COM S 6830 – Cryptography Oct 8, 2009

Lecture 13: CCA2-Secure Encryption and Public-Key Encryption

Instructor: Rafael Pass *Scribe: Edward Lui*

1 Review of CPA/CCA1/CCA2 Secure Encryption

Let $\Pi = (Gen, Enc, Dec)$ be an encryption scheme. For any non-uniform PPT machine A, $n \in \mathbb{N}$, and $b \in \{0,1\}$, let $IND_b^{O1,O2}(\Pi, A, n)$ be the probability distribution describing the output of the following experiment:

$$\begin{aligned}
&k \leftarrow Gen(1^n)\\
&m_0, m_1, \sigma \leftarrow A^{O_1(k)}(1^n)\\
&c \leftarrow Enc_k(m_b)\\
&\text{Output } A^{O_2(k,c)}(c, \sigma).
\end{aligned}$$

We say that Π is *CPA/CCA1/CCA2 secure* if for every non-uniform PPT machine A, we have

$$\{IND_0^{O_1,O_2}(\Pi, A, n)\}_{n\in\mathbb{N}} \approx \{IND_1^{O_1,O_2}(\Pi, A, n)\}_{n\in\mathbb{N}},$$

where O_1, O_2 are defined as:

Security	$O_1(k)$	$O_2(k,c)$
CPA	$(Enc_k, \cdot)$	—
CCA1	(Enc_k, Dec_k)	—
CCA2	(Enc_k, Dec_k)	(Enc_k, Dec'_k)

where $Dec'_k(c') = Dec_k(c')$ if $c' \neq c$, and $Dec'_k(c') = \perp$ otherwise.

Last lecture, we showed that the following encryption scheme is multi-message secure if $\{f_k \colon \{0,1\}^{|k|} \to \{0,1\}^{|k|}\}_{k\in\{0,1\}^*}$ is a family of PRFs:

$$\begin{aligned}
&Gen(1^n) : k \leftarrow \{0,1\}^n;\ \text{output } k.\\
&Enc_k(m) : r \leftarrow \{0,1\}^{|m|};\ \text{output } r||(m \oplus f_k(r)).\\
&Dec_k(r||c) :\ \text{Output } c \oplus f_k(r).
\end{aligned}$$

It is not hard to show that the above multi-message secure encryption scheme is also CPA secure and CCA1 secure. However, the encryption scheme is not CCA2 secure, since when the adversary receives the challenge ciphertext $r||c$, the adversary can ask the decryption oracle the query $r||0$ to obtain $f_k(r)$, which would allow the adversary to decrypt the challenge ciphertext.

2 A CCA2-Secure Encryption Scheme

We now construct an encryption scheme that is CCA2 secure.

Let $\{f_s\colon \{0,1\}^{|s|} \to \{0,1\}^{|s|}\}_{s\in\{0,1\}^*}, \{g_s\colon \{0,1\}^{|s|} \to \{0,1\}^{|s|}\}_{s\in\{0,1\}^*}$ be families of PRFs. Consider the following encryption scheme:

$Gen'(1^n)$: $s_1 \leftarrow \{0,1\}^n; s_2 \leftarrow \{0,1\}^{2n}$; output $s_1||s_2$.
$Enc'_{(s_1||s_2)}(m)$: Output $c_1||c_2$, where $c_1 = r||(m \oplus f_{s_1}(r))$ and $c_2 = g_{s_2}(c_1)$, where $r \leftarrow \{0,1\}^{|s_1|}$.
$Dec'_{(s_1||s_2)}(r||c'_1||c_2)$: Output $c'_1 \oplus f_{s_1}(r)$ if $c_2 = g_{s_2}(r||c'_1)$; otherwise, output $\perp$.

We note that $Enc'_{(s_1||s_2)}(m) = c_1||g_{s_2}(c_1)$, where $c_1 = Enc_{s_1}(m)$.

Theorem 1 *(Gen', Enc', Dec') is $CCA2$ secure.*

Proof. Suppose $\Pi' := (Gen', Enc', Dec')$ is not $CCA2$ secure. Then, there exists a non-uniform PPT machine A' that breaks CCA2 security of (Gen', Enc', Dec'). Using A', we will construct a non-uniform PPT machine A that breaks the CPA security of $\Pi := (Gen, Enc, Dec)$ (the encryption scheme defined earlier), which contradicts the fact that Π is CPA secure.

Let Enc_{s_1} be the encryption oracle for A. On input 1^n, A simulates A' on the same input. Each time A' makes the encryption query m (which would normally be for obtaining $c_1||c_2$ for some $c_1 = Enc_{s_1}(m)$ and $c_2 = g_{s_2}(c_1)$), A asks its own encryption oracle Enc_{s_1} to get $c = Enc_{s_1}(m)$. Then, A lets $r_c \leftarrow \{0,1\}^{|c|}$ and responds to A' with the answer $c||r_c$, and A stores (m, c, r_c) so that it can answer the decryption queries of A' consistently.

Each time A' makes the decryption query $c_1||c_2$, if A has stored (m, c_1, c_2) previously, then A answers m; otherwise, A answers $\perp$.

When A' outputs m_0, m_1, σ, A also outputs m_0, m_1, σ. When A receives the input c, σ (c is the challenge ciphertext), A lets $r \leftarrow \{0,1\}^{|c|}$ and forwards $c||r, \sigma$ to A'. Then, A outputs whatever A' outputs.

Consider the encryption scheme $\Pi'^{RF} := (Gen'^{RF}, Enc'^{RF}, Dec'^{RF})$ that is the same as (Gen', Enc', Dec') except that the PRF g_{s_2} has been replaced by a truly random function. Since $\{g_s\}_{s\in\{0,1\}^*}$ is a family of PRFs, A' also breaks CCA2 security of $(Gen'^{RF}, Enc'^{RF}, Dec'^{RF})$. Now, we observe that A almost simulates the CCA2 attack of A' on $(Gen'^{RF}, Enc'^{RF}, Dec'^{RF})$, except that when A' asks for the decryption of $c_1||c_2 = Enc'^{RF}(m)$ for some message m but have not asked for the encryption of m previously, A would answer $\perp$, which is incor-

rect. However, the decryption query $c_1||c_2$ satisfies $c_1||c_2 = Enc'^{RF}(m)$ for some message m only if $c_2 = g(c_1)$, where g is some random function. For such $c_1||c_2$ and m, if A' have not asked for the encryption of m previously, then the probability that A' would be able to guess $c_2 = g(c_1)$ is $2^{-|c_1|}$, which is negligible.

Thus, we have $\{IND_0^{CPA}(\Pi, A, n)\}_{n\in\mathbb{N}} \approx \{IND_0^{CCA2}(\Pi'^{RF}, A', n)\}_{n\in\mathbb{N}}$
$\not\approx \{IND_1^{CCA2}(\Pi'^{RF}, A', n)\}_{n\in\mathbb{N}} \approx \{IND_1^{CPA}(\Pi, A, n)\}_{n\in\mathbb{N}}$, contradicting the fact that $\Pi = (Gen, Enc, Dec)$ is CPA secure.

■

3 Public Key Encryption

Can parties communicate without sharing a secret?

Incorrect argument showing that this is not possible:

- To decrypt a message, you need a key (otherwise, anyone can decrypt).
- To encrypt a message, you also need the key; otherwise, the ciphertext is independent of the key and again, anyone can decrypt.

The problem with this argument is that it is assumed that the key for encryption needs to be the same as the key for decryption; however, the key for encrypting a message may be only part of whole key used in the encryption scheme (e.g., the key for encryption can be the public key in a (public key, secret key) pair, and the key for decryption can be the secret key in the (public key, secret key) pair).

Definition 1 (Public Key Encryption Scheme) (Gen, Enc, Dec) *is a* public-key encryption scheme *if the following hold:*

1. *Gen is a PPT algorithm:* $pk, sk \leftarrow Gen(1^n)$
2. *Enc is a PPT algorithm:* $c \leftarrow Enc_{pk}(m)$
3. *Dec is a PPT algorithm:* $m \leftarrow Dec_{sk}(c)$
4. $\forall m \in \{0,1\}^*, \Pr[pk, sk \leftarrow Gen(1^{|m|}) : Dec_{sk}(Enc_{pk}(m)) = m] = 1.$

Definition 2 (Secure Public Key Encryption Scheme) *A public-key encryption scheme* (Gen, Enc, Dec) *is said to be* (single-message) secure *if* $\forall$ *non-uniform PPT machine* D, $\exists$ *negligible function* ϵ *s.t.* $\forall n \in \mathbb{N}$, *and* $\forall m_0, m_1 \in \{0,1\}^n$, D *distinguishes the following distributions w.p.* $\leq \epsilon(n)$*:*

$$\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_0))\}$$
$$\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_1))\}$$

The definitions for CPA/CCA1/CCA2 security can be extended to public-key encryption systems in a natural way.

Perfect secrecy: We note that perfect secrecy is not possible, since an unbounded adversary can simply encrypt each message in $\{0,1\}^n$ and compare the encrypted message with the challenge ciphertext in order to determine the original plaintext message.

Deterministic encryption: We note that an encryption scheme with a deterministic encryption algorithm (even with state) would not be secure because an adversary can simply encrypt the message m_0 (with the public key pk) and compare the encryption of m_0 with the challenge ciphertext (which is the encryption of either m_0 or m_1).

Theorem 2 *If a public key encryption scheme is single-message secure, then it is also multi-message secure.*

Proof. Let (Gen, Enc, Dec) be a single-message secure public key encryption scheme. Now, suppose that (Gen, Enc, Dec) is not multi-message secure. Then, there exists a non-uniform PPT machine D and positive polynomials p and q s.t. for infinitely many $n \in \mathbb{N}$, there exist $m_1, \ldots, m_{q(n)} \in \{0,1\}^n$ and $m'_1, \ldots, m'_{q(n)} \in \{0,1\}^n$ s.t. D distinguishes the following distributions w.p. $\frac{1}{p(n)}$:

$$\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_1), \ldots, Enc_{pk}(m_{q(n)}))\}$$
$$\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m'_1), \ldots, Enc_{pk}(m'_{q(n)}))\}$$

Now, let

$$H^i_n = \{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_1), \ldots, Enc_{pk}(m_i), Enc_{pk}(m'_{i+1}), \ldots, Enc_{pk}(m'_{q(n)}))\}.$$

We note that $H^{q(n)}_n$ and H^0_n are equal to the pair of distributions for which D distinguishes w.p. $\frac{1}{p(n)}$. Thus, by the Hybrid Lemma, for infinitely many $n \in \mathbb{N}$, there exists an i s.t. D distinguishes H^i_n, H^{i+1}_n w.p. $\frac{1}{p(n)q(n)}$. Now, let M_n be the non-uniform PPT machine that on input (pk, c), outputs $(pk, Enc_{pk}(m_1), \ldots, Enc_{pk}(m_i), c, Enc_{pk}(m_{i+2}), \ldots, Enc_{pk}(m_{q(n)}))$. We note that $M_n(\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m'_{i+1}))\}) = H^i_n$ and $M_n(\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_{i+1}))\}) = H^{i+1}_n$.

Since (Gen, Enc, Dec) is single-message secure, $\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m'_{i+1}))\}_{n\in\mathbb{N}}$ is indistinguishable from $\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_{i+1}))\}_{n\in\mathbb{N}}$. Thus, by the Closure Under Efficient Operations Lemma, $\{H^i_n\}_{n\in\mathbb{N}}$ is indistinguishable from $\{H^{i+1}_n\}_{n\in\mathbb{N}}$, which contradicts the fact that for inifinitely many $n \in \mathbb{N}$, D distinguishes H^i_n, H^{i+1}_n w.p. $\frac{1}{p(n)q(n)}$.

■