Teoria dell'Informazione/RTI **Anno Accademico 2022–2023**

Lezione 14

Ugo Vaccaro

In questa lezione vedremo ulteriori applicazioni della Teoria dell'Informazione alla Crittografia. Tra gli strumenti più usati in Crittografia vi sono i cosiddetti Schemi per la Condivisione di Segreti. In uno schema per la condivisione di segreti vi è un Distributore che possiede un segreto, un insieme di partecipanti ed una collezione $\mathcal{A}$ di sottoinsiemi di partecipanti ($\mathcal{A}$ è chiamata la famiglia di *insiemi autorizzati*, o anche *struttura di accesso*). Uno schema di condivisione di segreti è un metodo attraverso il quale il Distributore distribuisce "informazioni" ai partecipanti in modo tale che le due seguenti condizioni siano soddisfatte:

1. Ogni sottoinsieme di partecipanti in $\mathcal{A}$ può ricostruire il segreto, a partire dalle informazioni ricevute dal Distributore.
2. Ogni sottoinsieme dei partecipanti non in $\mathcal{A}$ assolutamente *nulla* può ricostruire sul possibile segreto.

Oltre a trovare molteplici appliazioni in Crittografia, sistemi di condivisione di segreti astraggono molti problemi che si verificano in pratica. Ad esempio, immaginiamo la gestione dell'apertura di un caveau di una banca. In generale, non si può affidare la combinazione segreta (o la chiave) che permette l'apertura del caveau ad ogni impiegato, in quanto ciò permetterebbe a *ciascuno* di essi l'apertura del caveau, il che potrebbe essere fonte di ovvi problemi nel caso di impiegati disonesti. Si vorrebbe, quindi, progettare un sistema in cui solo l'inserimento simultaneo di due o più combinazioni può permettere l'apertura del caveau, ma nessun impiegato *da solo* debba avere idea di quale possa essere la combinazione per l'apertura. Questo problema può essere risolto mediante i sistemi di condivisione di segreti che studieremo. É da notare che un sistema simile sembra essere usato anche per la gestione dei codici di accesso per l'uso di armi nucleari. Secondo quanto riportato dalla rivista Time Magazine, per il lancio di armi nucleari russe è necessario che almeno due persone tra il Presidente russo, il Ministro della Difesa ed un funzionario del Ministero della Difesa inseriscano il loro codice di accesso, ma nessuno da solo ha la possibilità di dedurre quale potrebbe essere il codice che abilita siffatto lancio.

Stabiliamo un pò di terminologia che useremo in seguito.

Con $\mathcal{P} = \{p_1, \ldots, p_n\}$ denoteremo l'insieme dei partecipanti. Una collezione $\mathcal{A} = \{A : A \subseteq \mathcal{P}\}$ è detta *monotona* se $B \in \mathcal{A}$ e $C \supseteq B$ implica che $C \in \mathcal{A}$. Una *struttura di accesso* è una collezione monotona $\mathcal{A}$ di sottoinsiemi di $\mathcal{P}$. Gli insiemi in $\mathcal{A}$ sono detti insiemi di partecipanti *autorizzati*, gli insiemi non in $\mathcal{A}$ sono detti *non autorizzati*. Una *regola di distribuzione* è una funzione

$$f : \mathcal{P} = \{p_1, \ldots, p_n\} \mapsto \mathcal{S}$$

dove per ogni $p_i \in \mathcal{P}$ il valore $f(p_i)$ rappresenta l'informazione che viene assegnata al partecipante p_i. Tale informazione può essere di vario tipo, ad es., può essere un numero, un codice, etc.. Chiameremo $f(p_i)$ la *sequenza* assegnata al partecipante p_i. Denotiamo con $\mathcal{K}$ l'insieme dei possibili segreti che si intendono distribuire. Per ogni segreto $k \in \mathcal{K}$, sia $\mathcal{F}_k$ un associato insieme di regole di distribuzione. $\mathcal{F}_k$ sarà l'insieme delle regole di distribuzione che potranno essere utilizzate per distribuire sequenze ai partecipanti, *quando* il segreto da condividere sarà $k \in \mathcal{K}$. L'insieme delle regole di distribuzione $\mathcal{F}_k$ sono note a tutti. Ora, formiamo l'insieme

$$\mathcal{F} = \bigcup_{k \in \mathcal{K}} \mathcal{F}_k,$$

che corrisponde all'insieme di tutte le possibili regole di distribuzione. Se $k \in \mathcal{K}$ è il valore del segreto che il Distributore intende condividere con i partecipanti in $\mathcal{P}$, allora il Distributore sceglierà una regola di distribuzione $f \in \mathcal{F}_k$, ed userà f per assegnare sequenze ai partecipanti in $\mathcal{P}$. Assumiamo che i segreti in $\mathcal{K}$ vengano scelti in

accordo ad una distribuzione di probablilità $P_{\mathcal{K}} = \{P_{\mathcal{K}}(k) : k \in \mathcal{K}\}$ e che per ogni possibile valore del segreto $k \in \mathcal{K}$, il Distributore scelga la relativa regola di distribuzione $f \in \mathcal{F}_k$ in accordo ad una distribuzione di probabilità $P_{\mathcal{F}_k} = \{P_{\mathcal{F}_k}(f) : f \in \mathcal{F}_k\}$.

Date queste distribuzioni di probabilità, è semplice calcolare la distribuzione di probabilità sugli insiemi di sequenze che possono essere assegnate a ciascun sottoinsieme $B \subseteq \mathcal{P}$ di partecipanti. Per ogni possibile segreto $k \in \mathcal{K}$, la probabilità che vengano assegnate le informazioni $s_1, \ldots, s_n \in \mathcal{S}$ agli n partecipanti in $\mathcal{P}$, dato che il segreto da condividere sia k, sarà eguale a:

$$P(s_1, \ldots, s_n|k) = \sum_{f \in \mathcal{F}_k : f(p_1)=s_1, \ldots, f(p_n)=s_n} P_{\mathcal{F}_k}(f). \tag{1}$$

Inoltre, ogni $s_1, \ldots, s_n \in \mathcal{S}$ vale che

$$P(s_1, \ldots, s_n) = \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) P(s_1, \ldots, s_n|k) = \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \times \sum_{f \in \mathcal{F}_k : f(p_1)=s_1, \ldots, f(p_n)=s_n} P_{\mathcal{F}_k}(f). \tag{2}$$

La (2) rappresenta la probabilità congiunta che al partecipante p_1 venga assegnata la sequenza s_1, al partecipante p_2 venga assegnata la sequenza s_2, ..., al partecipante s_n venga assegnata la sequenza s_n. Se siamo interessati a calcolare la probabilità che un vettore di sequenze $(s_{i_1}, \ldots, s_{i_t})$ venga assegnato ai partecipanti di un sottoinsieme $B = \{p_{i_1}, \ldots, p_{i_t}\} \subseteq \mathcal{P}$, basterà usare la regola delle probabilità marginali, ovvero

$$P\{\text{a } p_{i_1} \text{ è assegnata } s_{i_1}, \ldots, \text{a } p_{i_t} \text{ è assegnata } s_{i_t}\} = \sum_{s_j \notin \{s_{i_1}, \ldots, s_{i_t}\}} P(s_1, \ldots, s_n).$$

Analogamente, ciò vale anche nel caso in cui siamo interessati a calcolare l'analoga probabilità condizionata dal fatto che il segreto è un dato $k \in \mathcal{K}$

$$P\{\text{a } p_{i_1} \text{ è assegnata } s_{i_1}, \ldots, \text{a } p_{i_t} \text{ è assegnata } s_{i_t}|k\} = \sum_{s_j \notin \{s_{i_1}, \ldots, s_{i_t}\}} P(s_1, \ldots, s_n|k).$$

Denotiamo con $\mathbf{K}$ la variabile casuale che assume come valori in segreti $k \in \mathcal{K}$ in accordo alla distribuzione di probabilità $P_{\mathcal{K}}$, e per ogni sottoinsieme $B = \{p_{i_1}, \ldots, p_{i_t}\} \subseteq \mathcal{P}$ di partecipanti denotiamo con $\mathbf{B}$ la variabile casuale che assume come valori i vettori di sequenze assegnati ai partecipanti in B, in accordo alle probabilità calcolate prima. Sarà possibile calcolare le probabilità condizionate, per ogni $k \in \mathcal{K}$ e per ogni

$$(s_{i_1}, \ldots, s_{i_t}) \in \underbrace{\mathcal{S} \times \ldots \times \mathcal{S}}_{t \text{ volte}}$$

mediante la formula

$$P\{\mathbf{K} = k|\mathbf{B} = (s_{i_1}, \ldots, s_{i_t})\} = \frac{P\{\mathbf{B} = (s_{i_1}, \ldots, s_{i_t})|\mathbf{K} = k\} P_{\mathcal{K}}(k)}{P\{\mathbf{B} = (s_{i_1}, \ldots, s_{i_t})\}}.$$

Possiamo quindi definire formalmente le proprietà che richieremo ad un Schema di Condivisione di Segreti.

Correttezza. *Per ogni insieme di partecipanti autorizzati $B = \{p_{i_1}, \ldots, p_{i_t}\} \in \mathcal{A}$, per ogni segreto $k \in \mathcal{K}$ e per ogni regola di distribuzione $f \in \mathcal{F}_k$ deve valere che*

$$P\{\mathbf{K} = k'|\mathbf{B} = (f(p_{i_1}), \ldots, f(p_{i_t}))\} = \begin{cases} 1 & \textit{se } k' = k \\ 0 & \textit{altrimenti} \end{cases} \tag{3}$$

Sicurezza. *Per ogni insieme di partecipanti non autorizzati* $A = \{p_{i_1}, \ldots, p_{i_s}\} \notin \mathcal{A}$, *per ogni segreto* $k \in \mathcal{K}$ *e per ogni regola di distribuzione* $f \in \mathcal{F}_k$ *deve valere che*

$$P\{\mathbf{K} = k | \mathbf{A} = (f(p_{i_1}), \ldots, f(p_{i_s}))\} = P\{\mathbf{K} = k\} = P_{\mathcal{K}}(k). \tag{4}$$

Il senso di queste due proprietà è ovvio. La proprietà di Correttezza essenzialmente afferma che i partecipanti di ogni insieme qualificato possono risalire in maniera univoca al segreto, a partire dalle sequenze ricevute dal Distributore. La proprietà di Sicurezza afferma che ogni insieme di partecipanti non qualificato non ha alcuna possibilità di dedurre alcunchè sul segreto, a partire dalle sequenze che il Distributore ha a loro assegnato.

Vediamo uno dei più importanti algoritmi di schemi di condivisione di segreti, detto Schema di Shamir, dal nome dello scopritore. In questo caso la struttura di accesso $\mathcal{A}$ è di questa forma

$$\mathcal{A} = \big\{A : A \subseteq \{p_1, \ldots, p_n\}, |A| \geq t\big\},$$

dove t è un intero fissato compreso tra 1 ed n. In altri termini, scelto un arbitrario segreto $k \in \mathcal{K}$, intendiamo distribuire "informazione" a ciascun partecipante $p \in \mathcal{P}$ in modo tale che *ogni* sottoinsieme composto da t o più persone possa ricostruire il segreto k, mentre *ogni* sottoinsieme di al più $t-1$ persone *assolutamente nulla* possa dedurre su k. Nello Schema di Shamir si suppone che l'insieme dei segreti sia $\mathcal{K} = \mathbb{F}_q$ =campo finito con q elementi, dove $q > n$ è una qualche potenza di numero primo. Siano $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ elementi distinti e diversi da 0, noti a tutti i partecipanti. Per ogni fissato possibile segreto $k \in \mathbb{F}_q$, l'insieme $\mathcal{F}_k$ delle possibili regole di distribuzione associate al segreto k è così definito:

$$\mathcal{F}_k = \{P(x) = k + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} : a_1, a_2, \ldots, a_{t-1} \in \mathbb{F}_q\}.$$

In altri termini, $\mathcal{F}_k$ consiste di *tutti* i possibili polinomi $P(x)$ di grado al più $t-1$, ed a coefficienti su $\mathbb{F}_q$, per cui vale che $P(0) = k$. Una volta aver scelto il segreto k ed una regola di distribuzione in $\mathcal{F}_k$, a caso ed equiprobabilmente, il Distributore assegnerà al generico partecipante $p_j \in \mathcal{P}$, $j = 1, \ldots, n$, il valore $P(\alpha_j) = s_j$ del polinomio $P(x)$ nel punto α_j, dove si intende che tutte le valutazioni vengono effettuate in accordo all'aritmetica del campo $\mathbb{F}_q$.

La correttezza e la sicurezza dello schema di Shamir si basano sul ben noto Teorema di Interpolazione di Lagrange, secondo il quale in ogni campo $\mathbb{F}$, e per ogni sequenza $(x_1, y_1), \ldots, (x_t, y_t)$, con $x_i, y_i \in \mathbb{F}$ per $i = 1, \ldots, t$ e $x_i \neq x_j$ per $i \neq j$, esiste un *unico* polinomio Q di grado al più $t-1$ con coefficienti in $\mathbb{F}$ tale che $Q(x_j) = y_j$, per $j = 1, \ldots, t$.

Proviamo innanzitutto la correttezza dello schema di Shamir. Consideriamo un generico insieme di partecipanti $B = \{p_{i_1}, \ldots, p_{i_s}\}$, con $s \geq t$. Essendo la cardinalità di B maggiore o uguale a t, B è un insieme autorizzato e quindi i partecipanti in B dovrebbero essere in grado di risalire al segreto k dalla conoscenza di tutti i valori che il Distributore ha dato loro. Ed infatti è così. Presi t valori arbitrari $s_{i_1}, \ldots, s_{i_t}$ tra quelli in loro possesso, i partecipanti in B possono innanzitutto calcolare il polinomio

$$Q(x) = \sum_{\ell=1}^{t} s_{i_\ell} \prod_{1 \leq j \leq t,\, j \neq \ell} \frac{\alpha_{i_j} - x}{\alpha_{i_j} - \alpha_{i_\ell}} \tag{5}$$

É semplice osservare che $Q(\alpha_{i_\ell}) = s_{i_\ell} = P(\alpha_{i_\ell})$, per ogni $\ell = 1, \ldots, t$. Pertanto, i polinomi Q e P sono entrambi polinomi di grado al più $t-1$ che coincidono su t valori. Dal Teorema di Interpolazione di Lagrange, essi sono uguali ed in particolare $Q(0) = P(0) = k$. Ne segue che i partecipanti in B possono ricostruire il segreto k semplicemente calcolando

$$Q(0) = \sum_{\ell=1}^{t} s_{i_\ell} \prod_{1 \leq j \leq t,\, j \neq \ell} \frac{\alpha_{i_j}}{\alpha_{i_j} - \alpha_{i_\ell}}.$$

Per provare la proprietà di Sicurezza, consideriamo un generico insieme $A = \{p_{i_1}, \ldots, p_{i_r}\}$ di partecipanti non autorizzato, di cardinalità quindi $r \leq t-1$. Dal Teorema di Interpolazione di Lagrange, *per ogni* possibile valore

del segreto $k \in \mathbb{F}_q$, esiste un polinomio Q di grado al più r che $Q(0) = k$ e $Q(\alpha_{i_j}) = s_{i_j}$, per $j = 1, \ldots, r$. Ciò lo si può anche osservare direttamente scrivendo il sistema di equazioni che i coefficienti del polinomio incognito $P(x) \in \mathcal{F}_k$ deve soddisfare, e notare che per ogni possibile valore di $k \in \mathbb{F}_q$, esiste un polinomio Q di grado al più r che $Q(0) = k$ e $Q(\alpha_{i_j}) = s_{i_j}$, per $j = 1, \ldots, r$. Pertanto, i partecipanti in A dalle informazioni in loro possesso non possono escludere alcun elemento in $\mathbb{F}_q$ come possibile segreto, quindi la proprietà di Sicurezza è garantita.

Una misura della bontà di uno schema di condivisione di segreti consiste nella quantità di informazione "privata" che lo schema distribuisce a ciascun partecipante $p \in \mathcal{P}$ (ovvero la $f(p)$, se f è la regla di distribuzione usata). Per motivi pratici, sarebbe opportuno che tale quantità di informazione sia la minore possibile. Ad esempio, se tale informazione fosse considerevole, allora i partecipanti sarebbero tentati di memorizzarla su supporti fisici (che potrebbero essere letti da malintenzionati) mentre se tale informazione fosse una stringa alfanumerica corta, allora ogni partecipante potrebbe ricordarla a memoria, e quindi non essere soggetti a furti di informazione. Nello Schema di Distribuzione di segreti di Shamir ogni partecipante riceve come informazione un elemento dello stesso campo $\mathbb{F}_q$ cui appartiene il segreto. In altri termini, la sequenza che ogni partecipante deve ricordare è "grande" quanto la sequenza che rappresenta il segreto (esprimendo il tutto in binario, ad esempio). É naturale chiedersi se si possa far di meglio, ovvero progettare sistemi di condivisione di segreti in cui l'informazione distribuita a ciascun partecipante sia rappresentabile mediante una sequenza "più corta" di quella che rappresenta il segreto. Per scoprire se ciò è possibile o meno, riformuliamo le proprietà di Correttezza e Sicurezza in termini Teorico-Informazionali. É evidente che le due proprietà possono essere così riformulate:

Correttezza. *Per ogni insieme di partecipanti autorizzati $B \in \mathcal{A}$, vale che $H(\mathbf{K}|\mathbf{B}) = 0$.*

Sicurezza. *Per ogni insieme di partecipanti non autorizzati $A \notin \mathcal{A}$, vale che $H(\mathbf{K}|\mathbf{A}) = H(\mathbf{K})$.*

Sia $\mathcal{A}$ una generica struttura d'accesso per i partecipanti $\mathcal{P}$. Da questo punto in poi, lavoriamo sotto l'ipotesi che per ogni partecipante $p \in \mathcal{P}$, esiste un sottoinsieme $A \subset \mathcal{P}$ (eventualmente, anche uguale all'insieme vuoto) tale che $A \notin \mathcal{A}$ ma $A \cup \{p\} \in \mathcal{A}$. Infatti, se $\forall A \subseteq \mathcal{P}$ per cui $A \notin \mathcal{A}$ vale anche che $A \cup \{p\} \notin \mathcal{A}$, vorrebbe dire che il partecipante p da solo non appartiene alla struttura ad accesso. Infatti, evidentemente $\emptyset \notin \mathcal{A}$ e $\emptyset \cup \{p\} = \{p\} \notin \mathcal{A}$. Quindi, p potrebbe eventualmente ricostruire il segreto *solo* con insiemi $A \in \mathcal{A}$, ovvero con insiemi che già senza il contributo di p potrebbero ricostruire il segreto. Detto in altri termini, il ruolo di p nella ricostruzione del segreto sarebbe nullo, e quindi teoricamente gli si può anche non assegnargli niente nella fase di distribuzione. Ricordiamo che denotiamo con $\mathbf{K}$ la variabile casuale che assume come valori i segreti $k \in \mathcal{K}$ in accordo alla distribuzione di probabilità $P_{\mathcal{K}}$, e per ogni sottoinsieme $B = \{p_{i_1}, \ldots, p_{i_t}\} \subseteq \mathcal{P}$ di partecipanti denotiamo con $\mathbf{B}$ la variabile casuale che assume come valori i vettori di sequenze assegnati ai partecipanti in B.

Teorema 1 *Dato un generico partecipante p in uno schema di condivisione di segreti corretto e sicuro, sia $\mathbf{p}$ la variabile casuale che assume come valori le possibili sequenze assegnate al partecipante p. Vale*

$$H(\mathbf{p}) \geq H(\mathbf{K}).$$

Dimostrazione. Dato $p \in \mathcal{P}$, sia $A \subset \mathcal{P}$ tale che $A \notin \mathcal{A}$ ma $A \cup \{p\} \in \mathcal{A}$. Dalla Proprietà di Correttezza sappiamo che $H(\mathbf{K}|\mathbf{Ap}) = 0$, e dalla Proprietà di Sicurezza sappiamo che $H(\mathbf{K}|\mathbf{A}) = H(\mathbf{K})$. Pertanto

$$\begin{aligned} H(\mathbf{Kp}|\mathbf{A}) &= H(\mathbf{K}|\mathbf{A}) + H(\mathbf{p}|\mathbf{AK}) \\ &= H(\mathbf{K}) + H(\mathbf{p}|\mathbf{AK}) \\ &= H(\mathbf{p}|\mathbf{A}) + H(\mathbf{K}|\mathbf{Ap}) \\ &= H(\mathbf{p}|\mathbf{A}), \end{aligned}$$

da cui

$$H(\mathbf{p}) \geq H(\mathbf{p}|\mathbf{A}) = H(\mathbf{K}) + H(\mathbf{p}|\mathbf{AK}) \geq H(\mathbf{K}).$$

□

Poichè il Teorema 1 deve valere *qualunque* sia la distribuzione di probabilità sui segreti, deve valere anche quando la distribuzione è quella equiprobabile, nel cui caso otteniamo che

$$\log(\#\text{possibili sequenze assegnate a } p) \geq H(\mathbf{p}) \geq H(\mathbf{K}) = \log(\#\text{possibili segreti}),$$

e quindi la dimensione delle sequenze assegnate a qualsiasi partecipante p devono essere almeno pari alla dimensione del segreto (misurate in numero di bits). Ne segue che lo schema di Shamir è ottimale da questo punto di vista.