

# Models and analysis of security protocols

## 1st Semester 2009-2010

### Public Encryption

### Lecture 3

**Pascal Lafourcade**

*Université Joseph Fourier, Verimag*

Master: September 28th 2009

## Last Time (I)

### Indistinguishability

- ▶ Indistinguishability
- ▶ Perfect Encryption OTP
- ▶ Adversary: CPA, CCA1, CCA2
- ▶ Security Notions: OW, IND, NM
- ▶ DL, DDH, CDH

Remarks, questions, comments ?

## Last Time (II)

### Exercises

- ▶ Perfect Security
- ▶ Perfect Encryption OTP
- ▶ DL, DDH, CDH
- ▶ Elgamal OW and IND-CPA

## Precisions about $1^n$

$$\Pr[D(X_n, 1^n) = 1]$$

$1^n$  describes the size of the output of the algorithm  $D$  on the input  $X_n$ . It is used mainly for hash functions, in the book Foundations of Cryptography.

# Outline of Today:

Perfect Encryption

## Outline of Today:

Perfect Encryption

Cyclic Groups

## Outline of Today:

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

- DL implies CDH

- CDH implies DDH

- RSA

- ElGamal

- Elgamal OW

- Elgamal IND-CPA

## Outline of Today:

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

## Outline of Today:

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

## Outline of Today:

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

# Outline

## Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

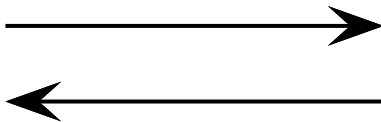
IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

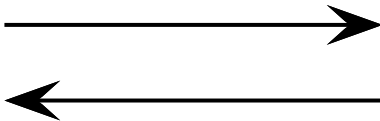
IND-CCA1  $\not\Rightarrow$  NM-CPA

Conclusion

## Description of Problem



## Description of Problem



Intruder



## Description of Problem



Intruder



## Description of Problem



Intruder



Message cannot be understood by anyone else

## Notations

If  $m$  is the message to be encrypted (also known as the “**plain-text**” or the “**clear-text**” then  $c = E_{k_e}(m, r)$  is the encrypted message or “**cipher-text**” with the key  $k_e$ . The decryption function is denoted by  $D_{k_d}(c)$

$k_e = k_d$  symmetric encryption

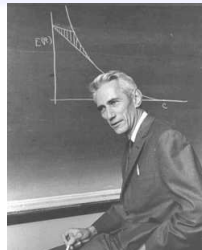
$k_e \neq k_d$  asymmetric encryption

A unique  $m$  satisfies the relation (with possibly several  $r$ )

→ At least an exhaustive search on  $m$  and  $r$  can lead to  $m$  !

⇒ unconditional secrecy is impossible, we need algorithmic assumptions

# Perfect Security (Shannon)



## Definition

Let  $m \in M$  be a random message and  $c \in C$  be the cipher-text of  $m$ , that is,  $c = E_k(m)$ . For any  $m' \in M$  and  $c' \in C$ , an encryption system is called **perfectly secure** if from the perspective of the attacker,

$$Pr(m = m' | c = c') = Pr(m = m')$$

This means that Eve's probability of guessing  $m$  remains unchanged after seeing any particular outcome  $c = c'$ .

## Exercise:

Messages are composed of  $\{0, 1\}$ , keys are  $\{A, B\}$  and we know  $P(0) = 1/4, P(1) = 3/4, P(A) = 1/4, P(B) = 3/4$ . The encryption is defined by:

$$E_A(0) = a, E_A(1) = b, E_B(0) = b, E_B(1) = a$$

Is this encryption perfectly secure?

## One Time Pad (OTP)

The One Time Pad encryption function is easily described; simply take the exclusive OR of the message string  $m$  and the key  $k$ .  
(Vernam encryption)

- ▶  $E_k(m) = m \oplus k$

- ▶  $D_k(c) = c \oplus k$

**Exercise:** Prove that OTP is perfectly secure.

# Entropy

## Definition

For a random variable  $X$  which takes a finite number of values  $x$  define

$$H(X) = - \sum_x \Pr[X = x] \log_2(\Pr[X = x])$$

$$H(X|Y) = H(X, Y) - H(Y)$$

## Joint entropy

For two random variables  $X, Y$  which takes a finite number of values  $x, y$  define

$$H(X, Y) = - \sum_{x,y} \Pr[X = x, Y = y] \log_2(\Pr[X = x, Y = y])$$

# Perfect Security Equivalence

$m$ : cleartext.

$c$ : ciphertext.

$k$ : key.

## Theorem

$$\text{Independence} + H(m|c) = H(m) \Leftrightarrow \Pr(m = m' | c = c') = \Pr(m = m')$$

Proof exercise

## OTP optimality

In OTP, the key is as long as the cleartext. You can't do better for a perfectly secure cipher:

theorem

For every perfectly secure cipher, we have

$$H(K) \geq H(X)$$

# Outline

Perfect Encryption

**Cyclic Groups**

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

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

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

## Reduction Proof Technique

Prove that an encryption scheme  $E$  is secure ?

1. Hypothesis: Consider an HARD problem  $P$  (RSA, DL, DDH, CDH)
2. Reduction:
  - ▶ If an adversary  $A$  breaks the encryption scheme  $E$
  - ▶ Then  $A$  can be used it to solve  $P$  in polynomial time.
3. Security: There does not exist an adversary in polynomial time under the hypothesis.

Application: Elgamal is IND-CPA secure under DDH assumption.

Consider an adversary breaking IND-CPA game for Egamal then he can solve DDH

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

## Definitions (recall)

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

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

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

Proof of  $CDH \leq DL$ 

Denote by  $X = g^x$ ,  $Y = g^y$  using  $DL$  you get  $y$  and  $Z = g^{xy}$ , with  $Z = g^{xy} = (g^x)^y = X^y$  and  $x = \text{Log}_g X$ , we conclude.

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

# CDH implies DDH

Let  $\mathcal{A}$  be an adversary against the CDH assumption and  $\mathcal{B}$  against DDH

**Adversary**  $\mathcal{B}(X, Y, Z)$ :

```
if  $Z = \mathcal{A}(X, Y)$  then return 1  
else return 0
```

# CDH implies DDH

Let  $\mathcal{A}$  be an adversary against the CDH assumption and  $\mathcal{B}$  against DDH

**Adversary**  $\mathcal{B}(X, Y, Z)$ :

**if**  $Z = \mathcal{A}(X, Y)$  **then return** 1  
**else return** 0

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

The number of elements in  $G$  is supposed large hence  $1/q$  is negligible. As the DDH assumption holds, the advantage of  $\mathcal{B}$  is negligible. Hence the advantage of  $\mathcal{A}$  against CDH is also negligible and the CDH assumption holds.

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

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!

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

## 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

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

ElGamal OW

ElGamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

## Example: ElGamal Encryption Scheme

### Exercise

Prove that ElGamal is OW-CPA under CDH assumption a

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

## Example: ElGamal Encryption Scheme

### Exercise

Prove that ElGamal is IND-CPA under DDH Assumption.

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

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.

# PROOF TODO

## 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 :

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

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

# 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

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

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

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

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

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

## End of the Proof

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

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

# Outline

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

**IND-CCA1  $\not\Rightarrow$  NM-CPA**

Conclusion

Idea: 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.

# PROOF TODO

## 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-CCA1: 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  $d.$

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

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

$\text{Adv}_{\mathcal{P}\mathcal{E}, A}^{\text{IND-CCA1}}(k) = p_k(1, 1) - p_k(0, 0)$  is negligible, assuming security of  $\mathcal{P}\mathcal{E}$  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  $A_2(x_0, x_1, s, y)$

$(\mathcal{R}, \vec{C}') \xleftarrow{R} B_2^{\mathcal{D}^{sk}}(M, s, y);$   
 $d \xleftarrow{R} B_2(x_0, x_1, s, y || \mathcal{E}_{pk}(\vec{x}_0));$   
 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

Perfect Encryption

Cyclic Groups

Simple Examples of Reduction Proof Technique

DL implies CDH

CDH implies DDH

RSA

ElGamal

Elgamal OW

Elgamal IND-CPA

IND-CCA2  $\Rightarrow$  NM-CCA2

Attack of the Scheme

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

Conclusion

# Summary

## Today

- ▶ Reduction proofs for
  - ▶ ElGamal
  - ▶ DH
- ▶  $\text{IND-CCA2} \Rightarrow \text{NM-CCA2}$
- ▶  $\text{NM-CCA1} \not\Rightarrow \text{NM-CPA}$

**Thank you for your attention.**

**Questions ?**