

1. Sia  $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$  una funzione pseudocasuale sicura e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme  $\{0,1\}^{L+1}$ . L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza  $n$ . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq L + 1$ ) return  $\perp$ 
   $r \leftarrow_R \{0,1\}^\ell$ 
  Sia  $m = m_1m_2\dots m_Lm_{L+1}$ 
   $y \leftarrow F_k(r) \oplus (m_1m_2\dots m_L)$ 
   $c \leftarrow y||m_{n+1}$ 
  return  $(c, r)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(c, r)
  if ( $|c| \neq L + 1$ ) return  $\perp$ 
  Sia  $y$  la stringa composta dai primi  $L$  bit di  $c$ 
   $M \leftarrow (y \oplus F_k(r))||c_{L+1}$ 
  return  $M$ 
```

E' questo metodo sicuro? Giustificare la risposta fornita.

SI HA UN AVVERSARIO A CHE HA ACCESSO  
BLACK BOX ALL'ORAColo DI CIFRATURA LR

PASSIAMO OSSERVARE CHE  $m_{L+1} = c_{L+1}$  QUINDI  
SI CONSIDERI  $x \in \{0,1\}^L$  E SIANO:

$$x_0 = x||0$$

$$x_1 = x||1$$

NEL MOMENTO IN CUI CIFRIAMO  $\text{Enc}_k(x_0)$  SI HA:

$$m = x_0^1 x_0^2 \dots x_0^L x_0^{L+1}$$

$$y \leftarrow F_k(r) \oplus m$$

$$c \leftarrow y||x_0^{L+1}$$

LA STESSA COSA SI OTTIENE CON  $\text{Enc}_k(x_1)$ :

$$c'' \leftarrow y||x_1^{L+1}$$

L'AVVERSARIO PUÒ EFFETTUARE IL SEGUENTE  
CONTROLLO: SE  $C_{L+1}$  È UGUALI A  $X_1^{L+1}$  ALLORA  
L'AVVERSARIO SI TROVA NEL MONDO 1, ALTRIMENTI  
NEL MONDO 0.

DEFINIAMO FORMALMENTE TALE AVVERSARIO:

A() :

$$X \leftarrow \{0, 1\}^L$$

$$X_0 = X \| 0$$

$$X_1 = X \| 1$$

$$C \leftarrow O_{ENC}(X_0, X_1)$$

if ( $C_{L+1} == 1$ ) return 1  
else return 0

$$\Pr[\text{Esp}^{\text{ind-CPA-1}}(A) = 1] = 1$$

$$\Pr[\text{Esp}^{\text{ind-CPA-0}}(A) = 1] = 0$$

$$\text{Adv}^{\text{ind-CPA}}(A) = |1 - 0| = 1$$

ABBIAMO DIMOSTRATO CHE QUESTO METODO  
NON È SICURO!

2. Sia  $F : \{0,1\}^k \times \{0,1\}^{\lambda\ell} \rightarrow \{0,1\}^L$  una funzione pseudocasuale e  $H$  una funzione hash resistente alle collisioni il cui insieme dei valori è  $\{0,1\}^L$ . Si consideri il seguente schema MAC II = (KeyGen, MAC, Ver).

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza  $t\ell$ , per  $0 \leq t \leq \lambda$ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di  $k$  bit. L'algoritmo MAC è definito come segue:

```

MACk(M)
  if ( $|M| \bmod \ell \neq 0$  or  $|M| > \ell\lambda$ ) return ⊥
   $k' \leftarrow_R F_k(|M|)$ 
  Let  $M = M_1 \cdots M_n$  (con  $|M_i| = \ell$ )
  for  $i = 1$  to  $n$ 
     $y_i \leftarrow F_k(M_i) \oplus H(M_i)$ 
   $Tag \leftarrow y_1 || \dots || y_n$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non è sicuro.

$$M = \{0,1\}^{t\ell} \quad 0 \leq t \leq \lambda$$

CONSIDERIAMO  $x, y \in M$  E SI HA  $z = x \parallel y$   
 LA CARDINALITÀ DI  $z$  È SICURAMENTE UN MULTIPLO  
 DI  $\ell$  E SARÀ MAGGIORE DI  $\ell\lambda$ .

A QUESTO PUNTO SI HA:

$$y_0 = F_k(x) \oplus H(x)$$

$$y_1 = F_k(y) \oplus H(y)$$

$$\text{Tag}' \leftarrow y_0 \parallel y_1$$

L'AVVERSARIO PUÒ CONSIDERARE  $w = y \parallel x$   
 PER CUI SI HA:

$$\text{Tag}'' \leftarrow y_1 \parallel y_0$$

DEFINIAMO FORMALMENTE L'AVVERSARIO:

A( $\Pi$ ):

$$x \leftarrow M$$

$$y \leftarrow M$$

$$z \leftarrow x || y$$

$$\begin{aligned} \text{Tag}' &\leftarrow O_{\text{MAC}}(z) \quad // \quad \text{Tag}' = y_0 || y_1 = \\ \text{Tag}'' &\leftarrow y_1 || y_0 \\ w &\leftarrow y || z \end{aligned}$$

$$\begin{aligned} &= F_k(x) \oplus H(x) || \\ &F_k(y) \oplus H(y) \end{aligned}$$

$$d \leftarrow \text{VF}_k(w, \text{Tag}'')$$

$$\Pr[\text{Esp}_{\Pi}^{\text{uf-cma}}(A) = 1] = 1$$

QUINDI:

$$\text{Adv}_{\Pi}^{\text{uf-cma}}(A) = 1$$

LO SCHEMA NON È SICURO!

3. Sia  $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$  una funzione pseudocasuale sicura e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme  $\{0, 1\}^L$ . L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza  $n$ . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
if ( $|M| \neq L$ ) return  $\perp$ 
if ( $M \bmod 2 == 0$ ) IV  $\leftarrow 0^\ell$ 
else IV  $\leftarrow 1^\ell$ 
 $c \leftarrow M \oplus F_k(IV)$ 
return  $(c, IV)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(c, IV)
if ( $|c| \neq L$ ) return  $\perp$ 
 $M \leftarrow c \oplus F_k(IV)$ 
return  $M$ 
```

E' questo metodo sicuro? Giustificare la risposta fornita.

SI CONSIDERI  $x \in \{0, 1\}^{L-1}$  PER CUI SI HA  
 $m_0 = x||0$  E  $m_1 = x||1$ .  $|m_0| = |m_1| = L$   
 QUINDI ENTRAMBE LE STRINGHE POSSANO ESSERE  
 CIFRATE. L'AVVERSARIO FARÀ I SEGUENTI PASSI:

- USA L'ORACOLO UNA PRIMA VOLTA PASSANDO  $m_0, m_1$  PER CUI OTTIENE  $C' \leftarrow \text{Enc}(m_0, m_1)$ ;
- USA L'ORACOLO UNA SECONDA VOLTA PASSANDO  $m_1, m_2$  PER CUI OTTIENE  $C'' \leftarrow \text{Enc}(m_1, m_2)$ ;

ALLORA:

$C = (c, IV)$ ;  $c = M \oplus F_k(IV)$   
 SE  $IV = 1^\ell$ , M È DISPARI QUINDI  $M = m_1$ ,  
 ALTRIMENTI SE  $IV = 0^\ell$ , M È PARI QUINDI  $M = m_0$   
 QUINDI SE  $C' = C''$  VUOL DIRE CHE L'AVVERSARIO  
 SI TROVA NEL MONDO 1, ALTRIMENTI NEL MONDO  
 0.

DEFINIAMO FORMALMENTE L'AVVERSARIO:

$A(E)$ :

$$\times \left\{ 0, 1 \right\}^{L-1}$$

$$m_0 = \times 110$$

$$m_1 = \times 111$$

$$c' = O_{ENC}(m_0, m_1)$$

$$c'' = O_{ENC}(m_2, m_1)$$

if ( $c' == c''$ ) return 1

else return 0

$$\Pr[E \stackrel{\text{ind-CPA}}{=} E(A) = 1] = 1$$

$$\Pr[E \stackrel{\text{ind-CPA}}{=} E(A) = 0] = 0$$

$$\text{Adv}_E^{\text{ind-CPA}}(A) = 1$$

4. Sia  $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$  una funzione pseudocasuale sicura e si consideri il seguente schema MAC (probabilistico)  $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$ .

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza  $t\ell$  ( $t \geq 1$ ).

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di  $k$  bit. L'algoritmo MAC è definito come segue:

```
MACk(M)
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $r \leftarrow_R \{0,1\}^\ell$ 
   $\text{Tag} \leftarrow F_k(r) \oplus F_k(M[1]) \oplus \cdots \oplus F_k(M[n])$ 
  Return  $(r, \text{Tag})$ 
```

L'algoritmo di verifica funziona nel seguente modo

```
Verk(M, (r, Tag))
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $T \leftarrow F_k(r) \oplus F_k(M[1]) \oplus \cdots \oplus F_k(M[n])$ 
  if Return  $T = \text{Tag}$  return 1
  else return 0
```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

SI CONSIDERINO  $m_0, m_1 \in \{0, 1\}^\ell$  E SI EFFETTUINO I SEGUENTI PASSI:

- $\Pi = m_0 \parallel m_1$
- $\text{MAC}_k(\Pi) = F_k(r) \oplus F_k(m_0) \oplus F_k(m_1) = (r, \overline{\text{Tag}})$

A QUESTO PUNTO È POSSIBILE CONSIDERARE  $\Pi' = m_1 \parallel m_0$  IL CUI  $\text{Tag}' = \overline{\text{Tag}}$  INFATTI:

$\text{Ver}_k(\Pi', (r, \overline{\text{Tag}}')) = 1$

SI DEFINISCE L'AVVERSARIO FORMALMENTE:  
 $A(\Pi)$ :

$m_0, m_1 \xleftarrow{R} \{0, 1\}^\ell$

$\Pi = m_0 \parallel m_1$

$\overline{\text{Tag}} = O_\Pi(\Pi) \parallel \text{Tag} = (r, \overline{\text{tag}})$

$\text{Ver}_k(m_1 \parallel m_0, \overline{\text{Tag}}')$

$\boxed{\Pr_{\Pi}(\text{Esp}_\Pi^{\text{inf-Cma}}(A) = 1) = 1}$   
 $\boxed{\text{Adv}(A) = 1}$

LO SCHEMA  
NON È SICURO!

5. Sia  $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$  una funzione pseudocasuale sicura e si consideri il seguente schema MAC (deterministico e senza stati)  $\Pi = (\text{KeyGen}, \text{MAC})$ .

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza  $t\ell$  ( $t$  arbitrario ma tale che  $t > 2$ ).

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di  $k$  bit. L'algoritmo MAC è definito come segue:

$\text{MAC}_k(M)$

```

if ( $|M| \bmod \ell \neq 0 \vee |M| < 2\ell$ ) return  $\perp$ 
Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
for  $i = 1, \dots, n$   $y_i \leftarrow F_k(M[i])$ 
 $Tag \leftarrow y_1 || y_n$ 
Return  $Tag$ 

```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

$$M \in \{0,1\}^{t\ell}, t > 2$$

SI CONSIDERI  $m \in \{0,1\}^{t\ell}$  PER CUI SI HA CHE  
 $|m| \bmod \ell = 0$  E  $|m| > 2\ell$  QUINDI  $m$   
 RAPPRESENTA UNA STRINGA VALIDA.

SIA  $X = m[1] \dots m[n]$  CON  $|m[i]| = \ell$ .

SIA  $y_i = F_k(m[i])$  PER  $i = 1, \dots, n$

$$\text{ALLORA } Tag = y_1 || y_m$$

A QUESTO PUNTO È POSSIBILE CONSIDERARE  
 $x' = m[m]m[2] \dots m[m-1]m[1]$

$$\text{ALLORA } Tag' = y_m || y_1$$

SI DEFINISCE FORMALMENTE L'AVVERSARIO:

$A(\Pi)$ :

$$m \xleftarrow{R} \{0,1\}^{t\ell}$$

$$X = m[1] \dots m[m]$$

$$Tag = O_\Pi(X) // Tag' = y_1 || y_m$$

$$x' = m[m]m[2] \dots m[m-1]m[1]$$

$$VF_k(x', y_m || y_1)$$

$$\Pr[\text{ESP}_{\pi}^{\text{uf-cma}}(A) = 1] = 1$$

$$\text{Adv}_{\pi}^{\text{uf-cma}}(A) = 1$$

Lo SCHEMA NON È SICURO!