Corso di Crittografia

Prova in Itinere del 20 Dicembre 2021

1. Introdurre e definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a crittotesto scelto) per cifrari simmetrici.

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

   $\mathbf{Enc}_k(M)$
   - if $(|M| \neq 3\ell)$ return $\perp$
   - Sia $M = M_1||M_2||M_3$ $\quad |M_i| = \ell$, *e* $||$ *indica concatenazione*
   - $r \leftarrow_R \{0,1\}^\ell$
   - $c_1 \leftarrow E_k(M_1) \oplus r$
   - $c_2 \leftarrow E_k(r) \oplus M_2$
   - $c_3 \leftarrow E_k(c_2) \oplus M_3$
   - $c \leftarrow c_1||c_2||c_3$
   - return (r, c)

   l'algoritmo di decifratura corrispondente è

   $\mathbf{Dec}_k(y_0, c)$
   - if $(|c| \neq 3\ell)$ return $\perp$
   - Sia $c = c_1||c_2||c_3$
   - $M_1 \leftarrow E_k^{-1}(r \oplus c_1)$
   - $M_2 \leftarrow E_k(r) \oplus c_2$
   - $M_3 \leftarrow E_k(c_2) \oplus c_3$
   - $M \leftarrow M_1||M_2||M_3$
   - return M

   Dimostrare che tale cifrario non è sicuro in senso IND-CPA.

3. In classe abbiamo definito il concetto di funzione resistente alle collisioni ($\mathtt{cr2-kk}$).

   Introduciamo adesso la nozione di funzione *twin collision resistance.*

   Sia $H : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^t$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

Esperimento $\mathbf{Esp}_H^{\texttt{twin-cr-kk}}(A)$

$k \leftarrow_R \mathcal{K}$;

$(y, x_1, x_2, x_3) \leftarrow A(k)$;

if $(H_k(y \oplus H_k(x_1 \oplus x_2)) = H_k(y \oplus H_k(x_1 \oplus x_3))$ and $(x_2 \neq x_3)$ and $(x_1, x_2, x_3 \in \{0,1\}^*, y \in \{0,1\}^t))$ Return 1

else Return 0

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\texttt{twin-cr-kk}} = \Pr\left[\mathbf{Esp}_H^{\texttt{twin-cr-kk}}(A) = 1\right]$$

Diciamo che H è una funzione twin-collision resistant se tale vantaggio è prossimo a zero per ogni avversario polinomialmente limitato.

Si dimostri che ogni funzione resistente alle collisioni è anche una funzione twin-collision resistant.

4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per message authentication codes.

5. Sia $F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$ una funzione pseudocasuale, si consideri il seguente schema MAC, $\Pi = (\texttt{KeyGen}, \texttt{MAC}, \texttt{Ver})$.

   Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 2ℓ.

   L'algoritmo di generazione della chiave si limita a restituire due stringhe casuali di n bit (k, x). L'algoritmo `MAC` è definito come segue:

   $\mathbf{MAC}_k(M)$

   if $(|M| \neq 2\ell)$ return $\perp$

   Sia $M = M_1||M_2$ // $|M_i| = \ell$

   $Tag \leftarrow (F_k(1) \oplus M_1) \oplus x || (F_k(2) \oplus M_2) \oplus x$ Return Tag

   Dimostrare che tale schema non e' sicuro.