Sicurezza su Reti **Anno Acc. 1997-98**

PROF. ALFREDO DE SANTIS

Schemi di condivisione di segreti

a cura di Di Leo Letizia, Iuzzolino Vita e Licciardi Maria *17 Luglio 1998*

Indice

1 Introduzione **2**

2 Definizione di uno schema a soglia (k, n) **2**

2.1 Schema a soglia (k, n) di Shamir 3

2.1.1 Metodi per il calcolo del segreto 4

2.2 Schema a soglia (n, n) 8

3 Struttura d'accesso **9**

3.1 Tasso di informazione 11

3.2 Definizione formale 12

3.2.1 Definizione probabilistica di SSS 13

3.3 Un limite all'entropia sul tasso di informazione 15

4 Costruzione per decomposizione **15**

1 Introduzione

Il problema principale che si vuole trattare è la costruzione di uno schema di condivisione di segreti, atto a garantire la massima sicurezza per quanto riguarda l'accesso a particolari strutture. Consideriamo il caso di una banca in cui lavorano tre cassieri e nella quale si trovi una cassaforte. Ad essa è associata una combinazione segreta che ne permette l'apertura.
Il principale per sicurezza non affida la combinazione della cassaforte ad uno solo di essi, ma ne assegna un pezzo a ciascuno, in maniera tale che se due di essi uniscono i loro pezzi di informazione riescono a ricavare la combinazione per aprire la cassaforte (regola del "due-su-tre").
In questo caso si è realizzato un sistema di condivisione di segreti, dove il segreto è la combinazione della cassaforte. Assegnando ad ogni cassiere un pezzo di combinazione, si evita il tentativo da parte di uno di essi di prelevare indebitamente denaro. Se invece due cassieri si mettono d'accordo, riescono nel loro intento.
Un altro esempio di condivisione di segreti si riscontra nel controllo dei missili nucleari in Russia, dove i codici segreti sono ripartiti tra tre partecipanti (presidente, ministro della difesa e ministero della difesa). Anche in tale ambito vige la regola del "due-su-tre", infatti se si uniscono due dei tre partecipanti riescono ad ottenere i codici segreti, mentre uno singolarmente non vi riesce.
Il metodo di distribuire un'informazione importante tra più individui è più sicuro rispetto a quello di nasconderla in una o più cassaforti o di memorizzarla in un computer, perchè potrebbero presentarsi problemi di furto o di breakdown.
Nei prossimi paragrafi si definirà un particolare schema di condivisione di segreti, il cosiddetto "threshold scheme" [5] (schema a soglia).

2 Definizione di uno schema a soglia (k, n)

Siano k, n interi positivi tali che $k \leq n$. Uno schema a soglia (k, n) è un metodo di condivisione di un segreto S tra un insieme di n partecipanti, tali che:

1. Ogni gruppo di partecipanti di cardinalità $\geq k$ riesce a recuperare il segreto S.

2. Ogni gruppo di partecipanti di cardinalità $\leq k-1$ non riesce a recuperare alcuna informazione riguardante il segreto S.

L'esempio della Russia per il controllo dei missili è uno schema a soglia (2,3). Il valore di S è scelto da un partecipante speciale chiamato "dealer".
Il dealer è denotato con D e si assume che D non appartiene a P che è l'insieme dei partecipanti, dove $P = \{P_i : 1 \leq i \leq n\}$. Quando D vuole distribuire il segreto S fra i partecipanti in P, assegna ad ogni partecipante delle informazioni parziali, dette *share*. Le share vengono distribuite segretamente, in modo che nessun partecipante conosce le share date agli altri partecipanti. Per chiarire il concetto, consideriamo un sottoinsieme di partecipanti B di P, che uniscono le loro share per cercare di ricavare il segreto. (Alternativamente, essi potrebbero dare le loro share ad una Trusted Autority (TA), che cerca di calcolare il segreto per essi.) Se $|B| \geq k$, allora essi riusciranno a calcolare il segreto S in funzione delle loro share; se $|B| < k$ allora non riusciranno a calcolare alcuna informazione sul segreto S.
Gli schemi a soglia sono stati inventati indipendentemente da Blakley [4] e da Shamir [5]

Un metodo per costruire uno schema a soglia (k, n) è quello presentato da Shamir nel 1979, chiamato appunto schema a soglia di Shamir.

2.1 Schema a soglia (k, n) di Shamir

Sia $\mathbf{S}$ l'insieme dei segreti (ovvero l'insieme di tutti i possibili segreti), Sh l'insieme delle share (ovvero l'insieme di tutte le possibili share), n il numero dei partecipanti. Sia inoltre, $\mathbf{S} = Sh = Z_p$, dove $p > n$ è un numero primo, ed S il segreto da condividere. I passi dell'algoritmo di distribuzione delle share del Dealer D sono descritti nella figura seguente.

FASE INIZIALIZZAZIONE

1. D sceglie n elementi distinti e non nulli di Z_p

$$x_1, \cdots, x_n$$

e distribuisce i valori x_i a P_i per $1 \leq i \leq n$.
I valori x_i sono pubblici.

DISTRIBUZIONE DELLE SHARE

2. Supponiamo che D vuole condividere il segreto S appartenente a Z_p, allora D sceglie a caso (uniformemente ed indipendentemente) $k - 1$ elementi di Z_p

$$a_1, \cdots, a_{k-1}$$

e costruisce il polinomio di grado $k - 1$

$$a(x) = S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

3. Per $i = 1, \cdots, n$ il dealer D calcola

$$y_i = a(x_i)$$

4. Per $1 \leq i \leq n$ distribuisce la share y_i a P_i.
Il valore y_i è noto solo a P_i.

Schema a soglia (k, n) di Shamir

Quindi in questo schema, il dealer costruisce un polinomio casuale $a(x)$ di grado al più $k - 1$, in cui il termine costante è proprio il segreto, ovvero $a(0) = S$. Alla fine ogni partecipante P_i ha la share (x_i, y_i), che rappresenta un punto del polinomio.

2.1.1 Metodi per il calcolo del segreto

Vediamo come un sottoinsieme di k partecipanti può ricostruire la chiave.
Esistono due metodi per ricavare il segreto S, uno basato sulla risoluzione di sistemi di equazioni lineari, l'altro basato sul concetto di interpolazione polinomiale.

Primo metodo Supponiamo che $P_{i_1}, \cdots, P_{i_k}$ uniscano le loro share per determinare S.
Sappiamo che $y_{i_j} = a(x_{i_j})$ per $1 \leq j \leq k$, dove $a(x)$ è il polinomio segreto a coefficienti in Z_p scelto dal dealer.
Poichè $a(x)$ ha grado $\leq k-1$ può essere scritto come segue:

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

dove $a_1, \cdots, a_{k-1}$ sono elementi incogniti in Z_p e $a_0 = S$ è il segreto.
Poichè $y_{i_j} = a(x_{i_j})$ per $1 \leq j \leq k$, i partecipanti ottengono un sistema di k equazioni in k incognite $a_0, \cdots, a_{k-1} \in Z_p$. Se le equazioni sono linearmente indipendenti, esisterà un'unica soluzione ed il valore di a_0 rappresenterà il segreto.
Il sistema delle equazioni lineari è il seguente:

$$\begin{cases} a_0 & + & a_1 x_{i_1} & + & \cdots & + & a_{k-1} x_{i_1}^{k-1} & = & y_{i_1} \\ a_0 & + & a_1 x_{i_2} & + & \cdots & + & a_{k-1} x_{i_2}^{k-1} & = & y_{i_2} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_0 & + & a_1 x_{i_k} & + & \cdots & + & a_{k-1} x_{i_k}^{k-1} & = & y_{i_k} \end{cases}$$

Esso può essere scritto in forma matriciale come segue:

$$\begin{pmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{k-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{k-1} \\ \vdots & \vdots & & & \vdots \\ 1 & x_{i_k} & x_{i_k}^2 & \cdots & x_{i_k}^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_k} \end{pmatrix}$$

Sia A la matrice $k \times k$ costruita. Essa è una matrice di Vandermonde. Il determinante di tale matrice è:

$$\det(\mathrm{A}) = \prod_{1 \leq j \leq t \leq k} (x_{i_t} - x_{i_j}) \bmod p.$$

Ricordiamo che essendo tutte le x_i distinte, ogni termine $(x_{i_t} - x_{i_j}) \neq 0$. Il prodotto è calcolato in Z_p, che è un campo per cui il prodotto di termini diversi da zero è non zero e quindi $det(A) \neq 0$. Essendo il determinante della matrice diverso da zero, il sistema ammette sempre un'unica soluzione. Questo dimostra che in uno schema a soglia, un gruppo di k partecipanti riuscirà a determinare il segreto S.
Vediamo cosa succede se un gruppo di $k-1$ partecipanti $P_{i_1}, \cdots, P_{i_{k-1}}$ si unisce nel tentativo di ricavare il segreto condiviso.
Procedendo come prima, si otterrà un sistema di $k-1$ equazioni in k incognite

$$a_0, \cdots, a_{k-1} \in Z_p.$$

Il sistema delle equazioni lineari è il seguente:

$$\begin{cases} a_0 & + & a_1 x_{i_1} & + & \cdots & + & a_{k-1} x_{i_1}^{k-1} & = & y_{i_1} \\ a_0 & + & a_1 x_{i_2} & + & \cdots & + & a_{k-1} x_{i_2}^{k-1} & = & y_{i_2} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_0 & + & a_1 x_{i_{k-1}} & + & \cdots & + & a_{k-1} x_{i_{k-1}}^{k-1} & = & y_{i_{k-1}} \end{cases} \tag{1}$$

Poiché per ogni polinomio i termini $a_1, \cdots, a_{k-1}$ sono scelti dal dealer in modo casuale e solo a lui noti, segue che i $k-1$ partecipanti non riescono a valutare il valore y_0.
Supponiamo che essi ipotizzino un valore y_0. Poichè il segreto è il termine costante del polinomio $a(x)$, ovvero $S = a(0)$, si pone $y_0 = a(0)$.
Sia $a_{y_0}(x)$ il polinomio $a(x)$ il cui termine noto è y_0. Quindi $y_0 = a_{y_0}(0)$ rappresenta la k-esima equazione del sistema. Il risultante sistema è dato dalla (1) e dalla

$$y_0 = a_{y_0}(0).$$

In tal modo la matrice dei coefficienti del risultante sistema di k equazioni in k incognite, sarà ancora una matrice di Vandermonde. Anche in tale caso il sistema ammette un'unica soluzione.
Ricordiamo che per ogni segreto esiste un unico polinomio, poichè il dealer sceglie per ogni segreto un'unica sequenza casuale di $k-1$ elementi $a_1, \cdots, a_{k-1}$.
Pertanto, ogni ipotizzato valore y_0 del segreto è equiprobabile e nessun valore del segreto può essere scartato, quindi $k-1$ partecipanti non possono ricavare alcuna informazione circa il segreto.

Esempio 1 *Supponiamo che $p = 17$, $k = 3$ e $n = 5$.*
I valori pubblici dei partecipanti sono $x_i = i$ per $1 \leq i \leq 5$.
Supponiamo che il dealer ha assegnato a P_1, P_2, P_3, P_4 e P_5 le seguenti share:

$P_1 \leftarrow 8 = a(1)$

$P_2 \leftarrow 4 = a(2)$

$P_3 \leftarrow 10 = a(3)$

$P_4 \leftarrow 0 = a(4)$

$P_5 \leftarrow 11 = a(5)$
Supponiamo che P_1, P_3 e P_5 vogliono ricavare il segreto condiviso fra i cinque partecipanti. Il polinomio calcolato dal dealer D di grado al più due è il seguente:

$$a(x) = a_0 + a_1 x + a_2 x^2.$$

Dati a(1), a(3) e a(5), essi ottengono le seguenti tre equazioni lineari in tre incognite in Z_{17} :

$$\begin{array}{ccccc} a_0 & + & a_1 & + & a_2 = 8 \\ a_0 & + & 3a_1 & + & 9a_2 = 10 \\ a_0 & + & 5a_1 & + & 8a_2 = 11 \end{array}$$

Tale sistema ammette un'unica soluzione in Z_{17}:

$$a_0 = 13,\ a_1 = 10 \ e \ a_2 = 2.$$

Il segreto condiviso è quindi $S = a_0 = 13$.

Lo schema di Shamir è stato analizzato in relazione alla risoluzione di sistemi di equazioni lineari in Z_p, ma esiste un altro metodo basato sulla formula di interpolazione di Lagrange ([3], pp. 738-739).

Secondo metodo L'interpolazione polinomiale è una tecnica che permette di risolvere il problema della rappresentazione di funzioni che presentano un andamento non regolare.
Mediante l'interpolazione polinomiale di Lagrange, un gruppo di k partecipanti può calcolare $a(x)$ e quindi da esso estrarre il segreto. La formula di interpolazione di Lagrange è una formula esplicita, che dati i punti (x_{i_j}, y_{i_j}) (la share di ogni partecipante), con $1 \leq i \leq n$ e $1 \leq j \leq k$, permette di rappresentare l'unico polinomio $a(x)$ di grado al piú k, precedentemente calcolato dal dealer.
La formula è la seguente :

$$a(x) = \sum_{j=1}^{k} y_{i_j} \prod_{1 \leq t \leq k, t \neq j} \frac{x - x_{i_t}}{x_{i_j} - x_{i_t}}.$$

È facile verificare la correttezza di questa formula mediante la sostituzione $x = x_{i_\ell}$ con $1 \leq \ell \leq k$. In questo modo tutti i termini della sommatoria si annullano eccetto il termine ℓ-esimo, il quale è

$$y_{i_\ell}.$$

Da questa verifica si deduce che abbiamo un polinomio di grado al più $k-1$, $y_{i_j} = a(x_{i_j})$ contenente k coppie ordinate (x_{i_j}, y_{i_j}), per $1 \leq j \leq k$.
Avendo dimostrato che il polinomio costruito è unico, possiamo concludere asserendo che il metodo di interpolazione ci permette di calcolare il polinomio.
Vediamo un esempio che chiarisce quanto detto.

Esempio 2 *Sia k=3, sviluppando la formula, otteniamo:*

$$a(x) = \sum_{j=1}^{3} y_{i_j} \prod_{1 \leq t \leq 3, t \neq j} \frac{x - x_{i_t}}{x_{i_j} - x_{i_t}} =$$

$$= y_{i_1} \left(\frac{x - x_{i_2}}{x_{i_1} - x_{i_2}} \right) \left(\frac{x - x_{i_3}}{x_{i_1} - x_{i_3}} \right) + y_{i_2} \left(\frac{x - x_{i_1}}{x_{i_2} - x_{i_1}} \right) \left(\frac{x - x_{i_3}}{x_{i_2} - x_{i_3}} \right) + y_{i_3} \left(\frac{x - x_{i_1}}{x_{i_3} - x_{i_1}} \right) \left(\frac{x - x_{i_2}}{x_{i_3} - x_{i_2}} \right).$$

Se fissiamo $x = x_{i_1}$ otteniamo:

$$y_{i_1} \left(\frac{x_{i_1} - x_{i_2}}{x_{i_1} - x_{i_2}} \right) \left(\frac{x_{i_1} - x_{i_3}}{x_{i_1} - x_{i_3}} \right) + y_{i_2} \left(\frac{x_{i_1} - x_{i_1}}{x_{i_2} - x_{i_1}} \right) \left(\frac{x_{i_1} - x_{i_3}}{x_{i_2} - x_{i_3}} \right) + y_{i_3} \left(\frac{x_{i_1} - x_{i_1}}{x_{i_3} - x_{i_1}} \right) \left(\frac{x_{i_1} - x_{i_2}}{x_{i_3} - x_{i_2}} \right) = y_{i_1}.$$

Quindi

$$a(x_{i_1}) = y_{i_1}.$$

Il metodo descritto può essere semplificato, in quanto i k partecipanti per calcolare il segreto non hanno bisogno di conoscere tutto il polinomio $a(x)$, ma è sufficiente conoscere soltanto il termine costante $S = a(0)$.
Il segreto S può essere calcolato mediante la seguente espressione, ottenuta sostituendo $x = 0$ nella formula di interpolazione di Lagrange:

$$S = \sum_{j=1}^{k} y_{i_j} \prod_{1 \leq t \leq k, t \neq j} \frac{x_{i_t}}{x_{i_t} - x_{i_j}}.$$

Ponendo

$$b_j = \prod_{1 \leq t \leq k, t \neq j} \frac{x_{i_t}}{x_{i_t} - x_{i_j}}$$

per $1 \leq j \leq k$ si ottiene

$$S = \sum_{j=1}^{k} b_j y_{i_j}$$

che è una combinazione lineare di k share.

Notare che i valori b_j possono essere precomputati ed inoltre il loro valore non è segreto.

Esempio 3 *Riprendiamo l'Esempio 1. I partecipanti* $\{P_1, P_3, P_5\}$ *possono calcolare* $\{b_1, b_2, b_3\}$ *mediante la formula*

$$b_j = \prod_{1 \leq t \leq k, t \neq j} \frac{x_{i_t}}{x_{i_t} - x_{i_j}}.$$

Si ottiene

$$b_1 = \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} \bmod 17 = 3 \times 5 \times (-2)^{-1} \times (-4)^{-1} \bmod 17 = 4.$$

Allo stesso modo, si ottiene

$$b_2 = 3 \text{ e } b_3 = 11.$$

Allora assegnate le share 8, 10 e 11 (rispettivamente) si ottiene

$$S = 4 \times 8 + 3 \times 10 + 11 \times 11 \bmod 17 = 13.$$

2.2 Schema a soglia (n, n)

Tale schema è un caso speciale di schema a soglia in cui $k = n$. Esso è stato presentato da Karnin, Greene ed Hellman [7].
Si assume di considerare i segreti e le share in Z_m, ovvero $\mathbf{S} = Sh = Z_m$, dove Sh è l'insieme delle share. In questo schema non è richiesto che m sia primo e non è necessario che sia

$m \geq n+1$.
Se il Dealer vuole condividere il segreto S$\in Z_m$, esegue le seguenti operazioni:

1. D sceglie segretamente (in maniera indipendente e casuale) $n-1$ elementi di Z_m
$$y_1, \cdots, y_{n-1}$$
2. D calcola $y_n = S - \sum_{i=1}^{n-1} y_i \bmod m$
3. Per $1 \leq i \leq n$, D assegna la share y_i a P_i. (Il valore y_i è noto solo a P_i).

Schema a soglia (n, n) in Z_m

Si osserva che se si uniscono n partecipanti possono calcolare il segreto S mediante la seguente formula:

$$S = \sum_{i=1}^{n} y_i \bmod m.$$

Se invece si uniscono $n-1$ partecipanti non possono calcolare il segreto, perchè ricevono $n-1$ elementi indipendenti appartenenti a Z_m come loro share. Consideriamo $n-1$ partecipanti appartenenti all'insieme $P - \{P_i\}$, per $1 \leq i \leq n-1$. Questi $n-1$ partecipanti posseggono le share

$$y_1, \cdots, y_{i-1}, y_{i+1}, \cdots, y_{n-1}$$

e

$$y_n = S - \sum_{i=1}^{n-1} y_i$$

da cui

$$S = y_n + \sum_{i=1}^{n-1} y_i.$$

Poichè un partecipante P_i, per $1 \leq i \leq n$, non partecipa al calcolo del segreto, si otterrà non S, ma il valore $S - y_i$. Quindi $n-1$ partecipanti, sommando le loro share, calcolano il valore $S - y_i$, ma poichè y_i è un valore scelto a caso, essi non ottengono nessuna informazione sul valore di S. Conseguentemente, si ha un schema a soglia (n, n).

Esempio 4 *Sia $P = \{P_1, P_2\}$ e sia $\mathbf{S} = \{0, 1\}$.*
Supponiamo che il segreto $S = a \oplus b$, dove $a, b \in \mathbf{S}$.
Se si vuole condividere il segreto S, allora il dealer potrebbe effettuare le seguenti assegnazioni:

$P_1 \leftarrow a$
$P_2 \leftarrow b$

Se $S = 0$ viene assegnato ai due partecipanti lo stesso valore, cioè (0,0) oppure (1,1), invece se $S = 1$ le loro share devono essere diverse (0,1) oppure (1,0). Il segreto S viene recuperato solo se P_1 e P_2 uniscono le loro share, per cui viene realizzato uno schema a soglia (2,2).

Supponiamo di voler condividere un segreto S tra $P = \{A, B, C, D\}$, in modo che solo i partecipanti AB e CD ricostruiscano il segreto. Allora un (2,4) "threshold-scheme" non permette di realizzare tale scopo, in quanto esso permette a due partecipanti qualsiasi che uniscano le loro share, di calcolare il segreto e non soltanto ad AB e CD.
Nel seguito si descriverá un metodo che permette di ottenere tale scopo.

3 Struttura d'accesso

Nel precedente paragrafo è stato descritto un metodo che permette ad ogni sottoinsieme di k partecipanti di ricavare il segreto S, unendo le loro share. Una situazione più generale è quella di specificare esattamente quali sottoinsiemi di partecipanti possono determinare esattamente la chiave e quali non ci riescono.
Sia

$$\Gamma = \{X \subseteq P : X \text{ recupera il segreto}\}.$$

I sottoinsiemi di Γ sono tutti abilitati a calcolare il segreto. Γ è chiamata *struttura d'accesso* [6] ed i suoi sottoinsiemi sono chiamati *sottoinsiemi autorizzati.* Sia $\mathbf{S}$ l'insieme dei segreti e sia Sh l'insieme delle share. Quando il dealer D vuole condividere un segreto $S \in \mathbf{S}$ assegnerà ad ogni partecipante una share di Sh. Successivamente un sottoinsieme di partecipanti potrà determinare il segreto S unendo le proprie share.

Definizione 1 *Uno schema di condivisione di segreti perfetto che realizza la struttura d'accesso Γ, è un metodo di condivisione dei segreti tra un insieme di n partecipanti denotato con P, in modo tale da soddisfare le seguenti proprietà:*

1. *Se un sottoinsieme autorizzato di partecipanti $B \subseteq P$ uniscono le loro share, allora essi possono determinare il valore del segreto.*
2. *Se un sottoinsieme non autorizzato $B \subseteq P$ uniscono le loro share non riescono a determinare nessuna informazione sul valore reale del segreto.*

Notiamo che uno schema a soglia (k, n) realizza la struttura d'accesso

$$\Gamma_{(k,n)} = \{B \subseteq P : |B| \geq k\}.$$

Una tale struttura d'accesso è denominata struttura d'accesso a *soglia.*
Abbiamo visto precedentemente, che lo schema di Shamir è uno schema perfetto che realizza una struttura d'accesso a soglia.
In seguito denoteremo uno shema a condivisione di segreti, in inglese *Secret Sharing Scheme*, con l'acronimo SSS.

Definizione 2 *La sicurezza degli schemi di condivisione di segreti è* **incondizionata** *quando non possiamo mettere nessun vincolo sulla potenza di calcolo dei sottoinsiemi non autorizzati, ovvero indipendentemente dalla potenza di calcolo dei sottoinsiemi non autorizzati, essi non riusciranno a determinare il segreto.*

Supponiamo che $B \in \Gamma$ e $B \subseteq C \subseteq P$. Supponiamo che il sottoinsieme C voglia determinare il segreto. Poichè B è un sottoinsieme autorizzato può determinare il segreto. Quindi il sottoinsieme C può calcolare il segreto ignorando le share dei partecipanti in $C - B$. D'altra parte, un insieme più grande di un insieme autorizzato è ancora un insieme autorizzato. Per quanto detto, una struttura d'accesso soddisfa la proprietà monotona.

Definizione 3 *Una struttura d'accesso soddisfa la proprietà monotona se dato $B \in \Gamma$ tale che $B \subseteq C \subseteq P$ risulta che $C \in \Gamma$.*

Di seguito assumeremo che le strutture d'accesso sono monotone.

Definizione 4 *Se Γ è una struttura d'accesso, allora $B \in \Gamma$ è un sottoinsieme minimale autorizzato se $A \notin \Gamma$, dove $A \subseteq B$ e $A \neq B$.*

L'insieme dei sottoinsiemi minimali autorizzati di Γ è denotato con Γ_0 ed è detta base di Γ, dove

$$\Gamma_0 = \{X \in \Gamma : \forall P \in X, X - \{P\} \notin \Gamma\}.$$

Poichè Γ consiste di tutti i sottoinsiemi di P che sono costituiti dagli insiemi della base Γ_0, Γ è determinata univocamente come una funzione di Γ_0.
Matematicamente

$$\Gamma = \{C \subseteq P : B \subseteq C, B \in \Gamma_0\}.$$

Esempio 5 *Supponiamo che $\{P_1, P_2, P_3, P_4\}$ e*

$$\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}.$$

Allora

$$\Gamma = \Gamma_0 \bigcup \{\{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}.$$

Contrariamente, data la struttura d'accesso Γ è facile vedere che Γ_0 consiste di sottoinsiemi minimali di Γ.

3.1 Tasso di informazione

Un'importante componente nell'implementazione di schemi SSS è la taglia delle share. Lo scopo principale è quello di limitare la taglia delle share di ogni partecipante a parità di segreto. Per poter misurare tale taglia introduciamo il concetto di tasso di informazione.

Definizione 5 *Supponiamo di avere un SSS perfetto che realizza una struttura d'accesso* Γ. *Il tasso di informazione per* P_i *è il seguente:*

$$\rho_i = \frac{\log_2 |\mathbf{S}|}{\log_2 |Sh(P_i)|}$$

dove $Sh(P_i)$ *è l'insieme delle possibili share che* P_i *può ricevere, quindi* $Sh(P_i) \subseteq Sh$.
Il tasso di informazione dello schema è denotato con ρ *ed è definito come*

$$\rho = \min\{\rho_i : 1 \leq i \leq n\}.$$

Poichè l'insieme dei segreti $\mathbf{S}$ è finito possiamo pensare il segreto S come rappresentato da una stringa binaria di lunghezza $\log_2 |\mathbf{S}|$. Allo stesso modo una share assegnata a P_i può essere rappresentata da una stringa binaria di lunghezza $\log_2 |Sh(P_i)|$.
Intuitivamente, P_i riceve $\log_2 |Sh(P_i)|$ bit d'informazione, mentre la lunghezza del segreto è $\log_2 |\mathbf{S}|$ bit.

Teorema 3.1 *In ogni SSS perfetto che realizza una struttura d'accesso* Γ, $\rho \leq 1$.

Quando $\rho = 1$ si ha una situazione ottimale. Pertanto uno schema con tale tasso viene detto **ideale**.
Gli schemi di Shamir sono degli schemi ideali.

Esempio 6 *Supponiamo che* $\{P_1, P_2, P_3, P_4\}$ *e*

$$\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}.$$

Sia m *un intero e supponiamo che il segreto* $S \in Z_m$. *Il dealer sceglie a caso cinque valori (share) in* Z_m *:*

$$a_1, a_2, b_1, b_2, c_1$$

e li distribuisce nel seguente modo :

$P_1 \leftarrow (a_1, b_1)$

$P_2 \leftarrow (a_2, c_1)$

$P_3 \leftarrow (b_2, S - c_1)$

$P_4 \leftarrow (S - a_1 - a_2, S - b_1 - b_2)$.

Quindi ogni partecipante P_i *riceve come share due elementi di* Z_m.
Proviamo che lo schema è perfetto.
Dapprima verifichiamo che ogni sottoinsieme della base può calcolare S.
Il sottoinsieme $\{P_1, P_2, P_4\}$ *calcola*

$$S = a_1 + a_2 + (S - a_1 - a_2) \bmod m.$$

Il sottoinsieme $\{P_1, P_3, P_4\}$ *calcola*

$$S = b_1 + b_2 + (S - b_1 - b_2) \bmod m.$$

Il sottoinsieme $\{P_2, P_3\}$ *calcola*

$$S = c_1 + (S - c_1) \bmod m.$$

Abbiamo visto che ogni sottoinsieme autorizzato può calcolare S*, ora poniamo la nostra attenzione sui sottoinsiemi non autorizzati.*
Siano B_1 *e* B_2 *sottoinsiemi non autorizzati con* $B_1 \subseteq B_2$ *e con* B_2 *che non può calcolare* S*, allora neanche* B_1 *può calcolare* S*.*
Un sottoinsieme $B \subseteq P$ *è un sottoinsieme non autorizzato massimale se dato*

$$B_1 \in \Gamma \ \forall B_1 \supseteq B \ \textit{risulta che} \ B_1 \neq B.$$

È sufficiente verificare che nessuno dei sottoinsiemi massimali non autorizzati può determinare informazioni su S*. Nel nostro caso, i sottoinsiemi massimali non autorizzati sono :*

$$\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}.$$

In ogni caso è facile vedere che S *non può essere calcolato, perchè alcuni pezzi di informazioni casuali mancano. Per esempio, il sottoinsieme* $\{P_1, P_2\}$ *possiede solo*

$$a_1, a_2, b_1, c_1.$$

Il sottoinsieme $\{P_3, P_4\}$ *possiede le share*

$$b_2, S - c_1, S - a_1 - a_2, S - b_1 - b_2.$$

Poiché i valori di

$$c_1, a_1, a_2 \ \textit{e} \ b_1$$

sono valori casuali non conosciuti, S *non può essere calcolato. In ogni caso, un sottoinsieme non autorizzato non ha nessuna informazione sul valore di* S*.*
Il tasso di informazione per questa struttura è:

$$\rho = \frac{\log_2 m}{\log_2 m^2} = \frac{1}{2}.$$

3.2 Definizione formale

In questa sezione daremo una definizione matematica formale di un SSS perfetto.
Rappresentiamo un SSS con delle regole di distribuzione.

Definizione 6 *Una regola di distribuzione è una funzione*

$$f : P \to Sh$$

dove P *è l'insieme dei partecipanti e* Sh *è l'insieme delle share.*

Una regola di distribuzione rappresenta una possibile distribuzione di share ai partecipanti, dove $f(P_i)$ è una share assegnata a P_i con $1 \leq i \leq n$.
Sia $\mathbf{S}$ l'insieme dei segreti, per ogni $S \in \mathbf{S}$ sia F_S l'insieme delle regole di distribuzione

corrispondenti al segreto avente valore S. L'insieme F_S è pubblico.
Successivamente definiamo

$$F = \bigcup_{S \in \mathbf{S}} F_S$$

dove F è l'insieme completo delle regole di distribuzione dello schema. Se $S \in \mathbf{S}$ è il valore del segreto che D desidera condividere, allora D sceglierà una regola di distribuzione $f \in F_S$ che userà per distribuire le share. Questo è un modello generale con cui si può studiare un SSS, infatti ogni schema può essere descritto specificando esattamente quale è la regola di distribuzione usata.
Diamo un esempio per illustrare le regole di distribuzione.

Esempio 7 *Vediamo ora le regole di distribuzione per l'Esempio 4.*
Ricordiamo che:

$$P = \{P_1, P_2\} \text{ e } \mathbf{S} = \{0, 1\},$$

dove il segreto

$$S = a \oplus b, \text{ con } a, b \in \mathbf{S}.$$

Indichiamo con F_0 l'insieme delle regole di distribuzione per il segreto $S = 0$, e con F_1 l'insieme delle regole di distribuzione per il segreto $S = 1$. F_0 e F_1 contengono ognuno due regole di distribuzione equiprobabili come rappresentato nella tabella, dove ogni riga rappresenta una regola di distribuzione.

	P_1	P_2
F_0	*0*	*0*
	1	*1*
F_1	*0*	*1*
	1	*0*

Tabella 1: Regole di distribuzione per un SSS

Forniamo alcuni concetti, i quali assicurano che un insieme di regole di distribuzione per uno schema realizza una specificata struttura di accesso.

3.2.1 Definizione probabilistica di SSS

Sia $\mathbf{S}$ l'insieme dei segreti e sia $p_{\mathbf{S}}$ una distribuzione di probabilità su $\mathbf{S}$. Inoltre per ogni $S \in \mathbf{S}$, D sceglierà una regola di distribuzione in F_S in accordo alla distribuzione di probabilità p_{F_S}. Date queste distribuzioni di probabilità è possibile calcolare la distribuzione di probabilità sulla lista delle share assegnata ad ogni sottoinsieme di partecipanti (autorizzato e non autorizzato).
Sia $B \in P$. Definiamo

$$Sh(B) = \{f|_B : f \in F\}$$

dove $f|_B$ denota la restrizione della regola di distribuzione f a B.
$f|_B : B \to Sh$ è definita come

$$f|_B(P_i) = f(P_i)$$

$\forall\ Pi \in B$. Quindi $Sh(B)$ è l'insieme di tutte le possibili distribuzioni di share assegnate ai partecipanti in B. La distribuzione di probabilità su $Sh(B)$ denotata con $p_{Sh}(B)$, è calcolata

come segue.
Sia $f_B \in Sh(B)$. Allora

$$p_{Sh(B)}(f_B) = \sum_{S \in \mathbf{S}} p_{\mathbf{S}}(S) \sum_{\{f \in F_S : f|_B = f_B\}} p_{F_S}(f).$$

Inoltre,

$$p_{Sh(B)}(f_B|s) = \sum_{\{f \in F_S : f|_B = f_B\}} p_{F_S}(f)$$

per ogni $f_B \in Sh(B)$ e S $\in \mathbf{S}$.

Diamo ora una definizione formale di SSS perfetto.

Definizione 7 *Supponiamo che Γ sia una struttura d'accesso e*

$$F = \bigcup_{S \in \mathbf{S}} F_S$$

un insieme di regole di distribuzione. Allora F è un SSS perfetto che realizza la struttura d'accesso Γ soddisfacente le seguenti proprietà:

1. *Per ogni sottoinsieme autorizzato di partecipanti $B \subseteq P$, non esistono due regole di distribuzione $f \in F_S$ e $f' \in F_{S'}$ con $S \neq S'$, tale che $f|_B = f'|_B$. (Questo significa che qualsiasi distribuzione di share ai partecipanti in un sottoinsieme autorizzato B determina il valore di S (segreto)).*

2. *Per ogni sottoinsieme non autorizzato di partecipanti $B \subseteq P$ e per ogni distribuzione di share $f|_B \in Sh_B, p_{\mathbf{S}}(S|_{f_B}) = p_{\mathbf{S}}(S)$ per ogni $S \in \mathbf{S}$ (ciò significa che la distribuzione di probabilità condizionata su $\mathbf{S}$, data una distribuzione di share f_B per un sottoinsieme B non autorizzato, è la stessa distribuzione di probabilità su $\mathbf{S}$. In altre parole la distribuzione di share a B non fornisce nessuna informazione sul valore del segreto.)*

Notare che la seconda proprietà della definizione 7, è molto simile al concetto di *sicurezza perfetta*. Questa similitudine è dovuta al fatto che il risultante schema di condivisione di segreti è *perfetto*.

3.3 Un limite all'entropia sul tasso di informazione

Denotiamo con

$$\rho^* = \rho^*(\Gamma)$$

il massimo tasso di informazione per un SSS perfetto che realizza una specificata struttura d'accesso Γ. La binary entropy [2] di una distribuzione di probabilità p su un insieme finito X è definita come:

$$H(X) = -\sum_{\{x \in X : p(x) > 0\}} p(x) \log_2 p(x).$$

Abbiamo precedentemente definito una distribuzione di probabilità $p_{\mathbf{S}}$ su $\mathbf{S}$; l'entropia di questa distribuzione di probabilità è denotata con $H(S)$. Per ogni sottoinsieme di partecipanti $B \subseteq P$, l'insieme F di regole di distribuzione di questo schema, insieme con la distribuzione

di probabilità su $\mathbf{S}$, induce una distribuzione di probabilità sulla lista delle share assegnate ai partecipanti in B.
Denoteremo questa distribuzione di probabilità con $p_{Sh}(B)$ e l'entropia di questa distribuzione di probabilità come $H(B)$.
Diamo ora un'altra definizione di un SSS perfetto in termini di entropia.
Questa definizione è equivalente alla definizione 7.

Definizione 8 *Supponiamo che Γ sia una struttura d'accesso ed F un insieme di regole di distribuzioni. Allora F è un SSS perfetto che realizza la struttura d'accesso Γ e che soddisfa le seguenti proprietà:*

1. *Per ogni sottoinsieme autorizzato di partecipanti $B \subseteq P, H(\mathbf{S}|B) = 0$.*
2. *Per ogni sottoinsieme non autorizzato di partecipanti $B \subseteq P, H(S|B) = H(\mathbf{S})$.*

4 Costruzione per decomposizione

Nell'esempio 5 abbiamo ottenuto un tasso di informazione

$$\rho = \frac{1}{2}.$$

È possibile costruire schemi con

$$\rho = \frac{2}{3}.$$

La nostra costruzione principale è una costruzione ricorsiva che usa schemi ideali come base per la costruzione di schemi più grandi. Questa tecnica è denominata *Costruzione per Decomposizione.*
Prima di descrivere dettagliatamente la costruzione per decomposizione, definiamo un importante concetto.

Definizione 9 *Sia Γ una struttura di accesso con base Γ_0. Sia $\mathbf{S}$ l'insieme dei segreti.*
Una $\mathbf{S}$-decomposizione ideale di Γ_0 consiste di un insieme

$$\{\Gamma_1, ..., \Gamma_m\}$$

soddisfacente le seguenti proprietà:

1. *$\Gamma_k \subseteq \Gamma_0$ per $1 \leq k \leq m$*
2. *$\bigcup_{k=1}^{m} \Gamma_k = \Gamma_0$*
3. *Per $1 \leq k \leq m$, esiste uno schema ideale con un insieme di segreti $\mathbf{S}$, sul sottoinsieme dei partecipanti*

$$P_k = \bigcup_{B \in \Gamma_k} B$$

per la struttura d'accesso avente base Γ_k.

Ricordiamo che uno schema è ideale quando $\rho = 1$.
Data una **S**-decomposizione ideale per una struttura d'accesso Γ, possiamo costruire un SSS perfetto, come descritto nel seguente teorema.

Teorema 4.1 *Sia Γ una struttura d'accesso con base Γ_0. Sia* **S** *l'insieme dei segreti specificati, e sia $\{\Gamma_1, ..., \Gamma_m\}$ una* **S***-decomposizione ideale di Γ. Per ogni partecipante P_i, definiamo*

$$R_i = |\{k : P_i \in P_k\}|.$$

Allora esiste uno SSS perfetto che realizza Γ avente tasso di informazione

$$\rho = \frac{1}{R}$$

dove

$$R = \max\{R_i : 1 \leq i \leq n\}.$$

Sia Γ una struttura d'accesso e Γ_0 la sua base. Ricordando che Γ_0 consiste di tutti i sottoinsiemi minimali autorizzati, si ha come conseguenza del teorema che

$$\forall\ \Gamma\ \exists \text{ un SSS perfetto che realizza } \Gamma.$$

Infatti dato un insieme di segreti **S**, dalla definizione 9 abbiamo che l'insieme $\{\Gamma_1, ..., \Gamma_m\}$ rappresenta una **S**-decomposizione ideale, dove Γ_i per $1 \leq i \leq m$ è un sottoinsieme minimale autorizzato di Γ_0. Dal Teorema 4.1 segue che $\exists$ un SSS perfetto.

Possiamo generalizzare il teorema andando a considerare ℓ **S**-decomposizioni ideali di Γ_0, invece di una sola. Ognuna delle ℓ decomposizioni è usata per condividere un segreto $\in$ **S**. In tal modo l'insieme dei segreti diviene $\mathbf{S}^\ell$. Per la costruzione di tale schema si utilizza il seguente teorema.

Teorema 4.2 *Sia Γ una struttura d'accesso con base Γ_0 e sia $\ell \geq 1$ un intero. Sia* **S** *l'insieme dei segreti specificato e per ogni $1 \leq j \leq \ell$, supponiamo che $D_j = \{\Gamma_{j,1}, ..., \Gamma_{j,m_j}\}$ è una decomposizione ideale di Γ_0. Sia $\mathbf{P}_{j,k}$ l'insieme dei partecipanti per la struttura d'accesso $\Gamma_{j,k}$. Per ogni partecipante P_i, definiamo*

$$R_i = \sum_{j=1}^{\ell} |\{k : P_i \in \mathbf{P}_{j,k}\}|.$$

Allora esiste un SSS perfetto che realizza Γ avente tasso di informazione

$$\rho = \frac{\ell}{R}$$

dove

$$R = \max\{R_i : 1 \leq i \leq n\}.$$

Esempio 8 *Sia* $\Gamma = \{P_1P_2, P_2P_3, P_3P_4\}$. *Sia* p *un numero primo, consideriamo due* Z_p*-decomposizioni ideali :*

$$D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$$

dove

$$\Gamma_{1,1} = \{\{P_1P_2\}\} \text{ mentre } \Gamma_{1,2} = \{\{P_2P_3\}, \{P_3P_4\}\}$$

e

$$D_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$$

dove

$$\Gamma_{2,1} = \{\{P_1P_2\}, \{P_2P_3\}\} \text{ e } \Gamma_{2,2} = \{\{P_3P_4\}\}.$$

Applicando il Teorema 4.1 per D_1 *si ottiene :*

$$R_1 = R_3 = R_4 = 1$$
$$R_2 = 2$$

pertanto abbiamo

$$\rho = \frac{1}{2}.$$

Analogamente, applicando il Teorema 4.1 D_2 *si ottiene :*

$$R_1 = R_2 = R_4 = 1$$
$$R_3 = 2.$$

Applicando il Teorema 4.2 con $\ell = 2$ *si ottiene:*

$$R_1 = R_4 = 2$$
$$R_2 = R_3 = 3$$

pertanto abbiamo

$$\rho = \frac{2}{3}.$$

Un'implementazione di questo è la seguente: D *sceglie a caso in* Z_p a, b, c, d. *Data una chiave* $(S_1, S_2) \in Z_p^2$ *e distribuisce le share come segue :*

$P_1 \leftarrow (a, c)$

$P_2 \leftarrow (a + S_1, b, c + S_2)$

$P_3 \leftarrow (b + S_1, c, d)$

$P_4 \leftarrow (b, d + S_2)$

Esempio 9 *Sia*

$$\Gamma = \{P_1P_2, P_2P_3, P_2P_4, P_3P_4\}.$$

Sia p un numero primo, consideriamo due Z_P-decomposizioni ideali:

$$D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$$

dove

$$\Gamma_{1,1} = \{\{P_1P_2\}\}$$

$$\Gamma_{1,2} = \{\{P_2P_3\}, \{P_2P_4\}, \{P_3P_4\}\}$$

e

$$D_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\},$$

dove

$$\Gamma_{2,1} = \{\{P_1P_2\}, \{P_2P_3\}, \{P_2P_4\}\}$$

$$\Gamma_{2,2} = \{\{P_3P_4\}\}.$$

Applicando il Teorema 4.2 alla decomposizione ideale D_1 si ottiene:

$$R_1 = 2$$

$$R_2 = R_3 = 3 = R_4 = 3$$

da cui si calcola $R = 3$.
Pertanto abbiamo

$$\rho = \frac{2}{3}$$

il quale è un valore ottimale.
Forniamo un'implementazione di quanto detto.
Il dealer sceglie 4 elementi casuali indipendenti appartenenti a Z_p, a, b, c, d. Dato un segreto $(S_1, S_2) \in Z_p^2$, D distribuisce le share come segue:

$P_1 \leftarrow (a + S_1, c + S_2)$

$P_2 \leftarrow (a, b, c)$

$P_3 \leftarrow (b + S_1, c + S_2, d)$

$P_4 \leftarrow (b + 2S_1, c + S_2, d + S_2)$

Riferimenti

[1] Douglas R. Stinson. *Cryptography: Theory and Practice.* Cap.11. CRC Press, Inc, 1995.

[2] Douglas R. Stinson. An Explication of Secret Sharing Scheme. *Design, Codes and Cryptography.* vol. 2, pp. 397-390, 1992.

[3] T. H. Cormen, C. E. Leiserson, R. L. Rivest. *Introduzione agli Algoritmi.* vol. 3, Jackson libri, 1995.

[4] G. R. Blakley. Safeguarding cryptographic keys. AFIPS *Conference Proceedings.* vol. 48, pp. 313-317, 1979.

[5] A. Shamir. How to share a secret. *Communications of the ACM.* vol. 22, pp. 612-613, 1979.

[6] M. Ito, A. Saito e T. Nishizeki. Secret sharing scheme realizing general access structure. *Proceedings IEEE Globecom '87.* pp. 99-102, 1987.

[7] E. D. Karnin, J. W. Greene, e M. E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory.* vol. 29, pp. 35-41, 1983