $\boxed{\mathcal{A}}$

① $\mathcal{B}$ chooses PK as $(g, X = g^a)$

② $\mathcal{A}$ outputs $M_0, M_1 \in G$.

③ $\mathcal{B}$ computes the ciphertext

$$C_1 = g^b, \quad C_2 = M_b \cdot T.$$

$\mathcal{B}$ receives g, g^a, g^b, T

④ $\mathcal{A}$ guesses the bit, outputs b'.

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

$$T \to g^{ab} \qquad C_2 = M_b \cdot g^{ab}$$

$$T \to \underline{\underline{g}}^{c}. \qquad C_2 = M_b \cdot \text{Random}$$

C_2 is itself random.

$$\Pr\left(\mathcal{B} \to 1 \,\middle|\, T = g^{ab}\right) = \Pr\left(b = b' \,\middle|\, T = g^{ab}\right)$$

$$= \frac{1}{2} + \varepsilon.$$

On the other hand

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

So Advantage of $\mathcal{B}$

$$Adv_{\mathcal{B}}(\lambda) = \left| \Pr[B \to 1 \mid T = g^{ab}] - \Pr[B \to 1 \mid T = g^c] \right|$$

$$= \varepsilon.$$

Advantage of $\mathcal{A}$ translates to Advantage of $\mathcal{B}$.