Definizione di Perfetta Sicurezza Alternativa

Sia $SE = (KeyGen, Enc, Dec)$ uno schema di cifratura con spazio dei messaggi M è perfettamente sicuro se per ogni distribuzione di probabilità su M, ogni messaggio $m \in M$ e ogni critto-testo $c \in C$ per cui $Pr[C = c] > 0$:

$$Pr[M = m|C = c] = Pr[M = m]$$

Teorema di Shannon (2)

Sia $SE = (KeyGen, Enc, Dec)$ uno schema di cifratura con uno spazio dei messaggi M, tale che $|M| = |K| = |C|$. Lo schema è perfettamente sicuro se e solo se:

1. $\forall k \in K$ è scelta con probabilità pari a $\frac{1}{|K|}$ dall'algoritmo $KeyGen$;
2. $\forall m \in M \wedge \forall c \in C$, esiste un'unica chiave $k \in K$ tale che $Enc_k(m) = c$.

Dimostrazione informale

(=>) L'intuizione dietro la dimostrazione è la seguente. Per vedere che le condizioni dichiarate implicano la perfetta sicurezza, si noti che la condizione **(2)** significa che qualsiasi testo cifrato c potrebbe essere il risultato della cifratura di qualsiasi possibile testo in chiaro m, perché esiste una qualche chiave k che mappa da m a c. Poiché esiste una tale chiave univoca e ogni chiave viene scelta con uguale probabilità, la perfetta sicurezza segue come per **OTP**.

(<=) Per l'altra direzione, la perfetta sicurezza implica immediatamente che per ogni m e c c'è almeno una mappatura delle chiavi da m a c. Il fatto che $|M| = |K| = |C|$ significa, inoltre, che per ogni m e c esiste esattamente una tale chiave $k \in K$. Detto questo, ogni chiave deve essere scelta con uguale probabilità, altrimenti la perfetta sicurezza non reggerebbe.

Dimostrazione formale

Assumiamo per semplicità che **Enc** sia deterministico. (Si può dimostrare che questo è senza perdita di generalità qui.) Dimostriamo innanzitutto che se lo schema di cifratura soddisfa le condizioni **(1)** e **(2)**, allora è perfettamente sicuro. La dimostrazione è essenzialmente la stessa di quella fatta per one-time pad. Si fissi arbitrariamente $c \in C$ e $m \in M$. Sia k la chiave univoca, garantita dalla condizione **(2)**, per la quale $Enc_k(m) = c$. Quindi,

$$Pr[C = c|M = m] = Pr[Enc_k(m) = c] = Pr[K = k] = \frac{1}{|K|}$$

l'uguaglianza finale vale per la condizione (1). Quindi:

$$Pr[C=c] = \sum_{m \in M} Pr(C=c, M=m) =$$
$$= \sum_{m \in M} Pr[C=c|M=m] \cdot Pr[M=m] =$$
$$= \sum_{m \in M} Pr[Enk_k(m)=c] \cdot Pr[M=m]$$

Questa probabilità viene chiamata **marginale**. Effettuando i conti otteniamo:

$$Pr[C=c] = \sum_{m \in M} \frac{1}{|K|} \cdot \frac{1}{|M|} = |M| \cdot \frac{1}{|K|} \cdot \frac{1}{|M|} = \frac{1}{|K|}$$

Questo vale per qualsiasi distribuzione su M. Quindi, per ogni distribuzione su M, ogni $m \in M$ con $Pr[M=m] \neq 0$ e ogni $c \in C$, si ha:

$$Pr[M=m|C=c] = \frac{Pr[C=c|M=m] \cdot Pr[M=m]}{Pr[C=c]} =$$
$$= \frac{Pr[Enc_k(m)=c] \cdot Pr[M=m]}{Pr[C=c]} = \frac{|K|^{-1} \cdot Pr[M=m]}{|K|^{-1}} = Pr[M=m]$$

quindi lo schema è perfettamente sicuro.

Per la seconda direzione, assumiamo che lo schema di cifratura sia perfettamente sicuro; mostriamo che valgono le condizioni **(1)** e **(2)**. Fissiamo arbitrariamente $c \in C$. Ci deve essere un messaggio m^* per il quale $Pr[Enc_k(m*)=c] \neq 0$, ma per la definizione di perfetta sicurezza (quella classica che conosciamo), deve valere che $\forall m_1, m_2 \in M \wedge \forall c \in C$, $Pr[Enc_k(m_1)=c] = Pr[Enc_k(m_2)=c]$. Questo significa che per ogni messaggio $m_i \in M$, posso associargli un insieme delle chiavi $K_i \subset K$ tale che $Enk_k(m_i) = c$ se e solo se $k \in K_i$. Inoltre, quando $i \neq j$ allora $K_i \cap K_j = \emptyset$. Dato che $|K| = |M|$ allora ogni K_i contiene una sola chiave, come richiesto dalla condizione **(2)**. Quindi si ha:

$$Pr[K=k_i] = Pr[Enc_k(m_i)=c] = Pr[Enc_k(m_j)=c] = Pr[K=k_j]$$

Dato che vale $1 \leq i, j \leq |M| = |K|$ e $k_i \neq k_j$ per $i \neq j$, questo significa che ogni chiave è scelta con probabilità $\frac{1}{|K|}$, come richiesto dalla condizione **(1)**.