1 OAEP and IND-CPA

Recall the OAEP we learned in last lesson, plaintext:

\[ m \rightarrow (G(r) \oplus (m \parallel 0^{K_1})) \parallel (H(s) \oplus r) \]

Here, \( m \) is \( K - K_0 - K_1 \) bits; \( s \) is \( G(r) \oplus (m \parallel 0^{K_1}) \), \( K - K_0 \) bits; \( t \) is \( H(s) \oplus r \), \( K_0 \) bits.

The central idea for using OAEP, instead of encryption \( m \), \( f(s \parallel t) \) is the encryption of \( m \).

Avoid supplying more information about plaintext to adversary by more random distribution. For example, \( f \) is RSA, \( f(x) = x^e \mod n \). If \( c \leftarrow f(x) \), then it holds that \( 2^e c \mod n = f(2x) \). But \( 2x \) is \( OAEP^{-1} \), that is,

\[ s \parallel t \rightarrow integer \]
\[ (2V \mod n) \rightarrow s_1 \parallel t_1 \]

**Plaintext Awareness**: if an adversary produces a ciphertext \( \phi \) that is “decryptable” then he must know the plaintext.

We want to show now that \( f - OAEP \) is \( IND - CPA \) secure under the assumption that \( f \) is a \( OWTP \).

The IND-CPA Game is shown in the figure 1. The modified game is shown in figure 2.

* shows if adversary makes \( h \) query to \( H \) either use \( H(h) \) if \( < h, H(h) > \in T_H \) or choose \( H(h) \) at random.

For each \( < g, G(g) > \in T_G, w_{h,g} = h \parallel (H(h) \oplus g) \).

If \( f(w_{h,g}) = y \), then we found \( f^{-1}(y) \)!

Similarly for query \( g \) to \( G \).

Proved.

The IND-CCA, IND-CCA2 Game are shown in figure 3.

2 Cramer Shoup Public-key Cryptosystem

This scheme is proposed in 1998.
GEN:

$Z_p^*$, $q$. Let $G$ be a subgroup of $Z_p$ of order $q$.
$x_1, x_2, y_1, y_2, z \leftarrow_R Z_q.$
$g_1, g_2 \leftarrow_R G,$
c $= g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^Z,$ and a hash function $H : G^3 \rightarrow Z_q.$

public key: $(g_1, g_2, c, d, h, H)$, secret key: $(x_1, x_2, y_1, y_2, z)$.

Encryption:

Encryption of $m \in G$, choose $r \leftarrow_R Z_q.$

$u_1 \leftarrow g_1^r.$
$u_2 \leftarrow g_2^r.$
Figure 3: The IND-CCA, IND-CCA2 Game.

e \leftarrow h^r m.
\alpha \leftarrow H(u_1, u_2, e).
v \leftarrow c^d r^\alpha.

Ciphertext: \((u_1, u_2, e, v)\).
Observe: \((u_1, e)\) is ElGamal Cipher with pk: \((g, h)\), sk: \((z)\).

Decryption:
Given \((V_1, V_2, E, V)\),
Compute \(\alpha = H(V_1, V_2, E)\).
Check if \(V_1^{x_1+y_1\alpha} V_2^{x_2+y_2\alpha} = V\).
If yes, return \(E/h^2\), else fail.

Observe: \(V_1 = g_1^r, V_2 = g_2^r, E = h^r m\), so we have,
\(V_1^{x_1+y_1\alpha} V_2^{x_2+y_2\alpha} = g_1^{r(x_1+y_1\alpha)} g_2^{r(x_2+y_2\alpha)} = (g_1^{y_1} g_2^{y_2})^r (g_1^{y_1} g_2^{y_2})^r = c^d r^\alpha = V\)