

Advanced Cryptography

1st Semester 2008-2009

Public Encryption

Pascal Lafourcade

Université Joseph Fourier, Verimag

Master: October 10th 2008

Last Time (I)

Indistinguishability

- Negligible function
- Probabilities
- Indistinguishability definition
- Hybrid argument

Remarks, questions, comments ?

Last Time (II)

Exercises done

- 1) Negligible functions
- 2) Probabilities
- 3 – 5) Indistinguishability

Outline of Today: **Security Notions**

1 Cyclic Groups

Outline of Today: **Security Notions**

- 1 Cyclic Groups
- 2 Hard Problems

Outline of Today: **Security Notions**

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions

Outline of Today: **Security Notions**

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions

Outline of Today: **Security Notions**

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal

Outline of Today: **Security Notions**

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$

Outline of Today: **Security Notions**

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Outline

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Definitions (I)

A **group** $(G, *)$ is composed of a set G and a binary operator $*$ on G which satisfy the three following axioms:

$$\forall a, b, c \in G, a * (b * c) = (a * b) * c \quad \text{Associativity}$$

$$\exists e \in G, \forall a \in G, e * a = a * e = a \quad \text{Neutral Element}$$

$$\forall a \in G, \exists b \in G, a * b = b * a = e \quad \text{Inverse Element}$$

b is called the inverse of a and is denoted by a^{-1} .

Example

$(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, permutation group, $(\mathcal{M}_{(n,n)}, +)$.

Counter-Example

$(\mathbb{N}, +)$, $(\mathcal{M}_{(n,n)}, *)$

Definitions (II)

Cyclic Group

A group G is **cyclic** if G is finite and there exists an element g of G such that:

$$\forall a \in G, \exists n \in \mathbb{N}, a = g^n$$

Element g is called a *generator* of group G .

Example

If p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group.

Outline

- 1 Cyclic Groups
- 2 Hard Problems**
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Integer Factoring and RSA

→ Use of algorithmically hard problems.

Factorization

- $p, q \mapsto n = p \cdot q$ easy (quadratic)
- $n = p \cdot q \mapsto p, q$ difficult

RSA function $n = pq$, p and q primes.

e : public exponent

- $x \mapsto x^e \pmod n$ easy (cubic)
- $y = x^e \pmod n \mapsto x \pmod n$ difficult
 $x = y^d$ where $d = e^{-1} \pmod{\phi(n)}$

Complexity Estimates

Estimates for integer factoring Lenstra-Verheul 2000

Modulus (bits)	Operations (\log_2)
512	58
1024	80
2048	111
4096	149
8192	156

$\approx 2^{60}$ years

→ Can be used for RSA too.

The Diffie-Hellman Key Exchange Protocol

Let g be a generator of a cyclic group of prime order q .

$$A \rightarrow B : g^a$$

$$B \rightarrow A : g^b$$

$$A \rightarrow B : \{N\}_{g^{ab}}$$

Hard Problems

Most cryptographic constructions are based on *hard problems*.

Their security is proved by reduction to these problems:

- **Discrete Logarithm** problem, DL. Given a group $\langle g \rangle$ and g^x , compute x .
- **Computational Diffie-Hellman**, CDH Given a group $\langle g \rangle$, g^x and g^y , compute g^{xy} .
- **Decisional Diffie-Hellman**, DDH Given a group $\langle g \rangle$, distinguish between the distributions (g^x, g^y, g^{xy}) and (g^x, g^y, g^r) .
- **RSA**. Given $N = pq$ and $e \in \mathbb{Z}_{\varphi(N)}^*$, compute the inverse of e modulo $\varphi(N) = (p - 1)(q - 1)$. **Factorization**

Relation between the problems

Prop

$DL \Rightarrow CDH \Rightarrow DDH.$

Prop (Moaurer & Wolf)

For many groups, $DL \Leftrightarrow CDH$

Prop (Joux & Wolf)

There are groups for which DDH is easier than CDH .

Usage of DH assumption

The Diffie-Hellman problems are widely used in cryptography:

- Public key cryptosystems [ElGamal, Cramer& Shoup]
- Pseudo-random functions [Noar& Reingold, Canetti]
- Pseudo-random generators [Blum& Micali]
- (Group) key exchange protocols [many]

Example: ElGamal Encryption Scheme

Key generation: Alice chooses a prime number p and a group generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ and $a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$.

Public key: (p, g, h) , where $h = g^a \pmod p$.

Private key: a

Encryption: Bob chooses $r \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and computes $(u, v) = (g^r, Mh^r)$

Decryption: Given (u, v) , Alice computes $M \equiv_p v \div u^a$

Justification: $v \div u^a = Mh^r \div g^{ra} \equiv_p M$

Remarque: re-usage of the same random r leads to a security flaw:

$$M_1 h^r \div M_2 h^r \equiv_p M_1 \div M_2$$

Practical Inconvenience: Cipher is twice as long as plain text.

Outline

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions**
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Adversary Model

Qualities of the adversary:

- **Clever**: Can perform all operations he wants
- **Limited time**:
 - Do not consider attack in 2^{60} .
 - Otherwise a Brute force by enumeration is always possible.

Model used: **Any Turing Machine**.

- Represents all possible algorithms.
- Probabilistic: adversary can generate keys, random number...

One-Wayness (OW)

Without the private key, it is computationally **impossible to recover the plain-text**. (Near of Perfect Security of Shannon)

Not enough

- Does not exclude to recover half of the plain-text
- Even worse if one has already partial information of the message:
 - Subject: XXXX
 - From: XXXX

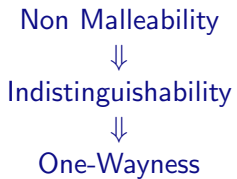
Indistinguishability (IND)

The adversary is not able to **guess in polynomial-time even a bit of the plain-text knowing the cipher-text**, notion introduced by S. Goldwasser and S.Micali ([GM84]).

Non Malleability (NM)

The adversary should **not be able to produce a new cipher-text** such that the plain-texts are meaningfully related, notion introduced by D. Dolev, C. Dwork and M. Naor in 1991 ([DDN91,BDPR98,BS99]).

Relations



Adversary Models

The adversary is given access to oracles :

→ encryption of all messages of his choice

→ decryption of all messages of his choice

Three classical security levels:

- Chosen-Plain-text Attacks (CPA)
- Non adaptive Chosen-Cipher-text Attacks (CCA1)
only before the challenge
- Adaptive Chosen-Cipher-text Attacks (CCA2)
unlimited access to the oracle (except for the challenge)

Chosen-Plain-text Attacks (CPA)

Adversary can obtain all cipher-texts from any plain-texts.

It is always the case with a Public Encryption scheme.

Non adaptive Chosen-Cipher-text Attacks (CCA1)

Adversary knows the public key, has access to a **decryption oracle multiple times before to get the challenge** (cipher-text), also called “Lunchtime Attack” introduced by M. Naor and M. Yung ([NY90]).

Adaptive Chosen-Cipher-text Attacks (CCA2)

Adversary knows the public key, has access to a **decryption oracle multiple times before and AFTER to get the challenge**, but of course cannot decrypt the challenge (cipher-text) introduced by C. Rackoff and D. Simon ([RS92]).

Parallels Attacks (PA0, PA1)

Introduced by M. Bellare and A. Sahai ([BS99]) to prove the link between NM and IND.

PA0 = Chosen Cipher-text Parallel Attack, **after** getting the challenge the adversary can ask for **decrypting a finite number of cipher-text all AT THE SAME TIME** which can be dependent of the challenge, but not of responses to decryption oracle.

PA1 = CCA1 followed by PA0.

Outline

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions**
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Asymmetric Encryption

An asymmetric encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined by

- \mathcal{K} : **key generation**
- \mathcal{E} : **encryption**
- \mathcal{D} : **decryption**

$$\mathcal{K}(\eta) = (k_e, k_d)$$

$$\mathcal{E}_{k_e}(m, r) = c$$

$$\mathcal{D}(c, k_d) = m$$

One-Wayness (OW)

Adversary \mathcal{A} : any polynomial time Turing Machine (PPTM)

Basic security notion: One-Wayness (OW)

Without the private key, it is computationally impossible to recover the plain text:

$$\Pr_{m,r}[\mathcal{A}(c) = m \mid c = E(m, r)]$$

is negligible.

Indistinguishability (IND)

Game Adversary: $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$

- 1 The adversary \mathcal{A}_1 is given the public key pk .
- 2 The adversary \mathcal{A}_1 chooses two messages m_0, m_1 .
- 3 $b = 0, 1$ is chosen at random and $c = E(m_b)$ is given to the adversary.
- 4 The adversary \mathcal{A}_2 answers b' .

The probability $Pr[b = b'] - \frac{1}{2}$ should be negligible.

The IND-CPA Games

Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{CPA}^b(\mathcal{A})$ be the following algorithm:

- Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1(\eta, pk)$
- $b' \xleftarrow{R} \mathcal{A}_2(\eta, pk, s, \mathcal{E}(pk, m_b))$
- return b' .

Then, we define the advantage against the IND-CPA game by:

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{CPA}}(\eta) = \Pr[b' \xleftarrow{R} \text{IND}_{CPA}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{CPA}^0(\mathcal{A}) : b' = 1]$$

The IND-CCA1 Games

Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{\text{CCA1}}^b(\mathcal{A})$ be the following algorithm:

- Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$ **where** $\mathcal{O}_1 = \mathcal{D}$
- $b' \xleftarrow{R} \mathcal{A}_2(\eta, pk, s, \mathcal{E}(pk, m_b))$
- return b' .

Then, we define the advantage against the IND-CCA1 game by:

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{CCA1}}}(\eta) = \\ \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA1}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA1}}^0(\mathcal{A}) : b' = 1]$$

The IND-CCA2 Games

Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{\text{CCA2}}^b(\mathcal{A})$ be the following algorithm:

- Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$ where $\mathcal{O}_1 = \mathcal{D}$
- $b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, \mathcal{E}(pk, m_b))$ **where** $\mathcal{O}_2 = \mathcal{D}$
- return b' .

Then, we define the advantage against the IND-CCA2 game by:

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{CCA2}}^b}(\eta) = \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA2}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA2}}^0(\mathcal{A}) : b' = 1]$$

IND-XXX Security

Definition

An encryption scheme is *IND-XXX secure*, if for any adversary \mathcal{A} the function $\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND-XXX}}$ is negligible.

Exercise

Prove that

$$\begin{aligned} \text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}^{\text{XXX}}}(\eta) &= \Pr[b' \stackrel{R}{\leftarrow} \text{IND}^1(\mathcal{A}) : b' = 1] \\ &\quad - \Pr[b' \stackrel{R}{\leftarrow} \text{IND}^0(\mathcal{A}) : b' = 1] \\ &= 2\Pr[b' \stackrel{R}{\leftarrow} \text{IND}^b(\mathcal{A}) : b' = b] - 1 \end{aligned}$$

Summary of IND-XXX Games

Given $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms. $\text{IND}_{\text{XXX}}^b(\mathcal{A})$ follows:

- Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$
- $b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, \mathcal{E}(pk, m_b))$
- return b' .

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{XXX}}}(\eta) =$$

$$\Pr[b' \xleftarrow{R} \text{IND}_{\text{XXX}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{XXX}}^0(\mathcal{A}) : b' = 1]$$

IND-CPA, IND-CCA1, IND-CCA2

IND-CPA: $\mathcal{O}_1 = \mathcal{O}_2 = \emptyset$ Chosen Plain text Attack

IND-CCA1: $\mathcal{O}_1 = \{\mathcal{D}\}$, $\mathcal{O}_2 = \emptyset$ Non-adaptive Chosen Cipher text Attack

IND-CCA2: $\mathcal{O}_1 = \mathcal{O}_2 = \{\mathcal{D}\}$ Adaptive Chosen Cipher text Attack.

Non Malleability

Game Adversary: $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$

- 1 The adversary \mathcal{A}_1 is given the public key pk .
- 2 The adversary \mathcal{A}_1 chooses a message space M .
- 3 Two messages m and m^* are chosen at random in M and $c = E(m; r)$ is given to the adversary.
- 4 The adversary \mathcal{A}_2 outputs a binary relation R and a cipher-text c' .

Probability $Pr[R(m, m')] - Pr[R(m, m^*)]$ is negligible, where $m' = \mathcal{D}(c')$

The NM-XXX Games

Given $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $m, m', m^* \in M$. Let $NM_{XXX}^b(\mathcal{A})$:

- Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- $(s, M) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk), m_0, m_1, \leftarrow M$
- $(R, C') \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, M, \mathcal{E}(pk, m_b)), M' \leftarrow \mathcal{D}(C')$
- return $R(m_b, M')$

Then, we define the advantage against the IND-CCA2 game by:

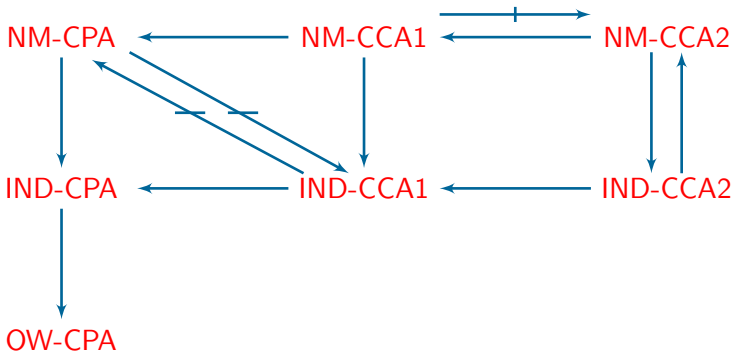
$$\begin{aligned} \text{ADV}_{\mathcal{S}, \mathcal{A}}^{NM_{XXX}}(\eta) &= \Pr[R(m, M') \xleftarrow{R} NM_{XXX}^1(\mathcal{A}) : R(m, M') = 1] \\ &\quad - \Pr[R(m, M^*) \xleftarrow{R} NM_{XXX}^0(\mathcal{A}) : R(m, M^*) = 1] \end{aligned}$$

NM-CPA: $\mathcal{O}_1 = \mathcal{O}_2 = \emptyset$ Chosen Plain text Attack

NM-CCA1: $\mathcal{O}_1 = \{\mathcal{D}\}, \mathcal{O}_2 = \emptyset$ Non-adaptive Chosen Cipher text Attack

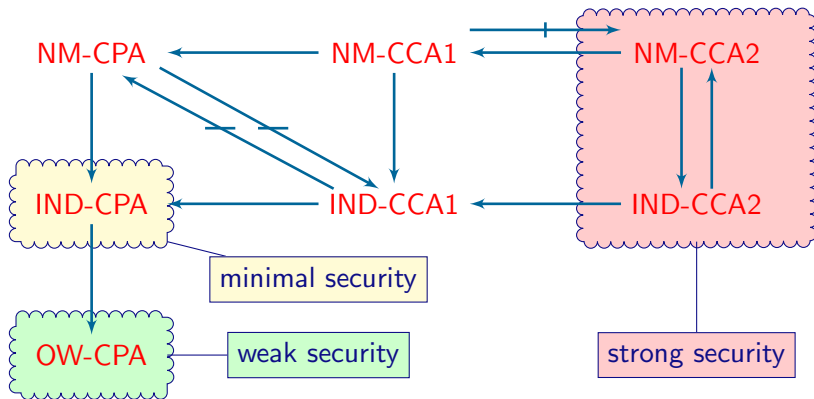
NM-CCA2: $\mathcal{O}_1 = \mathcal{O}_2 = \{\mathcal{D}\}$ Adaptive Chosen Cipher text Attack.

Relations



"Relations Among Notions of Security for Public-Key Encryption Schemes", **Crypto'98**, by Mihir Bellare, Anand Desai, David Pointcheval and Phillip Rogaway [BDPR'98]

Relations



"Relations Among Notions of Security for Public-Key Encryption Schemes", **Crypto'98**, by Mihir Bellare, Anand Desai, David Pointcheval and Phillip Rogaway [BDPR'98]

Outline

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples**
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Example: RSA

public	private
$n = pq$	$d = e^{-1} \bmod \phi(n)$
e (public key)	(private key)

RSA Encryption

- $E(m) = m^e \bmod n$
- $D(c) = c^d \bmod n$

OW-CPA = RSA problem by definition!

IND-XXX and the Determinism

Prop

The encryption algorithm of an IND-XXX scheme must probabilistic, if it is stateless.

Proof.

An exercise. □

The Discret Logarithm (DL)

Let $G = (\langle g \rangle, *)$ be any finite cyclic group of prime order.

Idea: it is hard for any adversary to produce x if he only knows g^x .

For any adversary \mathcal{A} ,

$$\mathbf{Adv}^{DL}(\mathcal{A}) = Pr \left[\mathcal{A}(g^x) \rightarrow x \mid x, y \stackrel{R}{\leftarrow} [1, q] \right]$$

is negligible.

Computational Diffie-Hellman (CDH)

Idea: it is hard for any adversary to produce g^{xy} if he only knows g^x and g^y .

For any adversary \mathcal{A} ,

$$\mathbf{Adv}^{CDH}(\mathcal{A}) = Pr\left[\mathcal{A}(g^x, g^y) \rightarrow g^{xy} \mid x, y \stackrel{R}{\leftarrow} [1, q]\right]$$

is negligible.

Decisional Diffie-Hellman (DDH)

Idea: Knowing g^x and g^y , it should be hard for any adversary to distinguish between g^{xy} and g^r for some random value r .

For any adversary \mathcal{A} , the advantage of \mathcal{A}

$$\begin{aligned} \mathbf{Adv}^{DDH}(\mathcal{A}) = & Pr\left[\mathcal{A}(g^x, g^y, g^{xy}) \rightarrow 1 \mid x, y \stackrel{R}{\leftarrow} [1, q]\right] \\ & - Pr\left[\mathcal{A}(g^x, g^y, g^r) \rightarrow 1 \mid x, y, r \stackrel{R}{\leftarrow} [1, q]\right] \end{aligned}$$

is negligible.

This means that an adversary cannot extract a single bit of information on g^{xy} from g^x and g^y .

Examples

Diffie-Hellman

$$DDH \leq CDH \leq DL$$

Exercise

$$DDH \leq CDH \leq DL$$

Recall Elgamal

- $G = (\langle g \rangle, *)$ finite cyclic group of prime order q .
- x : **private** key.
- $y = g^x$: **public** key.

$$\mathcal{E}(m; r) = (g^r, y^r m) \rightarrow (c, d) \text{ and } \mathcal{D}(c, d) = \frac{d}{c^x}$$

OW = CDH Assumption
IND-CPA = DDH Assumption

OW-CPA for Elgamal

Exercise

Prove that under CDH assumption El-Gamal is OW-CPA.

IND-CPA for Elgamal

Exercise

Prove that under DDH assumption El-Gamal is IND-CPA.

Outline

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Intuition for IND-CCA2 \Rightarrow NM-CCA2

Non-malleability deals with the ability to output ciphertexts.

As the adversary is granted access to the decryption oracle during its whole attack, it can decrypt any ciphertext it outputs.

The ability to output ciphertexts is thus not likely to increase the power of the adversary.

Main Idea

- We assume the scheme \mathcal{PE} is secure in the IND-CCA2 sense.
- We let $B = (B_1, B_2)$ be an NM-CCA2 adversary attacking \mathcal{PE} . We must show that $\mathbf{Adv}_{\mathcal{PE}, B}^{NM-CCA2}(k)$ is negligible.
- We construct an IND-CCA2 adversary A attacking the scheme, using B .
- Comparing these two adversaries, we show the advantages are such that :

$$\mathbf{Adv}_{\mathcal{PE}, B}^{NM-CCA2}(k) = 2 \cdot \mathbf{Adv}_{\mathcal{PE}, A}^{IND-CCA2}(k)$$

Algorithm of Attack

Algorithm $A_1^{\mathcal{D}_{sk}}(pk)$

$(s, M) \xleftarrow{R} B_1^{\mathcal{D}_{sk}}(pk);$

$(m_0, m_1) \xleftarrow{R} M;$

$s' \leftarrow (m_0, m_1, M, s);$

Return (m_0, m_1, s') .

Algorithm $A_2^{\mathcal{D}_{sk}}(s', y)$

$(\mathcal{R}, \vec{C}') \xleftarrow{R} B_2^{\mathcal{D}_{sk}}(M, s, y);$

$\vec{M}' \leftarrow \mathcal{D}_{sk}(\vec{C}');$

if $\mathcal{R}(m_0, \vec{M}')$ then $d \leftarrow 0$ else $d \xleftarrow{R} \{0, 1\}.$

Return d .

Notation

$$\mathbf{Adv}_{\mathcal{P}\mathcal{E},A}^{\text{IND-CCA2}}(k) = pk(0) - pk(1)$$

$$pk(b) = Pr[(pk, sk) \leftarrow \mathcal{K}(\eta); (s', m_0, m_1) \leftarrow \mathcal{A}_1^{\mathcal{D}_{sk}}(pk) : \mathcal{A}_2^{\mathcal{D}_{sk}}(s', \mathcal{E}(pk, m_b)) = 0]$$

$$\mathbf{Adv}_{\mathcal{P}\mathcal{E},B}^{\text{NM-CCA2}}(k) = pk'(0) - pk'(1)$$

$$pk'_k(b) = Pr[(pk, sk) \leftarrow \mathcal{K}(\eta); (s, M) \stackrel{R}{\leftarrow} B_1^{\mathcal{D}_{sk}}(pk); (m_0, m_1) \stackrel{R}{\leftarrow} M;$$

$$(\mathcal{R}, \vec{C}') \stackrel{R}{\leftarrow} B_2^{\mathcal{D}_{sk}}(M, s, \mathcal{E}(pk, m_b)) \vec{M}' \leftarrow \mathcal{D}_{sk}(\vec{C}'); \mathcal{R}(m_b, \vec{M}')]]$$

End of the Proof

$$\begin{aligned}
 p_k(0) &= p'_k(0) \cdot \Pr[d = 0 | R(m_0, \vec{M})] + (1 - p'_k(0)) \cdot \Pr[d = 0 | \text{coinflip}] \\
 &= p'_k(0) + \frac{1}{2} - \frac{1}{2} \cdot p'_k(0) \\
 &= \frac{1}{2} \cdot (1 + p'_k(0)) \\
 p_k(1) &= \frac{1}{2} \cdot (1 + p'_k(1))
 \end{aligned}$$

$$\begin{aligned}
 \mathbf{Adv}_{\mathcal{PE}, A}^{\text{IND-CCA2}}(k) &= p_k(0) - p_k(1) \\
 &= \frac{1}{2} \cdot (1 + p'_k(0)) - \frac{1}{2} \cdot (1 + p'_k(1)) \\
 &= \frac{1}{2} \cdot (p'_k(0) - p'_k(1)) \\
 &= \frac{1}{2} \cdot \mathbf{Adv}_{\mathcal{PE}, B}^{\text{NM-CCA2}}(k)
 \end{aligned}$$

IND-CCA1 $\not\Rightarrow$ NM-CPAIdea: IND-CCA1 $\not\Rightarrow$ NM-CPA

Assume there exists some IND-CCA1 secure encryption $P\mathcal{E}$.

We modify $P\mathcal{E}$ to build $P\mathcal{E}'$ which is also IND-CCA1 secure but not NM-CPA secure.

Algorithm \mathcal{PE}' :Algorithm $\mathcal{E}'_{pk}(x)$ $y_1 \xleftarrow{R} \mathcal{E}_{pk}(x); y_2 \xleftarrow{R} \mathcal{E}_{pk}(\bar{x});$
Return $y_1 || y_2$

Where $y_1 || y_2$ is a pair, and \bar{x} us the bitwise complement of x .

Algorithm $\mathcal{D}'_{sk}(y_1 || y_2)$ Return $\mathcal{D}_{sk}(y_1)$.

\mathcal{PE}' is not NM-CPA: Idea

Given a cipher text $y_1 || y_2$ of a message x it is easy to create a cipher of \bar{x} : just output $y_2 || y_1$. Thus the scheme is malleable.

Formally: $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks \mathcal{PE}' in the sense of NM-CPA.

$(\emptyset, M) \stackrel{R}{\leftarrow} \mathcal{A}_1(pk)$, where M puts uniform distribution on $\{0, 1\}^k$
 $(R, y_2 || y_1) \stackrel{R}{\leftarrow} \mathcal{A}_2(\emptyset, M, y_1 || y_2)$, where $R(m_1, m_2) = 1$ if $m_1 = \overline{m_2}$

$$\text{Adv}_{\mathcal{PE}', B}^{\text{NM-CPA}}(k) = 1 - 2^{-k}$$

\mathcal{PE}' is IND-CPA: Idea

Let $B = (B_1, B_2)$ be some polynomial time adversary attacking \mathcal{PE}' in the IND-CCA1 sense. Show that $\mathbf{Adv}_{\mathcal{PE}', B}^{\text{IND-CCA1}}(k)$ is negligible, using an hybrid argument.

$$p_k(i, j) = \Pr[(s, m_0, m_1) \stackrel{R}{\leftarrow} B_1^{\mathcal{D}_{sk}}; y_1 \stackrel{R}{\leftarrow} \mathcal{E}_{p_k}(x_i); y_2 \stackrel{R}{\leftarrow} \mathcal{E}_{p_k}(\bar{x}_j) : \\ B_2(s, m_0, m_1, y_1 || y_2) = 1]$$

$$\mathbf{Adv}_{\mathcal{PE}', B}^{\text{IND-CCA1}}(k) = p_k(1, 1) - p_k(0, 0)$$

$$\mathbf{Adv}_{\mathcal{PE}', B}^{\text{IND-CCA1}}(k) = p_k(1, 1) - p_k(1, 0) + p_k(1, 0) - p_k(0, 0)$$

Claim 1: $p_k(1, 1) - p_k(1, 0)$ is negligible

Algorithm $A_1^{\mathcal{D}_{sk}}(pk)$

$(s, m_0, m_1) \xleftarrow{R} B_1^{\mathcal{D}'_{sk}}(pk);$
Return $(\overline{m_0}, \overline{m_1}, s).$

Algorithm $A_2(s, m_0, m_1, y)$

$(\mathcal{R}, \vec{C}') \xleftarrow{R} B_2^{\mathcal{D}_{sk}}(M, s, y);$
 $d \xleftarrow{R} B_2(\overline{m_0}, \overline{m_1}, s, \mathcal{E}_{pk}(\overline{m_1}) || y);$
Return $d.$

$$\Pr[(m_0, m_1, s) \xleftarrow{R} \mathcal{A}_1^{\mathcal{D}_{sk}}(pk) : \mathcal{A}_2(m_0, m_1, s, \mathcal{E}_{pk}(m_1))] = p_k(1, 1)$$

$$\Pr[(m_0, m_1, s) \xleftarrow{R} \mathcal{A}_1^{\mathcal{D}_{sk}}(pk) : \mathcal{A}_2(m_0, m_1, s, \mathcal{E}_{pk}(m_0))] = p_k(1, 0)$$

$\text{Adv}_{\mathcal{PE}, A}^{\text{IND-CCA1}}(k) = p_k(1, 1) - p_k(0, 0)$ is negligible, assuming security of \mathcal{PE} in the IND-CCA1 sense.

Claim 2: $p_k(1, 0) - p_k(0, 0)$ is negligible

Algorithm $A_1^{\mathcal{D}^{sk}}(pk)$

$(x_0, x_1, s) \xleftarrow{R} B_1^{\mathcal{D}'^{sk}}(pk);$
Return (x_0, x_1, s) .

Algorithm $A_2(x_0, x_1, s, y)$

$(\mathcal{R}, \vec{C}') \xleftarrow{R} B_2^{\mathcal{D}^{sk}}(M, s, y);$
 $d \xleftarrow{R} B_2(x_0, x_1, s, y || \mathcal{E}_{pk}(\overline{x_0}));$
Return d .

$$\Pr[(x_0, x_1, s) \xleftarrow{R} A_1^{\mathcal{D}^{sk}}(pk) : \mathcal{A}_2(x_0, x_1, s, \mathcal{E}_{pk}(x_1))] = p_k(1, 0)$$

$$\Pr[(x_0, x_1, s) \xleftarrow{R} A_1^{\mathcal{D}^{sk}}(pk) : \mathcal{A}_2(x_0, x_1, s, \mathcal{E}_{pk}(x_0))] = p_k(0, 0)$$

$\text{Adv}_{\mathcal{P}\mathcal{E}, A}^{\text{IND-CCA1}}(k) = p_k(1, 0) - p_k(0, 0)$ is negligible, assuming security of $\mathcal{P}\mathcal{E}$ in the IND-CCA1 sense.

Outline

- 1 Cyclic Groups
- 2 Hard Problems
- 3 Ideas of Security Notions
- 4 Definitions of Security Notions
- 5 Examples
 - RSA
 - Diffie-Hellman
 - ElGamal
- 6 Proofs
 - $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
 - $\text{IND-CCA1} \not\Rightarrow \text{NM-CPA}$
- 7 Conclusion

Summary

Today

- Cyclic Groups
- Hard Problems
- One-way
- IND-CPA, IND-CCA1, IND-CCA2
- NM-CPA, NM-CCA1, NM-CCA2
- Examples
 - RSA
 - ElGamal
- IND-CCA2 \Rightarrow NM-CCA2
- NM-CCA1 $\not\Rightarrow$ NM-CPA

Thank you for your attention.

Questions ?