Notes of Cryptography

Squirrel

March 23, 2025

Preface

Course

密碼學設計與分析 Cryptography Design and Analysis (11320IIS500900) in NTHU

5 L5

5.1 Basics

§ Scenario

Sender S 和 receiver R 彼此有有一把相同的 key k，且 S 想要發送訊息給 R。
在發送訊息前，S 會先使用 k 將明文 m 加密為密文 c（$c \leftarrow \mathrm{Enc}_k(m)$），之後 S 將 c 傳送給 R。
R 在收到 c 後，使用同一把 key k 將 c 解密（$m := \mathrm{Dec}_k(c)$）來得到 m。

關於這個 scenario 的正式的定義可以參見 Definition 5 Private key encryption。

§ 安全性定義

使用前面提到的 $PrivK^{eav}_{A,\Pi}$，參見 3.2 Perfect secrecy III。

5.2 EAV-security

EAV = eavesdropping

Definition 6 (EAV-secruity of private key encryption)
A private key encryption scheme Π is **EAV-secure** if for all PPT adversary A, there is a negligible function negl such that for all n,

$$\Pr[PrivK^{eav}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$$

(The probability is taken over randomness used by adversary and used in experiment.)

§ Equivalent Formulation of EAV-security

前一節 EAV-security 的定義等價於下面這句話：
「無論 PPT adversary A 看到由 m_0 或 m_1 加密過後的密文，其表現都相同。」
(Every PPT adversary behaves the same whether it sees ciphertext of m_0 or m_1.)

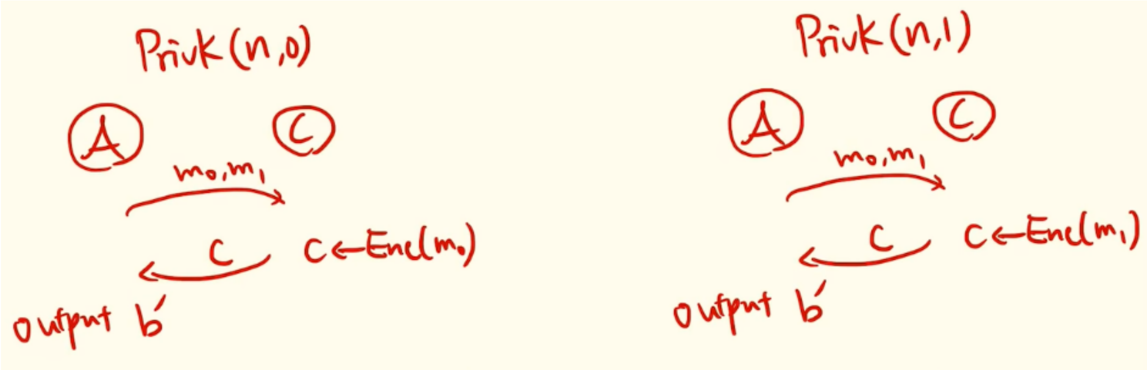
更精確的定義是：

- 修改之前的定義為 $PrivK^{eav}_{A,\Pi}(n, b)$，其定義都和之前一樣，除了 b 是固定的，而不是隨機選擇的。
- 定義 $out_A(PrivK^{eav}_{A,\Pi}(n, b)) = b'$，其中 b' 是 A 的 output。
- 沒有 PPT adversary A 可以知道現在是 experiment $PrivK^{eav}_{A,\Pi}(n, 0)$ 或 $PrivK^{eav}_{A,\Pi}(n, 1)$。

正式定義如下：

Definition 7 (Equivalent formulation of EAV-security)
Π is EAV-secure if for all PPT adversary A, there is a negligible function negl such that

$$|\Pr[out_A(PrivK^{eav}_{A,\Pi}(n, 0)) = 1] - \Pr[out_A(PrivK^{eav}_{A,\Pi}(n, 1)) = 1]| \leq \mathrm{negl}(n)$$



Quiz

In $PrivK$, we define A to choose two messages with the same length.
Please write your thought for the impossibility to support arbitrary-length messages.

5.3 Private Key Encryption

§ Pseudorandom Generator

Definition 8 (pseudorandom generator, PRG)
Let l be a polynomial and G is a deterministic polynomial-time algorithm. For any n and input $s \in \{0,1\}^n$, the output of $G(s)$ is $l(n)$-length.
We say G is a PRG if:

- Expansion: for every n, it holds $l(n) > n$. l is a so-called expansion factor of G.
- Pseudorandomness: for any PPT algorithm D (aka distinguisher), there is a negligible function negl such that
$$|\Pr[D(G(s))=1] - \Pr[D(r)=1]| \ \leq \ \mathrm{negl}(n)$$
where $s \in \{0,1\}^n$ and $r \in \{0,1\}^{l(n)}$ is a turly random variable.

§ PRG-based Construction of Fixed-length Private Key Encryption

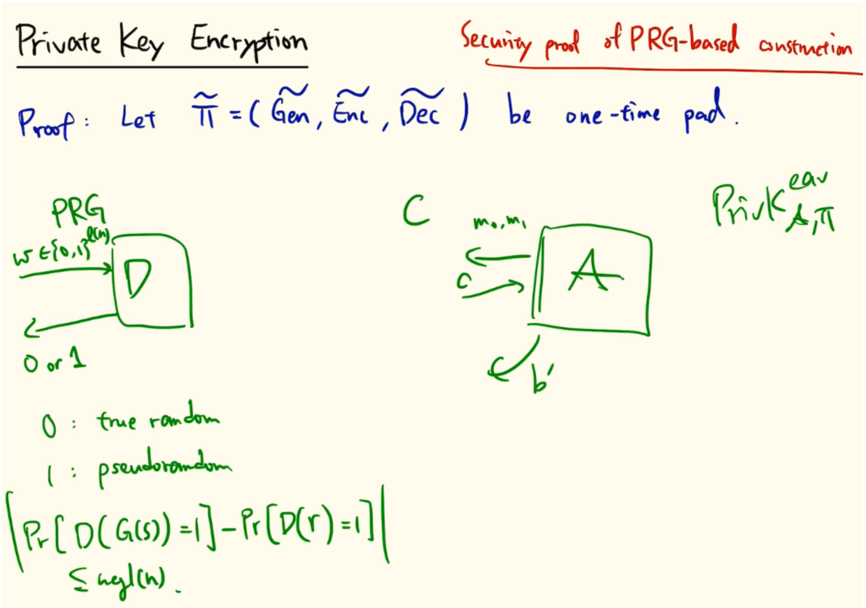
Let G be a PRG with expansion factor l.
Scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$.

- $\mathrm{Gen}(1^n)$: on input 1^n, choose uniform $k \in \{0,1\}^n$.
- $\mathrm{Enc}(k,m)$: with input of a message $m \in \{0,1\}^{l(n)}$ and outputs a ciphertext $c = G(k) \oplus m$
- $\mathrm{Dec}(k,c)$: with input of a ciphertext $c \in \{0,1\}^{l(n)}$ and outputs a message $m = G(k) \oplus c$

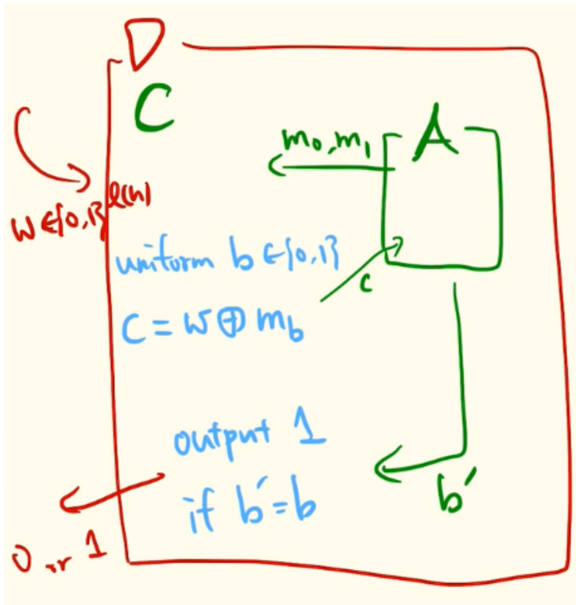
這種構造法和 OTP（見 3.3 One-Time Pad (OTP)）很像。那時候的 OTP 會遇到 perfect secrecy 的限制，也就是 key 的長度至少要和 message 一樣長（$|\mathcal{K}| \geq |\mathcal{M}|$）。在這裡，我們通過 PRG 來將原本的 key 長度 n 擴展成 $l(n)$，藉此來降低 key 的長度。而其代價就是，這種使用 PRG 的方法一定不是 perfect secrecy。

P.S. 由於 private key encryption 要求雙方要事先使用安全通道交換同一把 key。若在這種情景下使用和 message 一樣長的 key，那我們就可以直接使用這個安全通道交換訊息本身了，而無需進行加密。

§ PRG-based construction is EAV-secure



(a) Distinguisher D and adversary A



(b) Reduction in proof

Theorem 3
If G is a pseudorandom generator, then the construction Π is a EAV-secure.

其逆否命題為「如果 Π 不是 EAV-secure，則 G 也不是 PRG」。

證明思路
由 D 扮演 challenger。
在 reduction 時是 D 包在 A 的外面。

Let $\tilde{\Pi} = (\widetilde{\text{Gen}}, \widetilde{\text{Enc}}, \widetilde{\text{Dec}})$ be one-time pad.

1. If w is uniform chosen form $\{0,1\}^{l(n)}$,

$$\Pr[D(w) = 1] = \Pr[PrivK^{eav}_{A,\tilde{\Pi}}(n) = 1] = \frac{1}{2}$$

   這種情況是 one-time pad 的情況，也就是使用 true randomness。

2. If $w = G(k)$ by choosing uniform $k \in \{0,1\}^n$,

$$\Pr[D(G(k)) = 1] = \Pr[PrivK^{eav}_{A,\Pi}(n) = 1]$$

   這種情況是使用 pseudorandomness。
   這個機率是我們所要證明的，可以透過第三點來反推其機率為 $\leq \frac{1}{2} + \text{negl}(n)$

3. If G is PRG,

$$|\Pr[D(G(k)) = 1] - \Pr[D(w) = 1]| \;\leq\; \text{negl}(n)$$

Proof details
Let A be a PPT adversary. Our goal is to contract a distinguisher D (which is going to break PRG) that takes a string w as input.

Goal of D: determine whether
(i) w was chosen uniformly (where $w \in \{0,1\}^{l(n)}$)
(ii) w was generated by choosing uniform $k \in \{0,1\}^n$ and computing $w = G(k)$ (where $w \in \{0,1\}^{l(n)}$ and $l(n) > n$)

Output of D: outputs 1 if case (i) mentioned above; otherwise, outputs 0

Theorem used:

$$|\Pr[D(r) = 1] - \Pr[D(G(k)) = 1]| \ \leq \ \mathrm{negl}(n)$$

where $r \leftarrow \{0,1\}^{l(n)}$, and $k \leftarrow \{0,1\}^n$.

Activites of D: (connect A and D)
Emulate the eav experiment $PrivK^{eav}_{A,\Pi}$ for A

— If A wins, D thinks $w := G(k)$.

— If A fails, D thinks w is uniform chosen.

Proof

(Refer to figure Reduction in proof)
Distinguisher D get an input of a string $w \in \{0,1\}^{l(n)}$.

Step 1： Run A to obtain a pair of messages $m_0, m_1 \in \{0,1\}^{l(n)}$

Step 2： Choose a uniform bit $b \in 0, 1$. Set $c = w \oplus m_b$

Step 3： Send c to A

Step 4： Later, A returns b'

D outputs

— 1, if $b' = b$

— 0, if $b' \neq b$

Note that probability of output of D is related to $\Pr[PrivK^{eav}_{A,\Pi}]$.
If $\Pr[PrivK^{eav}_{A,\Pi}] > \frac{1}{2} + \mathrm{negl}$,

$$\Pr[out_D = 1] > \frac{1}{2} + \mathrm{negl}$$
$$\Pr[out_D = 0] \leq \frac{1}{2} - \mathrm{negl}$$

□

5.4 Chosen Plaintext attack & CPA-security

CPA = Chosen Plaintext Attack

§ CPA security

在這個情景下的 adversary A 可以存取 encryption oracle。

Encryption oracle：是一個黑盒子，我們不知道其運作原理，但給它輸入和取得它的輸出。A 可以將明文 m 給 oracle，之後 oracle 會將明文加密為密文 $c \leftarrow \mathrm{Enc}_k(m)$ 回傳給 A。

Experiment $PrivK^{cpa}_{A,\Pi}$

Step 1： A 可以選擇明文 m_i 給 C

Step 2： C 建立密鑰 $k \leftarrow \mathrm{Gen}(1^n)$，並將明文加密為密文 $c_i \leftarrow \mathrm{Enc} \ m_i)$ 回傳給 A。

Step 3： A 此時可以將這些收集到明文-密文對（plaintext-ciphertext pair）儲存起來。由於 A 是 PPT adversary，所以 A 可以收集的 pair 數為 poly-many。

Step 4： A 選擇 m_0 和 m_1 傳給 C 進行 chanllenge。之後的事情都和之前的 EAV-secure 的 experiment 一樣。

Step 5： 若 A 贏了，則 $PrivK^{cpa}_{A,\Pi}(1^n) = 1$。

P.S. 前三步稱為 encryption oracle query。而 challenge 之後一樣可以進行 eneryption oracle query，直到 A output b'。

Quiz

Show PRG-based construction Π is not CPA-secure.
(Hint: give A in $PrivK^{cpa}_{A,\Pi}$ to break Π)

6 L6

6.1