

Security models

1st Semester 2007/2008

P.Lafourcade

ROUAULT Boris

GABIAM Amanda

ARNEDO Pedro

Lecture Note 3

Date: 28.09.2009

Contents

| | | |
|----------|--|-----------|
| 1 | Perfect Encryption | 3 |
| 1.1 | Notations | 3 |
| 1.2 | Perfect security(Shannon) | 3 |
| 1.2.1 | Definition 1 | 3 |
| 1.2.2 | Definition 2 | 3 |
| 1.2.3 | Example | 3 |
| 1.3 | One Time Pad (OTP) | 4 |
| 1.4 | Entropy | 4 |
| 1.4.1 | Theorem | 5 |
| 1.4.2 | Theorem: Impracticality of perfectly secure encryption | 5 |
| 2 | Cyclic groups | 5 |
| 3 | Examples of reduction proof | 6 |
| 3.1 | Reduction Proof Technique | 6 |
| 3.2 | Recall | 6 |
| 3.3 | DL implies CDH | 6 |
| 3.4 | CDH implies DDH | 7 |
| 3.5 | ElGamal | 7 |
| 3.6 | ElGamal is OW-CPA under CDH assumption | 8 |
| 3.7 | ElGamal is IND-CPA under DDH assumption | 8 |
| 4 | IND-CCA2 \Rightarrow NM-CCA2 | 9 |
| 5 | IND-CCA1 $\not\Rightarrow$ NM-CPA | 10 |
| 6 | Bibliography | 10 |

1 Perfect Encryption

1.1 Notations

- m is the message to be encrypted (**plain-text** or **clear-text**).
- c is the encrypted message (**cipher-text**) with the key k_e .
- E_{k_e} is the encryption function.
- D_{k_d} is the decryption function.
- Need of algorithmic assumptions because we will see that unconditional secrecy is practically impossible.

1.2 Perfect security(Shannon)

1.2.1 Definition 1

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

$$Pr(m = m' \mid c = c') = Pr(m = m')$$

That is to say that the knowledge of any particular outcome $c = c'$ don't give any information about the plaintext.

1.2.2 Definition 2

Another equivalent definition of perfect security is that all the messages are equally likely to be the plain-text corresponding to a given cipher-text, e.g

$$Pr(E_k(m_1) = c) = Pr(E_k(m_2) = c) \quad \forall m_1, m_2 \in M \text{ and } c \in C$$

1.2.3 Example

With the previous definition, we can prove that the encryption defined by :

$$\begin{aligned} m &\in \{0, 1\} \\ c &\in \{a, b\} \\ K &\in \{A, B\} \\ P(0) &= \frac{1}{4}, P(1) = \frac{3}{4}, P(A) = \frac{1}{4}, P(B) = \frac{3}{4} \\ E_A(0) &= a, E_A(1) = b, E_B(0) = b, E_B(1) = a \end{aligned}$$

is not perfectly secure. For that, we just need to find a counterexample. We have on one hand:

$$P(E_K(0) = a) = P(A) \times P(E_A(0) = a) + P(B) \times P(E_B(0) = a) = \frac{1}{4} \times 1 + \frac{3}{4} \times 0 = \frac{1}{4}$$

On the other hand:

$$P(E_K(1) = a) = P(A) \times P(E_A(1) = a) + P(B) \times P(E_B(1) = a) = \frac{1}{4} \times 0 + \frac{3}{4} \times 1 = \frac{3}{4}$$

The message 1 is more likely to be encrypted in a than the message 0, so this encryption is not perfectly secure.

1.3 One Time Pad (OTP)

- Encryption consist on taking exclusive OR of the message string m and the key k .
- Also called Vernam encryption.
- The key is as long as the clear-text.

$$\begin{aligned} E_k(m) &= m \oplus k \\ D_k(c) &= c \oplus k \end{aligned}$$

Remarks

- OTP is perfectly secure. In fact if $k \in \{0, 1\}^l$ where l is the length of the key, $\forall m \in M, Pr(E_k(m) = c) = Pr(m \oplus k = c) = Pr(k = m \oplus c) = \frac{1}{2^l}$

This means that each $m \in M$ is equally likely to be the plaintext corresponding to a given ciphertext, that is to say that OTP is perfectly secure (according to the Definition 2).

- Unbreakable if used properly, OTP was intensively used for diplomatic communications security in the 20th century.

1.4 Entropy

- Quantified the information contained in a message.
- If X, Y are random variables which takes a finite number of values x, y

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

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

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

1.4.1 Theorem

With the previous notations, we have:

$$\text{Independance} + H(m | c) = H(m) \equiv Pr(m = m' | c = c') = Pr(m = m')$$

1.4.2 Theorem: Impracticality of perfectly secure encryption

For a perfectly secure scheme, the key space is at least as big as the message space, i.e:

$$H(K) \geq H(M)$$

Proof

We will start by proving that $|K| \geq |M|$, then the definition of entropy will be used for concluding. Let us consider a perfectly secure scheme such that $c = E_K(m)$. Given c an adversary trying to break this scheme will compute all possible plaintext values m_i using all possible keys K_i such that $m_i = D_{K_i}(c)$. If we assume that $|K| < |M|$ then there will not be complete mappings from the key K to message space M . Therefore ,

$$Pr(E_{K_i}(m_i) = c) = 0 \text{ for some } m_i \in M \text{ and } \forall K_i$$

However for the remaining m_i such that $m_i = D_{K_i}(c)$, the probabilities are non-zero. It means that all the messages are not likely to the possible plaintext corresponding to a given ciphertext. It leads to a contradiction according to the Definition 2 of perfect secrecy.

Since a perfect encryption secure encryption requires key space to be at least as big as the message space, it would be impossible to use a perfectly secure encryption scheme in practice . This motivates us to consider a weaker practical adversary, the one whose computation is bounded.

2 Cyclic groups

- A group $(G, *)$ satisfies:
 - Associativity $\forall a, b, c \in G, a * (b * c) = (a * b) * c$
 - Neutral element $\exists e \in G, \forall a \in G, e * a = a * e = a$
 - Inverse element $\forall a \in G, \exists b \in G, a * b = b * a = e$
- G is **cyclic** if G is finite and there exists an element $g \in G$ (*generator*) such that:

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

- Example : if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is cyclic.

3 Examples of reduction proof

3.1 Reduction Proof Technique

For proving that a 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 to solve P in polynomial time
3. Security: There does not exist an adversary in polynomial time under the hypothesis.

3.2 Recall

- Advantage for Discrete Logarithm :

$$\mathbf{Adv}^{DL}(\mathcal{A}) = Pr[\mathcal{A}(g^x) \rightarrow x | x, y \xleftarrow{R} [1, q]]$$

- Advantage for Computational Diffie-Hellman :

$$\mathbf{Adv}^{CDH}(\mathcal{A}) = Pr[\mathcal{A}(g^x, g^y) \rightarrow g^{xy} | x, y \xleftarrow{R} [1, q]]$$

- Advantage for Decisional Diffie-Hellman :

$$\mathbf{Adv}^{DDH}(\mathcal{A}) = Pr[\mathcal{A}(g^x, g^y, g^{xy}) \rightarrow 1 | x, y \xleftarrow{R} [1, q]] - Pr[\mathcal{A}(g^x, g^y, g^r) \rightarrow 1 | x, y, r \xleftarrow{R} [1, q]]$$

3.3 DL implies CDH

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 $x = \text{Log}_g X$. So if you can break DL, you can also easily break CDH.

3.4 CDH implies DDH

Let A be an adversary against the CDH assumption and B against DDH, then :

Adversary $B(X,Y,Z)$:

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

With this algorithm for B , we get :

$$\begin{aligned}
 & \mathbf{Adv}^{DDH}(B) \\
 & = \\
 & Pr[B(g^x, g^y, g^{xy}) \rightarrow 1 | x, y \xleftarrow{R} [1, q]] - Pr[B(g^x, g^y, g^r) \rightarrow 1 | x, y, r \xleftarrow{R} [1, q]] \\
 & = \\
 & Pr[A(g^x, g^y) \rightarrow g^{xy} | x, y \xleftarrow{R} [1, q]] - Pr[A(g^x, g^y) \rightarrow g^r | x, y, r \xleftarrow{R} [1, q]] \\
 & = \\
 & \mathbf{Adv}^{CDH}(A) - 1/q
 \end{aligned}$$

If we consider that q is large enough (which is usually the case), then $1/q$ is negligible and we can conclude about the implication.

Example : RSA

- public :
 - $n = pq$ (p, q prime numbers)
 - e (public key)
- private : $d = e^{-1} \bmod \phi(n)$ (private key)

RSA encryption

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

RSA problem is OW-CPA by definition (hard to factorize n).

3.5 ElGamal

- Key Generation : Alice chooses a prime number p , a group generator g of $(\mathbb{Z}/p\mathbb{Z})^*$, and $a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$.
 - Public Key : $p, g, h = g^a \bmod p$
 - Private Key : a

- Encryption : Bob takes a pseudo-random generated number $r \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and computes $(u, v) = (g^r, M.h^r) \bmod p$ with M the initial message we want to transmit.
- Decryption : Given (u, v) , Alice computes $M = v \div u^a \bmod p$
We note that $v \div u^a = M.h^r \div g^{ra} = M \bmod p$

Remark : be careful not to use two times the same pseudo-random number r :

$$M_1.h^r \div M_2.h^r = M_1 \div M_2 \bmod p$$

Practical inconvenience : it is rather costly since we get a cypher which is twice as long as the plain text.

3.6 ElGamal is OW-CPA under CDH assumption

We suppose that a CPA attacker succeed to retrieve $M = v \div u^a$ from (p, g, h, u, v) , then we show that he can retrieve g^{xy} from (g^x, g^y) .

Let $x, y \stackrel{R}{\leftarrow} [1, p]$, we write $a = x, u = g \div g^y = g^{1-y}$ and $v = g^x$.

We know the attacker can compute $v \div u^a = g^x \div g^{(1-y)a} = g^x . g^{xy-x} = g^{xy}$

Thus the attacker is able to solve a CDH problem.

Hence we can conclude that if an attacker (CPA) is not able to solve a CDH problem then the One-Wayness of ElGamal is verified.

3.7 ElGamal is IND-CPA under DDH assumption

Let's assume that an attacker \mathcal{A} is able to resolve an IND-CPA issue on ElGamal.

It means that, given $(p, g, h, u, v_b, M_0, M_1)$ ($b \in \{0, 1\}$) and $v_b = M_b.h^r$, he can say if $b = 0$ or 1.

Let $x, y, r \stackrel{R}{\leftarrow} (\mathbb{Z}/(p-1)\mathbb{Z})^*$, we write $h = g^a = g^x$, $u = g^y$, $M_0 = 1$, and $M_1 = g^r \div g^{xy} = g^{r-xy}$, such that $v_0 = g^{xy}$, and $v_1 = g^r$.

\mathcal{A}_1 sends (u, v_b) to \mathcal{A}_2 .

In the case $b = 0$, then \mathcal{A}_2 knows the message is $M_0 = 1$ and $v_b = g^{xy}$, otherwise $b = 1$ and then \mathcal{A}_2 knows the message is $M_1 = g^{r-xy}$ and $v_b = g^r$.

So $Pr(\mathcal{A}_2(g^x, g^y, g^{xy}) = 1) - Pr(\mathcal{A}_2(g^x, g^y, g^r) = 1)$ is not negligible.

Thus \mathcal{A}_2 is able to solve a DDH problem.

Hence we can conclude that if an attacker (CPA) is not able to solve a DDH problem, then the Indistinguishability of ElGamal is verified.

4 IND-CCA2 \Rightarrow NM-CCA2

The advantage of adversary A who is IND-CCA2 and attacks \mathcal{PE} scheme is the substraction between the probability of being message 0 and the probability of being message 1, so if the result is less than 0 the message is the 1 and is it is greater than 0 is the message 0. Usualy both are $1/2$, so the substracion is 0.

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

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

We assume that encryption scheme \mathcal{PE} is secure in the IND-CCA2 sense. We will show it is also secure in the NM-CCA2 sense. Since the adversary has acces to de decryption oracle, he can decrypt the ciphertexs he would output.

For the proof let $B = (B_1, B_2)$ be and NM-CCA2 adversary attacking \mathcal{PE} . We must show that $\mathbf{Adv}_{\mathcal{PE},B}^{NM-CCA2}(k)$ is negligible.

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

$$pk'(b) = Pr[(pk, sk) \leftarrow \mathcal{K}(\eta); (s, M) \stackrel{R}{\leftarrow} B_1^{\mathcal{D}_{sk}}(pk); (m_0, m_1) \stackrel{R}{\leftarrow} M; \\ (\mathcal{R}, \vec{C}') \stackrel{R}{\leftarrow} B_2^{\mathcal{D}_{sk}}(M, s, \mathcal{E}(pk, m_b)) \vec{M}' \leftarrow \mathcal{D}_{sk}(\vec{C}'); \mathcal{R}(m_b, \vec{M}')]]$$

To get this we describe an IND-CCA2 adversary $A = (A_1, A_2)$ attacking \mathcal{PE} . (*show slide 38 for the attack of adversary A*)

In the slide 40, we can see that A_2 may return 0 either when x is R-related to x_0 or as a result of the coin flip. Continuing with the advantage then,

$$\mathbf{Adv}_{\mathcal{PE},A}^{IND-CCA2}(k) = pk(0) - pk(1) = 1/2(1 + pk'(0)) - 1/2(1 + pk'(1)) = 1/2(pk'(0) - pk'(1))$$

We can observe that the experiment of B_2 , in case it is x_0 is exactly that defining $\mathbf{Succ}_{\mathcal{PE},B}^{IND-CCA2}(k)$. So

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

But we know that $\mathbf{Adv}_{\mathcal{PE},A}^{IND-CCA2}(k)$ is negligible because \mathcal{PE} is secure in the sense of IND-CCA2. It follows that $\mathbf{Adv}_{\mathcal{PE},B}^{IND-CCA2}(k)$ is negligible, as desired.

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

If there exists an encryption scheme \mathcal{PE} which is secure in the sense of IND-CCA1, then there exists an encryption scheme \mathcal{PE}' which is secure in the sense of IND-CCA1 but which is not secure in the sense of NM-CPA.

Assume there is some IND-CCA1 secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. We now modify \mathcal{PE} to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also IND-CCA1 secure but not secure in the NM-CPA sense. This will prove the theorem.

The new encryption scheme $\mathcal{PE}' = (\mathcal{P}', \mathcal{E}', \mathcal{D}')$ is defined as follows. Here $\neg x$ is the bitwise complement of string x , namely the string obtained by flipping each bit of x .

Algo $\mathcal{K}'(1^k)$ $(pk, sk) \leftarrow \mathcal{K}'(1^k)$ return (pk, sk)

Algo $\mathcal{E}'_pk(x)$ $y_1 \leftarrow \mathcal{E}_pk(x); y_2 \leftarrow \mathcal{E}_pk(\neg x)$ return $y_1 || y_2$

Algo $\mathcal{D}'_sk(y_1 || y_2)$ return $\mathcal{D}'_sk(y_1)$

In other words, a ciphertext in the new scheme is a pair $y_1 || y_2$ consisting of the encryption of the message and its complement. In decrypting, the second component is ignored.

As it is proved here <http://cseweb.ucsd.edu/users/mihir/papers/relations.pdf> we establish that \mathcal{PE}' is not secure in the sense of NM-CPA while it is secure in the sense of IND-CCA1.

6 Bibliography

Advances in cryptology: proceedings
CS 6903 Modern Cryptography