3 Segretezza Perfetta

Nel 1949, Claude Shannon pubblicò sulla rivista ***"Bell Systems Technical Journal"*** un articolo dal titolo ***"Communication Theory of Secrecy Systems"***. Questo articolo ebbe una notevole influenza sullo studio della crittografia.

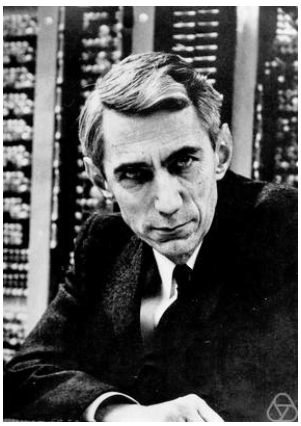

Figura 3.1: Claude Elwood Shannon (1916 – 2001) e il suo celebre articolo del 1949.

In questo capitolo discutiamo varie idee di Shannon. In primo luogo, tuttavia, consideriamo alcuni dei vari approcci per valutare la sicurezza di un crittosistema e definiamo alcuni dei criteri più utilizzati ora.

3.1 Criteri di Sicurezza

Definizione 3.1. Un crittosistema si dice **computazionalmente sicuro** se il miglior algoritmo per violare il sistema richiede almeno N operazioni, dove N è un numero specificato molto elevato.

Nella realtà nessun crittosistema è computazionalmente sicuro. Infatti, un crittosistema può essere computazionalmente sicuro **solo** rispetto a certi tipi di attacchi ma non ad altri.

Definizione 3.2. Un crittosistema si dice **dimostrabilmente sicuro** se la sua sicurezza si basa sulla difficoltà di risoluzione di un problema ampiamente studiato.

La sicurezza dimostrabile di un crittosistema **relativa** ad un problema non è una dimostrazione assoluta di sicurezza.

Definizione 3.3. Un crittosistema si dice **incondizionatamente sicuro** se esso non può essere violato anche se l'avversario è munito di risorse computazionali infinite.

Quando si studia la sicurezza di un crittosistema è necessario specificare il tipo di attacco rispetto al quale la si analizza. Per esempio, i crittosistemi affini e di Vigenère **non** sono computazionalmente sicuri rispetto all'attacco basato sulla conoscenza del testo cifrato, se l'avversario ha a disposizione una quantità sufficiente di quest'ultimo.

Analizziamo alcuni crittosistemi che sono incondizionatamente sicuri rispetto all'attacco basato sulla conoscenza del testo cifrato, se quest'ultimo è sufficientemente piccolo. Come conseguenza di quest'analisi, otterremo che i crittosistemi affini e di Vigenère sono incondizionatamente sicuri, se ogni messaggio in chiaro è cifrato con una chiave diversa, e nel caso di Vigenère, se il messaggio e la chiave hanno la stessa lunghezza.

3.2 Segretezza Perfetta

Sia $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ un crittosistema in cui ogni chiave $K \in \mathcal{K}$ viene utilizzata per una sola cifratura. Supponiamo che

(1) Sia definita una distribuzione di probabilità nello spazio delle unità di messaggio in chiaro $\mathcal{P}$. Questa definisce una variabile aleatoria che denoteremo con $\mathbf{x}$. Quindi, la probabilità che la variabile $\mathbf{x}$ assuma valore x sarà denotata con $\mathbf{P}[\mathbf{x} = x]$.
(2) Sia definita una distribuzione di probabilità nello spazio delle chiavi $\mathcal{K}$. Questa definisce una variabile aleatoria che denoteremo con $\mathbf{K}$. La probabilità che la variabile $\mathbf{K}$ assuma valore K sarà denotata con $\mathbf{P}[\mathbf{K} = K]$.
(3) Le variabili $\mathbf{x}$ e $\mathbf{K}$ siano indipendenti (segue dal fatto che le chiavi vengono scelte dagli utenti crittosistema prima del testo da cifrare).

Le distribuzioni di probabilità su $\mathcal{P}$ e $\mathcal{K}$ inducono una distribuzione di probabilità su $\mathcal{C}$. Questa, a sua volta, definisce una variabile aleatoria $\mathbf{y}$.
Quindi

$$\begin{aligned}\mathbf{P}[\mathbf{y} = y] &= \sum_{\{K:y\in e_K(\mathcal{P})\}} \mathbf{P}[\mathbf{K} = K, \mathbf{x} = d_K(y)] = \\ &= \sum_{\{K:y\in e_K(\mathcal{P})\}} \mathbf{P}[\mathbf{K} = K]\mathbf{P}[\mathbf{x} = d_K(y)].\end{aligned}$$

Inoltre

$$\mathbf{P}[\mathbf{y} = y \mid \mathbf{x} = x] = \sum_{\{K:x=d_K(y)\}} \mathbf{P}[\mathbf{K} = K].$$

E quindi, utilizzando il **Teorema di Bayes**, si ha che

$$\begin{aligned}\mathbf{P}[\mathbf{x} = x \mid \mathbf{y} = y] &= \frac{\mathbf{P}[\mathbf{x} = x]\mathbf{P}[\mathbf{y} = y \mid \mathbf{x} = x]}{\mathbf{P}[\mathbf{y} = y]} = \\ &= \frac{\mathbf{P}[\mathbf{x} = x] \times \sum_{\{K:x=d_K(y)\}} \mathbf{P}[\mathbf{K} = K]}{\sum_{\{K:y\in e_K(\mathcal{P})\}} \mathbf{P}[\mathbf{K} = K]\mathbf{P}[\mathbf{x} = d_K(y)]}.\end{aligned}$$

Esempio 3.4. Si consideri il crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, dove $\mathcal{P} = \{a, b\}$, $\mathcal{C} = \{1, 2, 3, 4\}$ e $\mathcal{K} = \{K_1, K_2, K_3\}$ e dove $\mathcal{E}, \mathcal{D}$ sono definite mediante la seguente **matrice di cifratura**

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

e supponiamo che soddisfi le ipotesi **(1)**–**(3)**.
Quindi, siano $\mathbf{P}[a] = 1/4$ e $\mathbf{P}[b] = 3/4$, e $\mathbf{P}[K_1] = 1/2$ e $\mathbf{P}[K_2] = \mathbf{P}[K_3] = 1/4$ le distribuzioni di probabilità su $\mathcal{P}$ e $\mathcal{K}$, rispettivamente.

Calcoliamo la distribuzione di probabilità su $\mathcal{C}$

$$\begin{aligned}\mathbf{P}[1] &= \mathbf{P}[K_1]\mathbf{P}[a] = 1/8 \\ \mathbf{P}[2] &= \mathbf{P}[K_1]\mathbf{P}[b] + \mathbf{P}[K_2]\mathbf{P}[a] = 3/8 + 1/16 = 7/16 \\ \mathbf{P}[3] &= \mathbf{P}[K_2]\mathbf{P}[b] + \mathbf{P}[K_3]\mathbf{P}[a] = 3/16 + 1/16 = 1/4 \\ \mathbf{P}[4] &= \mathbf{P}[K_3]\mathbf{P}[b] = 3/16.\end{aligned}$$

Infine, calcoliamo la probabilità condizionata

$$\begin{aligned}
\mathbf{P}[a \mid 1] &= \frac{\mathbf{P}[a]\mathbf{P}[K_1]}{\mathbf{P}[1]} = \frac{1/4 \times 1/2}{1/8} = 1 \\
\mathbf{P}[a \mid 2] &= \frac{\mathbf{P}[a]\mathbf{P}[K_2]}{\mathbf{P}[2]} = \frac{1/4 \times 1/4}{7/16} = 1/7 \\
\mathbf{P}[a \mid 3] &= \frac{\mathbf{P}[a]\mathbf{P}[K_3]}{\mathbf{P}[3]} = \frac{1/4 \times 1/4}{1/4} = 1/4 \\
\mathbf{P}[a \mid 4] &= \frac{\mathbf{P}[a] \times 0}{\mathbf{P}[4]} = 0.
\end{aligned}$$

In modo analogo si calcolano $\mathbf{P}[b \mid y]$ con $y \in \mathcal{C}$.

Definizione 3.5. Un crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ fornisce **segretezza perfetta** se per ogni $x \in \mathcal{P}$ e $y \in \mathcal{C}$ risulta $\mathbf{P}[x \mid y] = \mathbf{P}[x]$.

In altre parole, i crittosistemi dotati di segretezza perfetta sono tutti e soli quelli in cui la conoscenza del testo cifrato non fornisce alcuna informazione sul testo in chiaro.

Lemma 3.6. *Se un crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ fornisce segretezza perfetta, allora per ogni $x \in \mathcal{P}$ e $y \in \mathcal{C}$ esiste almeno una chiave $K \in \mathcal{K}$ tale che $y = e_K(x)$. In particolare, $|\mathcal{K}| \geq |\mathcal{P}|$.*

Dimostrazione. Siano $x \in \mathcal{P}$ e $y \in \mathcal{C}$, allora per il **Teorema di Bayes** e per la segretezza perfetta vale che

$$\mathbf{P}[y \mid x] = \mathbf{P}[y].$$

Possiamo assumere che $\mathbf{P}[y] > 0$ per ogni $y \in \mathcal{C}$, altrimenti consideriamo $(\mathcal{P}, \mathcal{C}', \mathcal{K}, \mathcal{E}, \mathcal{D})$ con $\mathcal{C}' = \mathcal{C} - \{y\}$. Pertanto, per ogni $x \in \mathcal{P}$ e $y \in \mathcal{C}$ vale che $\mathbf{P}[y \mid x] = \mathbf{P}[y] > 0$. Quindi, esiste almeno una chiave $K \in \mathcal{K}$ tale che $y = e_K(x)$. Pertanto, fissato $x \in \mathcal{P}$, vale che

$$\mathcal{C} = \{e_K(x) : K \in \mathcal{K}\}.$$

Da ciò segue che $|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{P}|$.

□

3.3 Teorema di Shannon

Forniamo ora una caratterizzazione della perfetta sicurezza, dovuta originariamente a Shannon (1949), per i crittosistemi in cui vale $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Teorema 3.7. *Un crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, tale che $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$, fornisce segretezza perfetta se, e solo se, valgono i seguenti fatti:*

1. *Le chiavi sono equiprobabili con probabilità $1/|\mathcal{K}|$;*
2. *Per ogni $x \in \mathcal{P}$ e $y \in \mathcal{C}$ esiste un unica una chiave $K \in \mathcal{K}$ tale che $y = e_K(x)$.*

Dimostrazione. Supponiamo che valgano **(1)** e **(2)**. Allora segue che

$$\begin{aligned}
\mathbf{P}[\mathbf{y} = y] &= \sum_{\{K : y \in e_K(\mathcal{P})\}} \mathbf{P}[\mathbf{K} = K]\mathbf{P}[\mathbf{x} = d_K(y)] = \\
&= \sum_{K \in \mathcal{K}} \frac{1}{|\mathcal{K}|}\mathbf{P}[\mathbf{x} = d_K(y)] = \\
&= \frac{1}{|\mathcal{K}|} \sum_{K \in \mathcal{K}} \mathbf{P}[\mathbf{x} = d_K(y)].
\end{aligned}$$

Per **(2)** e per $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$ segue che $\{d_K(y) : K \in \mathcal{K}\} = \mathcal{P}$. Quindi,

$$\sum_{K \in \mathcal{K}} \mathbf{P}[\mathbf{x} = d_K(y)] = \sum_{x \in \mathcal{P}} \mathbf{P}[\mathbf{x} = x] = 1$$

e quindi $\mathbf{P}[\mathbf{y} = y] = 1/|\mathcal{K}|$. D'altra parte, **(1)** e **(2)** implicano

$$\mathbf{P}[\mathbf{y} = y \mid \mathbf{x} = x] = \mathbf{P}[\mathbf{K} = K] = \frac{1}{|\mathcal{K}|},$$

dove K è la chiave tale che $y = e_K(x)$. Pertanto,

$$\begin{aligned}
\mathbf{P}[\mathbf{x} = x \mid \mathbf{y} = y] &= \frac{\mathbf{P}[\mathbf{x} = x]\mathbf{P}[\mathbf{y} = y, \mathbf{x} = x]}{\mathbf{P}[\mathbf{y} = y]} = \\
&= \frac{\mathbf{P}[\mathbf{x} = x] \times \frac{1}{|\mathcal{K}|}}{\frac{1}{|\mathcal{K}|}} = \\
&= \mathbf{P}[\mathbf{x} = x]
\end{aligned}$$

che è la segretezza perfetta.

Supponiamo che il crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ fornisca segretezza perfetta. Fissato $x \in \mathcal{P}$, dal **Lemma 3.6** segue che per ogni $y \in \mathcal{C}$ esiste almeno un $K \in \mathcal{K}$ tale che $y = e_K(x)$. Allora

$$|\mathcal{C}| = |\{e_K(x) : K \in \mathcal{K}\}| \leq |\mathcal{K}|$$

e quindi $|\{e_K(x) : K \in \mathcal{K}\}| = |\mathcal{K}|$, essendo $|\mathcal{C}| = |\mathcal{K}|$.
Pertanto, per ogni $x \in \mathcal{P}$ e $y \in \mathcal{C}$ esiste un unica una chiave $K \in \mathcal{K}$ tale che $y = e_K(x)$. Abbiamo così provato che vale **(2)**.

Sia $n = |\mathcal{K}|$, allora $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$. Fissato $y \in \mathcal{C}$, indicizziamo gli elementi di $\mathcal{K}$ in modo tale che per ogni $1 \leq i \leq n$ risulti $e_{K_i}(x_i) = y$. Sfruttando l'ipotesi di segretezza perfetta e il **Teorema di Bayes** segue che

$$\mathbf{P}[\mathbf{x} = x_i] = \mathbf{P}[\mathbf{x} = x_i \mid \mathbf{y} = y] = \frac{\mathbf{P}[\mathbf{x} = x_i]\mathbf{P}[\mathbf{y} = y \mid \mathbf{x} = x_i]}{\mathbf{P}[\mathbf{y} = y]}.$$

Quindi

$$\mathbf{P}[\mathbf{y} = y \mid \mathbf{x} = x_i] = \mathbf{P}[\mathbf{y} = y].$$

Siccome K_i è l'unica chiave tale che $e_{K_i}(x_i) = y$, si ha

$$\mathbf{P}[\mathbf{y} = y \mid \mathbf{x} = x_i] = \mathbf{P}[\mathbf{K} = K_i].$$

Pertanto

$$\mathbf{P}[\mathbf{K} = K_i] = \mathbf{P}[\mathbf{y} = y].$$

Quindi le chiavi sono tutte equiprobabili con probabilità $\mathbf{P}[\mathbf{y} = y]$ con y fissato. Siccome le chiavi sono $|\mathcal{K}|$, segue **(1)**.

□

Corollario 3.8. *Se le* 26 *chiavi nel cifrario mediante spostamento sono equiprobabili, allora il cifrario mediante spostamento fornisce segretezza perfetta indipendentemente dalla distribuzione di probabilità del testo in chiaro.*

Dimostrazione. Segue dal **Teorema 3.7**, basta notare che $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ e che per ogni $x, y \in \mathbb{Z}_{26}$ vale che $K = y - x$ è l'unica chiave che realizza $y = e_K(x)$.

□

Corollario 3.9. *Se le* 26^m *chiavi nel cifrario di Vigènere sono equiprobabili e ogni chiave è utilizzata per cifrare una sola unità di messaggio in chiaro, allora il cifrario fornisce segretezza perfetta indipendentemente dalla distribuzione di probabilità del testo in chiaro.*

Dimostrazione. Segue dal **Teorema 3.7**, per le ipotesi fatte, siccome

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m.$$

□

Una ben nota realizzazione della segretezza perfetta è il cifrario One-time Pad, che fu costruito da Vernam nel 1917 nell'ambito della cifratura e decifratura dei messaggi telegrafici.

Figura 3.2: Gilbert Sandford Vernam (1890 – 1960)

Definizione 3.10. (Cifrario One-time Pad).
Sia $n \geq 1$ un intero, allora il crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ dove $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$ e dove, fissato $K \in \mathcal{K}$, per ogni $x \in \mathcal{P}$ e $y \in \mathcal{C}$ vale che $e_K(x) = x \oplus K$ e $d_K(y) = y \oplus K$.

Se le chiavi nel cifrario One-time pad sono equiprobabili e ogni chiave è utilizzata per cifrare una sola unità di messaggio in chiaro, allora il cifrario fornisce segretezza perfetta per il **Teorema 3.7**.

Limitazioni dei crittosistemi incondizionatamente sicuri:

- Poiché $|\mathcal{K}| \geq |\mathcal{P}|$, una notevole quantità di chiavi deve essere trasmessa attraverso un canale sicuro. Questa limitazione sarebbe relativa, se una chiave potesse essere utilizzata per cifrare più messaggi. Tuttavia la perfetta segretezza depende dal fatto che ogni chiave è utilizzata per una sola cifratura. Questo crea grossi problemi con la gestione delle chiavi.
- Nel caso del cifrario One-time pad è fondamentale che ogni chiave sia utilizzata per una sola cifratura, altrimenti sarebbe il cifrario sarebbe vulnerabile all'attacco basato sulla conoscenza del testo in chiaro. Infatti, $K = x \oplus e_K(x)$.

3.4 Cifrari Prodotto

Nel 1949 il noto matematico Claude Shannon nel suo **"Communication Theory of Secrecy Systems"**, propose di combinare due o più crittosistemi, attraverso il loro **prodotto**. Quest'operazione determina quindi un terzo sistema partendo da due crittosistemi dati. L'idea dei cifrari prodotto avrà un ruolo fondamentale nella creazione di alcuni tra i più moderni cifrari, come ad esempio l'**Advanced Encryption Standard**.

Definiamo ora nel dettaglio il crittosistema prodotto.

Definizione 3.11. (Crittosistema Prodotto).
Siano $\mathbb{S}_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ e $\mathbb{S}_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$, allora il prodotto di $\mathbb{S}_1$ e $\mathbb{S}_2$ è il crittosistema

$$\mathbb{S}_1 \times \mathbb{S}_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D}),$$

in cui le funzioni di cifratura e decifratura sono

$$e_{(K_1,K_2)} = e_{K_1} \circ e_{K_2}$$
$$d_{(K_1,K_2)} = d_{K_2} \circ d_{K_1},$$

dove (e_{K_1}, d_{K_1}), (e_{K_2}, d_{K_2}) sono le funzioni di cifratura e decifratura di $\mathbb{S}_1$ e $\mathbb{S}_2$, rispettivamente.

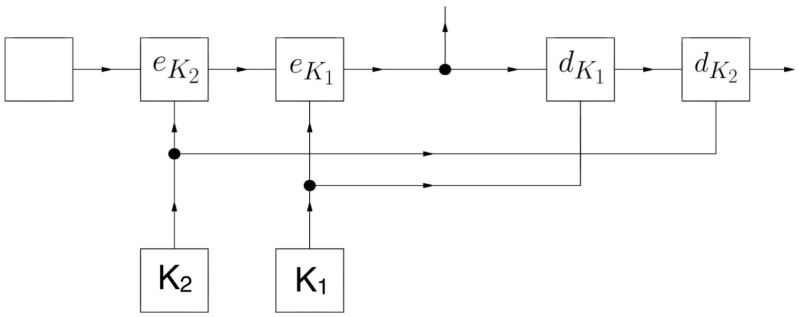

Figura 3.3: Prodotto di due sistemi $\mathbb{S}_1, \mathbb{S}_2$

Chiaramente, vale che $\mathbb{S}_1 \times \mathbb{S}_2 \neq \mathbb{S}_2 \times \mathbb{S}_1$. Qualora si verifichi che $\mathbb{S}_1 \times \mathbb{S}_2 = \mathbb{S}_2 \times \mathbb{S}_1$ allora si dice che $\mathbb{S}_1$ e $\mathbb{S}_2$ **commutano**.

Proponiamo ora un esempio di cifrario prodotto.
Sia $\mathbb{S}_1$ il cifrario moltiplicativo, quindi $e_a : x \mapsto ax \ mod\ 26$ con $\mathrm{mcd}(a, 26) = 1$, e $\mathbb{S}_2$ il cifrario mediante spostamento $e_b : x \mapsto x + b \ mod\ 26$. Allora il cifrario prodotto $\mathbb{S}_1 \times \mathbb{S}_2$ ha come insieme delle chiavi $\mathcal{K} = \{(a, b) : \mathrm{mcd}(a, 26) = 1\}$, e come funzione di cifratura e decifratura

$$e_{(a,b)} : x \mapsto ax + b \ mod\ 26 \qquad d_{(a,b)} : y \mapsto a^{-1}(y - b) \ mod\ 26.$$

Quindi, il cifrario prodotto del cifrario moltiplicativo e di quello mediante spostamento è affine. È facile vedere, inoltre, che il cifrario moltiplicativo e quello mediante spostamento commutano.

Un crittosistema endomorfo $\mathbb{S}$ si definisce **idempotente** se $\mathbb{S}^2 = \mathbb{S}$. In generale, la sicurezza del crittosistema $\mathbb{S}^n$ è incrementata solo quando **non** è idempotente.

Proposizione 3.12. Il cifrario di Vigenére è idempotente.

Dimostrazione. Sia $\mathbb{S}$ un cifrario di Vigenére, (K, K') una chiave di $\mathbb{S}^2$ e $(x_1, \ldots, x_n)$ una n-upla di un'unità di messaggio in chiaro.
Segue dalla definizione di cifrario prodotto che

$$\begin{aligned} e_{(K,K')}(x_1, \ldots, x_m) &= (e_{K'} \circ e_K)(x_1, \ldots, x_m) \\ &= e_{K'}(e_K(x_1, \ldots, x_m)) \\ &= e_{K'}(x_1 + k_1, \ldots, x_m + k_m) \\ &= ((x_1 + k_1) + k'_1, \ldots, (x_m + k_m) + k'_m) \\ &= (x_1 + (k_1 + k'_1), \ldots, x_m + (k_m + k'_m)) \\ &= e_{(K+K')}(x_1, \ldots, x_m). \end{aligned}$$

Pertanto $e_{(K,K')} = e_{K+K'}$ e in modo analogo si prova che $d_{(K,K')} = d_{K+K'}$. Quindi $\mathbb{S}^2 = \mathbb{S}$, che è l'asserto.

□

Lemma 3.13. *Siano $\mathbb{S}_1, \mathbb{S}_2$ due crittosistemi. Se $\mathbb{S}_1$ e $\mathbb{S}_2$ sono idempotenti e commutano, allora il loro prodotto è idempotente.*

Dimostrazione. Per dimostrarlo si sfrutta la proprietà associativa del prodotto. Quindi,

$$\begin{aligned} (\mathbb{S}_1 \times \mathbb{S}_2)^2 &= (\mathbb{S}_1 \times \mathbb{S}_2) \times (\mathbb{S}_1 \times \mathbb{S}_2) \\ &= \mathbb{S}_1 \times (\mathbb{S}_2 \times \mathbb{S}_1) \times \mathbb{S}_2 \\ &= (\mathbb{S}_1 \times \mathbb{S}_1) \times (\mathbb{S}_2 \times \mathbb{S}_2) \\ &= \mathbb{S}_1 \times \mathbb{S}_2. \end{aligned}$$

□

Un modo per costruire crittosistemi non idempotenti è quello di considerare il prodotto di crittosistemi semplici, eventualmente idempotenti, che non commutino.