IND-CCA Attack

1. \(< pk, sk >\leftarrow GEN(1^k)\)
2. \(< aux, m_0, m_1 >\leftarrow A^{DEC(s_k, \cdot)}(play, 1^k, pk)\)
3. \(b \leftarrow R\{0,1\}\)
4. \(\psi \leftarrow ENC(m_b)\)
5. \(b^* \leftarrow A(guess, aux, \psi)\)
6. if \(b = b^*\) then succeed else fail

The Chosen Ciphertext Attack (CCA) is also known as “lunch-time” attack. It assumes that the attacker can use the decryption device and sees the encryption algorithm as an idealized opaque box.

Issue: It is not clear how to prove that encryption schemas are secure against this attack.

Intuition: Encryption should be “plaintext aware”, that is if ciphertext \(\psi\) prepared by the adversary is “decryptable”, then the adversary knows the corresponding plaintext.

“Adaptive” IND-CCA2 Attack

It captures the properties from both lunch-time attack and non-malleability. It is a satisfactory proof of security of a schema.

1. \(< pk, sk >\leftarrow GEN(1^k)\)
2. \(< aux, m_0, m_1 >\leftarrow A^{DEC(s_k, \cdot)}(play, 1^k, pk)\)
3. \(b \leftarrow R\{0,1\}\)
4. \(\psi \leftarrow ENC(m_b)\)
5. \(b^* \leftarrow A^{DEC^{-\psi}(s_k, \cdot)}(guess, aux, \psi)\)
6. if \(b = b^*\) then succeed else fail

Non-malleability

Non-malleability implies that the scheme cannot be attacked by using a malleability attack:

Given a ciphertext \(\psi\) the attacker outputs \(\psi'\) and some relation \(R\) s.t.
\(R(DEC(s_k, \psi), DEC(s_k, \psi')) = true\)
El Gamal is Malleable

\[< G, H >= < g^n, h^n \cdot M >\]
\[< G', H' >= < G, H \cdot 2 >\]
\[DEC(G', H') = 2 \cdot M\]
\[DEC(G, H) = M\]

there is a predictable relationship \( R \) between both decryptions

Optimal Asymmetric Encryption Padding (OAEP)

Goal: turn any “one-way trapdoor permutation” (OWTP) into an IND-CCA secure encryption

Example of an OWTP:
RSA cryptosystem
\[x \rightarrow x^e mod n\]
it is bijective, hard to invert and easy to compute.
Trapdoor: factorization of \( e \)

Description of OAEP

Randomized mapping
\[\{0, 1\}^{k-k_0-k_1} \rightarrow \{0, 1\}^k\]
\[G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0} \text{ "generator"}\]
\[H : \{0, 1\}^{k-k_0} \rightarrow \{0, 1\}^{k_0} \text{ "hash"}\]

Example: for 1024 bit RSA
\[k = 1024\]
Suggested values:
\[k_0 = 160\]
\[k_1 = 160\]
OAEP Function

Given $m \in \{0, 1\}^{k-k_0-k_1}$
OAEP: Select $r \leftarrow \{0, 1\}^{k_0}$
$[G(r) \oplus (m||O_k)||H(s) \oplus r]$

Inversion of OAEP

given $(s,t)$
$[G(H(s) \oplus t) \oplus s, H(s) \oplus t]$

How to use OAEP?

Given OWTP $f$
to encrypt
$f(OAEP(m)) \rightarrow c$
to decrypt
$OAEP^{-1}(f(c))$
take first $k-k_0$ bits and test whether they contain $k_1$ zeroes in the end
if yes return first $k-k_0-k_1$
else fail
This offers a protection, if $\psi$ is tweaked, it would fail