Provable security - CCA enc)

(c_1, c_2)

$\downarrow^n$, $y^n \cdot m$.

$\downarrow$

g^y, $y^n \cdot 2m$.

It is indistinguishable:

$C \longrightarrow PK \rightarrow A$.

$c = E(m_b)$

Dec oracle

A wins if $b = b'$

$\left| Pr(b=b') - \frac{1}{2} \right| \leq neg(\text{sec parm})$.

---

oracle model:

decryption oracle:

$C^e \xleftarrow{c}$

$m ?\ t \rightarrow$

chosen cipher text Attack

CCA

Hash function

- Training phase
- Challenge
- Response

oracle.
Enc
Dec.
Hash.
Random oracle.

Ciphertext only Attack:

$(m_1, C_m) \rightarrow Enc$

$(c, m_c) \rightarrow Dec.$

$C \xrightarrow{PK} A$

$\xleftarrow{(m_0, m_1)}$

$\xrightarrow{c = e(m_b)}$

$\xleftarrow{b'}$

A wins if $b = b'$.

---

cyclic group of prime order.

every element is a generator

---

g_1, g_2 two gen of $\underline{G}$.

Key Gen:

$x, y \leftarrow Z_q$.

$h = g_1^x g_2^y$ //

$PK = (g_1, g_2, h)$.

$SK = (x, y)$.

Enc (m)

$r \leftarrow Z_q$.

output $\langle g_1^r, g_2^r, h^r \cdot m \rangle$.

Dec (u, v, e).

$m = \frac{e}{u^x v^y}$.

$u^x v^y = g_1^{rx} \cdot g_2^{ry}$

$= (g_1^x g_2^y)^r$

$= h^r$

$\left\{ \frac{e}{u^x v^y} = \frac{e}{h^r} = \frac{h^r m}{h^r} = m \right\}$

A

g_1, g_2, g_3, g_4

$g_3 = g_1^{x'}$

$g_4 = g_2^{y'}$

$\rightarrow g_1, g_2, g_3, g_4$

A is an oracle where we can ask g_3^r for any r that we want

g_3^r

$h = h'$

$h \neq h'$.

A' (g_1, g_2, g_3, g_4).

$x, y \leftarrow Z_q$.

$h = g_1^x g_2^y$.

$PK = \langle g_1, g_2, h \rangle$.

$\{m_0, m_1\} \leftarrow A(PK)$

$b \leftarrow \{0,1\}$

$C = \langle g_3, g_4, g_3^x g_4^y m_b \rangle$

$b' = A(PK, C)$

if $(b = b')$ then output "DDH Triple"

else output "Random Triple"

$\{g_1, g_2, g_3, g_4\}$ is a DDH Triple.

else output (g_1, g_2, g_3, g_4) is a Random triple.

Suppose g_1, g_2, g_3, g_4 is a DDH Triple:

$\Rightarrow \exists\ \underline{r} \Rightarrow$

$g_3 = g_1^r$, $g_4 = g_2^r$.

$g_3^x g_4^y = g_1^{rx} g_2^{ry}$

$= g_1^{rx} g_2^{ry} g_1^x$

$C = \langle g_3, g_4, g_3^x g_4^y m_b \rangle$

$= \langle g_1^r, g_2^r, g_1^{rx} m_b \rangle$.

Then C will be a valid ciphertext for m_b.

$\Rightarrow$ A will return a b' with the prop that $Pr(b = b') = \frac{1}{2} + \epsilon$.

The conclusion of A' is correct with prob $\frac{1}{2} + \epsilon$.

$g_3 = g_1^r$

$g_4 = g_2^{r'}$

C

$(g_3, g_4, g_3^x g_4^y \cdot m_b)$.

$h = g_1^x g_2^y$

$e = g_3^x g_4^y m_0$

Determine a unique pair (x_0, y_0).

$h = g_1^x \cdot (g_2^x)^y$.

$C = g_1^{rx} \cdot (g_2^{rx})^y \cdot m_0$

$\log_{g_1} h = x + \alpha y$

$\log_{g_1} e = rx + \alpha r' y + \log_{g_1} m_0$

$\log_{g_1} e - \log_{g_1} m_0 = \underline{r} x + \alpha r' y$

There is a unique sol for the eq. (x_0, y_0).

Had A' chosen x_0, y_0 as key:

Then, $h = g_1^{x_0} g_2^{y_0}$.

$= g_1^{x_0} g_2^{x_0 y_0}$

$= g_1^{x_0 + \alpha x_0}$

$m_0 \rightarrow m_1$

(x_1, y_1)

$\Rightarrow$ C looks like an encryption of m_0 under the key (x_0, y_0) as well as encryption of m_1 under the key (x_1, y_1).

if (g_1, g_2, g_3, g_4) were a DDH Triple, A's response will be correct with prob $\frac{1}{2} + \epsilon$.

if (g_1, g_2, g_3, g_4) were not a DDH Triple A is completely lost & his response will probably look like a random bit.

$\{0, 1\}$

$x + h = 60$

$\geq 3/4$

$\frac{1}{2} + \epsilon$

$\frac{1}{2}$ $\frac{1}{2}$

A'. $\longrightarrow \epsilon$ - dist.