

# Cifratura CPA sicura da funzioni pseudocasuali

Paolo D'Arco  
pdarco@unisa.it

Università di Salerno

Elementi di Crittografia

1 Cifratura CPA sicura

2 Schema

3 Riduzione

# Cifratura CPA sicura da funzioni pseudocasuali

Costruiremo uno schema di cifratura per messaggi di lunghezza fissa

Ne possiamo ottenere facilmente uno per lunghezze arbitrarie applicando i risultati precedenti

Primo tentativo:

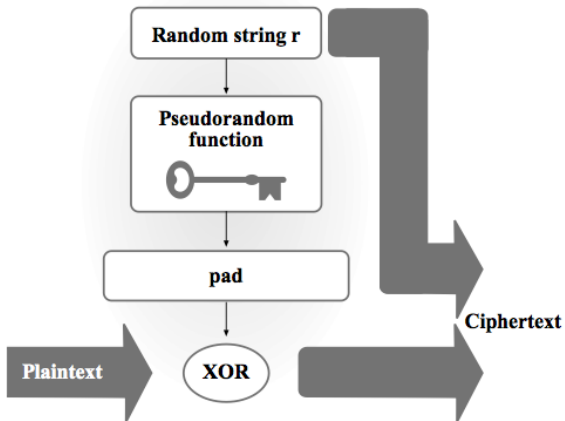
$$Enc_k(m) = F_k(m)$$

Deterministico ... non funziona ... (stesso messaggio  $\Rightarrow$  stesso cifrato)

Approccio giusto:

Applichiamo  $F_k$  ad una stringa casuale  $r$  per produrre un "pad" pseudocasuale.

Cifriamo calcolando l'xor tra il pad ed il messaggio  $m$ .



## **CONSTRUCTION 3.30**

Let  $F$  be a pseudorandom function. Define a private-key encryption scheme for messages of length  $n$  as follows:

- Gen: on input  $1^n$ , choose uniform  $k \in \{0, 1\}^n$  and output it.
- Enc: on input a key  $k \in \{0, 1\}^n$  and a message  $m \in \{0, 1\}^n$ , choose uniform  $r \in \{0, 1\}^n$  and output the ciphertext

$$c := \langle r, F_k(r) \oplus m \rangle.$$

- Dec: on input a key  $k \in \{0, 1\}^n$  and a ciphertext  $c = \langle r, s \rangle$ , output the plaintext message

$$m := F_k(r) \oplus s.$$

**Teorema 3.31.** Se  $F$  è pseudocasuale, allora la Costruzione 3.30 realizza uno schema di cifratura CPA-sicuro per messaggi di lunghezza  $n$ .

**Dim.** Nota preliminare: le prove di sicurezza per schemi basati su PRF procedono solitamente in due fasi

- Prima fase: consideriamo una versione "ipotetica" della costruzione in cui la funzione pseudocasuale viene sostituita da una funzione casuale. Mostriamo che questa modifica *non* influisce sulla probabilità di successo di Adv
- Seconda fase: analizziamo lo schema ipotetico che utilizza la funzione casuale

Sia  $\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$  costruito a partire da  $\Pi = (Gen, Enc, Dec)$ , tale che

- $\tilde{\Pi}$  usa  $f \in Func_n$  scelta uniformemente a caso
- $\Pi$  usa  $F_k$ , dove  $k$  è scelta uniformemente a caso

Ovviamente,  $\tilde{\Pi}$  non è efficiente:  $f$  richiede spazio esponenziale in  $n$  per la memorizzazione.

Per ogni Adv  $A$  PPT sia  $q(n)$  un limite superiore al numero di query che  $A(1^n)$  rivolge al suo oracolo per la cifratura ( $q(n)$  deve essere un polinomio)

Mostriamo che esiste una funzione trascurabile  $negl$  tale che

$$|Pr[PrivK_{A,\Pi}^{cpa}(n) = 1] - Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1]| \leq negl(n).$$

Procediamo per riduzione: usiamo  $A$  per costruire un distinguisher  $D$  per la funzione pseudocasuale  $F$

Se  $A$  ha successo contro  $\Pi$  (con prob. significativa)  
 $\Rightarrow D$  distingue (con prob. significativa)

Precisamente:

- $D$  ha accesso all'oracolo  $O(\cdot)$  ed il suo scopo è stabilire se la funzione è " $F_k$ , per  $k$  uniforme in  $\{0,1\}^n$ " oppure " $f \in \text{Func}_n$ , uniforme".
- $D$  emula l'esperimento  $\text{PrivK}_{A,?}^{cpa}(n)$  per  $A$  ed osserva se  $A$  ha successo.



## Distinguisher $D$ :

$D$  is given input  $1^n$  and access to an oracle  $\mathcal{O} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ .

1. Run  $\mathcal{A}(1^n)$ . Whenever  $\mathcal{A}$  queries its encryption oracle on a message  $m \in \{0, 1\}^n$ , answer this query in the following way:
  - (a) Choose uniform  $r \in \{0, 1\}^n$ .
  - (b) Query  $\mathcal{O}(r)$  and obtain response  $y$ .
  - (c) Return the ciphertext  $\langle r, y \oplus m \rangle$  to  $\mathcal{A}$ .
2. When  $\mathcal{A}$  outputs messages  $m_0, m_1 \in \{0, 1\}^n$ , choose a uniform bit  $b \in \{0, 1\}$  and then:
  - (a) Choose uniform  $r \in \{0, 1\}^n$ .
  - (b) Query  $\mathcal{O}(r)$  and obtain response  $y$ .
  - (c) Return the challenge ciphertext  $\langle r, y \oplus m_b \rangle$  to  $\mathcal{A}$ .
3. Continue answering encryption-oracle queries of  $\mathcal{A}$  as before until  $\mathcal{A}$  outputs a bit  $b'$ . Output 1 if  $b' = b$ , and 0 otherwise.

$D$  computa in tempo polinomiale poichè  $A$  computa in tempo polinomiale.  
Inoltre, si noti che:

- 1 Se l'oracolo di  $D$  contiene al suo interno una funzione **pseudocasuale**

Vista di  $A$  come subroutine di  $D =$  Vista di  $A$  in  $\text{PrivK}_{A,\Pi}^{cpa}(n)$

- 2 Se l'oracolo di  $D$  contiene al suo interno una funzione **casuale**

Vista di  $A$  come subroutine di  $D =$  Vista di  $A$  in  $\text{PrivK}_{A,\tilde{\Pi}}^{cpa}(n)$

Pertanto, possiamo dire che:

$$\textcircled{1} \Rightarrow \Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] = \Pr[\text{PrivK}_{A,\Pi}^{cpa}(n) = 1]$$

$$\textcircled{2} \Rightarrow \Pr_{f \leftarrow \text{Func}_n} [D^{f(\cdot)}(1^n) = 1] = \Pr[\text{PrivK}_{A,\tilde{\Pi}}^{cpa}(n) = 1]$$

Ma l'assunzione che  $F$  è pseudocasuale implica che  $\exists \text{negl}(n)$  tale che:

$$|\Pr_{k \leftarrow \{0,1\}^n} [D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \text{Func}_n} [D^{f(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$



$$|\Pr[\text{PrivK}_{A,\Pi}^{cpa}(n) = 1] - \Pr[\text{PrivK}_{A,\tilde{\Pi}}^{cpa}(n) = 1]| \leq \text{negl}(n)$$

Pertanto possiamo analizzare lo schema ipotetico.

# Successo di $A$ nello schema ipotetico

Mostriamo che

$$\Pr[\text{PrivK}_{A, \tilde{\Pi}}^{\text{cpa}}(n) = 1] \leq 1/2 + q(n)/2^n.$$

Nota che, ogni volta che un messaggio  $m$  viene cifrato, in  $\text{PrivK}_{A, \tilde{\Pi}}^{\text{cpa}}(n)$  viene scelto un  $r \in \{0, 1\}^n$  uniforme, ed il cifrato risulta

$$\langle r, f(r) \oplus m \rangle$$

Sia  $r^*$  la stringa usata per produrre il cifrato di sfida, cioè

$$c^* := \langle r^*, f(r^*) \oplus m_b \rangle$$

Possono verificarsi due casi:

# Successo di $A$ nello schema ipotetico

- Il valore di  $r^*$  non è mai usato prima da  $O(\cdot)$  per rispondere alle query di  $A$

$\Rightarrow A$  non sa nulla circa  $f(r^*)$ , che risulta uniforme ed indipendentemente distribuito dal resto dell'esperimento

$$\Rightarrow \Pr[\text{PrivK}_{A, \tilde{\Pi}}^{\text{cpa}}(n) = 1] = \Pr[b' = b] = 1/2$$

- Il valore di  $r^*$  è stato usato in precedenza

$\Rightarrow A$  può capire facilmente se è stato cifrato  $m_0$  o  $m_1$ . Infatti, disponendo di  $f(r^*)$ , poichè  $c^* := \langle r^*, f(r^*) \oplus m_b \rangle$ , risulta

$$f(r^*) \oplus (f(r^*) \oplus m_b) = m_b.$$

Il valore  $f(r^*)$  può essere recuperato dalla query in cui  $r^*$  è usato: se  $A$  ha ricevuto dall'oracolo, per qualche  $m$ , il cifrato  $c := \langle r^*, s \rangle = \langle r^*, f(r^*) \oplus m \rangle$ , allora

$$s \oplus m = f(r^*).$$

# Successo di $A$ nello schema ipotetico

Tuttavia, poichè  $A$  effettua al più  $q(n)$  query all'oracolo, al più  $q(n)$  valori distinti di  $r$  vengono usati, scelti indip. e uniformemente in  $\{0,1\}^n$ .

Pertanto, la prob. che  $r^*$ , scelto uniformemente, sia uguale ad un  $r$  precedente è al più  $q(n)/2^n$ .

Indichiamo con **Repeat** l'evento che  $r^*$  sia uguale a qualche  $r$  scelto prima.

Risulta  $Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1]$  uguale a

$$\begin{aligned} & Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1 \wedge \mathbf{Repeat}] + Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1 \wedge \overline{\mathbf{Repeat}}] \\ \leq & Pr[\mathbf{Repeat}] + Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1 \mid \overline{\mathbf{Repeat}}] \cdot Pr[\overline{\mathbf{Repeat}}] \\ \leq & Pr[\mathbf{Repeat}] + Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1 \mid \overline{\mathbf{Repeat}}] \\ \leq & q(n)/2^n + 1/2. \end{aligned}$$

# Successo di $A$ nello schema ipotetico

Poichè abbiamo mostrato che

$$|Pr[PrivK_{A,\Pi}^{cpa}(n) = 1] - Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1]| \leq \text{negl}(n)$$

si ha:

$$\begin{aligned} Pr[PrivK_{A,\Pi}^{cpa}(n) = 1] &\leq Pr[PrivK_{A,\tilde{\Pi}}^{cpa}(n) = 1] + \text{negl}(n) \\ &\leq q(n)/2^n + 1/2 + \text{negl}(n) \\ &\leq 1/2 + q(n)/2^n + \text{negl}(n) \\ &\leq 1/2 + \text{negl}'(n). \end{aligned}$$

Pertanto,  $\Pi$  è CPA-sicuro.