Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

SCHEMI DI CONDIVISIONE DI SEGRETI

Tesi di Laurea in
ALGORITMI DELLA TEORIA DEI NUMERI E CRITTOGRAFIA

Relatore:
Prof.
DAVIDE ALIFFI

Presentata da:
GIORGIA MILANDRI

Sessione II
Anno accademico 2013-2014

Indice

Introduzione

Il termine italiano *Schemi di Condivisione di Segreti* è la traduzione del termine inglese *Secret Sharing Schemes*, le cui iniziali danno luogo all'acronimo SSS.

Supponiamo di avere un messaggio segreto S, rappresentato da un numero intero, da dividere tra più persone in modo tale che, se non cooperano tra loro, non riescano a ricostruire il messaggio. Vediamo due casi:

- Il caso più semplice è quando vogliamo dividere S tra due persone A e B. La soluzione è molto semplice: diamo ad A un numero casuale r e a B diamo $S - r$ .Per ricostruire il messaggio A e B dovranno sommare i loro frammenti.

- Più in generale se vogliamo dividere il segreto S tra m persone dobbiamo scegliere $m-1$ numeri casuali $r_1, ..., r_{m-1} \mod n$, dove n è un intero più grande di tutti i possibili S, e darne uno ciascuno alle $m-1$ persone. All'ultima persona daremo $S - \sum_{k=1}^{m-1} r_k \mod n$).

Uno schema di condivisione come questo richiede che *tutti* i partecipanti si accordino per la ricostruzione del messaggio. Questo schema presenta notevoli difficoltà qualora non tutti i partecipanti siano d'accordo o non possano essere contattati.

Immaginiamo di avere una cospicua somma di denaro e di volerla lasciare in eredità ai nostri parenti. I soldi sono al sicuro in una cassaforte di cui solo noi conosciamo la combinazione. Poichè non ci fidiamo di tutti i sette figli, dividiamo la combinazione tra loro in modo che tre di loro debbano collaborare per ricostruire la combinazione intera. In questo caso chiunque voglia ottenere l'eredità deve cooperare con almeno due fratelli.

Questa volta è necessario e sufficiente che solo 3 delle parti collaborino per ricostruire S.

Uno schema di condivisione di questo tipo si definisce *schema a soglia*:

Definizione 1. *Siano t e w interi positivi con $t \geq w$. Uno schema a soglia (t,w) è un metodo per condividere un messaggio S tra w partecipanti in modo che un qualunque sottoinsieme di t partecipanti possa ricostruire S, mentre nessun sottoinsieme di cardinalità inferiore possa riuscirci.*

Nei prossimi paragrafi si approfondirà questo particolare schema di condivisione dei segreti, inventato indipendentemente nel 1979 sia da Adi Shamir che da Blakley.

Capitolo 1

Schema a soglia (t,w)

Siano t e w interi positivi tali che $t < w$. Uno schema a soglia (t,w) è un metodo di condivisione di una chiave k tra un insieme di w partecipanti, tale che:

- Ogni gruppo di partecipanti di cardinalità $\geq t$ riesce a ricostruire la chiave k
- Ogni gruppo di partecipanti di cardinalità $< t$ non riesce ad ottenere alcuna informazione riguardante il segreto k

Il valore di k è scelto da un partecipante speciale chiamato *Dealer*, che sarà denotato con la lettera D. Si assume che D $\notin P$ dove

$$P = \{P_i : 1 \leq i \leq w\}$$

è l'insieme dei partecipanti. Quando D vuole condividere la chiave k tra i partecipanti in P, assegna ad ogni partecipante un' informazione parziale, detta *share*. Le *share* vengono distribuite segretamente in modo che nessun partecipante conosca le *share* date agli altri partecipanti.

Successivamente, consideriamo un sottoinsieme di partecipanti $B \subseteq P$ che uniscono le loro *share* per cercare di risalire alla chiave k. Se $|B| \geq t$ allora essi saranno in grado di ricavare la chiave k come funzione delle loro *share*, mentre se $|B| < t$ non riusciranno a risalire a k.

Le notazioni che userò saranno:

- $P = \{P_i : 1 \leq i \leq w\}$ come l'insieme dei w partecipanti
- K, l'insieme di tutte le possibili chiavi
- S, l'insieme di tutti i possibili share

Nelle prossime pagine presenterò dei metodi per costruire uno schema a soglia (t,w) chiamato *Schema a Soglia di Shamir*, inventato appunto da Shamir nel 1979.

1.1 Schema a soglia di Shamir (t,w)

Sia $K = Z_p$, con $p \geq w + 1$ primo e $S = Z_p$, (cioè la chiave e ogni share condivisa con i partecipanti sono elementi di (Z_p).

I passi dell'algoritmo di distribuzione delle share del Dealer D sono i seguenti:

- FASE INIZIALE

  1. D sceglie w elementi distinti e non nulli di Z_p:

  $$x_i \in Z_p \qquad \text{con} \qquad 1 \leq i \leq w$$

  e distribuisce i valori x_i ai P_i con $1 \leq i \leq w$. I valori x_i e p sono *pubblici*.

- DISTRIBUZIONE DELLE SHARE

  2. Supponiamo che D voglia condividere $k \in Z_p$. Allora D sceglie segretamente e casualmente (uniformemente e indipendentemente) $t - 1$ elementi di Z_p, che denota $a_1, ..., a_{t-1}$.

  3. Per $1 \leq i \leq w$ D calcola $y_i = a(x_i)$, dove

  $$a(x) = k + \sum_{j=1}^{t-1} a_j x^j \mod p$$

  4. Per $1 \leq i \leq w$, D distribuisce le share y_i ai P_i segretamente

In questo schema, D costruisce un polinomio casuale $a(x)$ di grado massimo $t - 1$ e dove il termine costante è la chiave segreta k. Ogni partecipante P_i ottiene un punto (x_i, y_i) del grafico del polinomio.

Vediamo ora come un sottoinsieme di partecipanti $B \subseteq P$ può ricostruire la chiave k.

Esistono due metodi per ricavare k: uno basato sulla *risoluzione di sistemi di equazioni lineari* e l'altro basato sul *concetto di interpolazione polinomiale*.

1.2 Metodo per il calcolo della chiave k basato sulla risoluzione di sistemi di equazioni lineari

Supponiamo che $P_{i_1}, ..., P_{i_t}$ vogliano determinare k. Ora

$$y_{i_j} = a(x_{i_j})$$

per $1 \leq j \leq t$, dove $a(x) \in Z_p[x]$ è il polinomio segreto scelto da D. Poichè $a(x)$ ha grado massimo $t-1$, a(x) può essere scritto come:

$$a(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$$

dove i coefficenti $a_0, ..., a_{t-1}$ sono elementi incogniti in Z_p e $a_0 = k$ è la chiave.

Poichè $y_{i_j} = a(x_{i_j})$ sono lineari nei coefficenti di $a(x)$, per $1 \leq j \leq t$ i partecipanti ottengono un sistema di t equazioni in t incognite $a_0, ..., a_{t-1} \in Z_p$. Se le equazioni sono linearmente indipendenti, ci sarà un unica soluzione, e a_0 rivelerà la chiave.
Il sistema di equazioni lineari è il seguente:

$$\begin{cases} a_0 + a_1 x_{i_1} + ... + a_{t-1} x_{i_1}^{t-1} = y_{i_1} \\ a_0 + a_1 x_{i_2} + ... + a_{t-1} x_{i_2}^{t-1} = y_{i_2} \\ \vdots \\ a_0 + a_1 x_{i_t} + ... + a_{t-1} x_{i_t}^{t-1} = y_{i_t} \end{cases}$$

scritto anche in forma matriciale come segue:

$$\begin{pmatrix} 1 & x_{i_1} & x_{i_1}^2 & \dots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \dots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_t} & x_{i_t}^2 & \dots & x_{i_t}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_t} \end{pmatrix}$$

Sia A la matrice t x t cosí costruita. Essa è una matrice di Vandermonde[1], e il suo determinante è:

$$det(A) = \prod_{1 \leq j < k \leq t} (x_{i_k} - x_{i_j}) \mod p$$

Ricordiamo che essendo tutte le x_i distinte, ogni termine $(x_{i_k} - x_{i_j}) \neq 0$. Il prodotto è calcolato in Z_p, che è un campo per cui il prodotto di termini diversi da zero è diverso da zero e quindi il $det(A) \neq 0$. Essendo il determinante diverso da 0, il sistema ammette sempre un'unica soluzione. Questo dimostra che in uno schema a soglia, un gruppo di t

[1]In algebra lineare la matrice di Vandermonde è la matrice le cui righe (o colonne) hanno elementi, a partire da 1, in progressione geometrica. Le proprietà del suo determinante saranno sviluppate in appendice.

partecipanti riuscirà sempre a determinare la chiave k in modo univoco.

Vediamo ora invece cosa succede se un gruppo di $t-1$ partecipanti $P_{i_1}, ..., P_{i_{t-1}}$ si unisce nel tentativo di ricavare la chiave k. Procedendo come prima, si otterrà un sistema di $t-1$ equazioni in t incognite $a_0, ..., a_{t-1} \in Z_p$. Il sistema delle equazioni lineari è il seguente:

$$\begin{cases} a_0 + a_1 x_{i_1} + ... + a_{t-1} x_{i_1}^{t-1} = y_{i_1} \\ a_0 + a_1 x_{i_2} + ... + a_{t-1} x_{i_2}^{t-1} = y_{i_2} \\ \vdots \\ a_0 + a_1 x_{i_{t-1}} + ... + a_{t-1} x_{i_{t-1}}^{t-1} = y_{i_{t-1}} \end{cases}$$

Poichè per ogni polinomio i termini $a_1, ..., a_{t-1}$ sono scelti dal Dealer in modo casuale e solo a lui noti, segue che i $t-1$ partecipanti non riusciranno a trovare il valore a_0, perchè il sistema avrà sempre soluzioni non uniche, almeno p.

1.2.1 Esempio

Supponiamo $p = 17$, $t = 3$ e $w = 5$; le coordinate pubbliche sono $x_i = i$ per $1 \leq i \leq 5$. Supponiamo che $B = \{P_1, P_3, P_5\}$ uniscano le loro share, che sono rispettivamente 8, 10 e 11. Allora il polinomio $a(x)$

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

darà per i tre partecipanti in Z_{17}, le seguenti share:

$$a(1) = a_0 + a_1 + a_2 = 8$$

$$a(3) = a_0 + 3a_1 + 9a_2 = 10$$

$$a(5) = a_0 + 5a_1 + 8a_2 = 11$$

Questo sistema ha un' unica soluzione in Z_{17}: $a_0 = 13$, $a_1 = 10$ e $a_2 = 2$, perciò la chiave $k = a_0 = 13$.

1.3 Metodo per il calcolo della chiave k basato sul concetto di interpolazione polinomiale

L'interpolazione polinomiale è una tecnica che permette di risolvere il problema della approssimazione di funzioni che presentano un andamento non lineare.

Premettiamo un teorema:

Teorema 1 (Formula di interpolazione di Lagrange)**.** [2]
Supponiamo p primo, $x_1, ..., x_{m+1}$ elementi distinti di Z_p e $a_1, ..., a_{m+1}$ elementi non necessariamente distinti di Z_p. Allora esiste un unico polinomio $A(x) \in Z_p[x]$ con grado massimo m, tale che $A(x_i) = a_i$, $1 \leq i \leq m+1$.
Il polinomio $A(x)$ è il seguente:

$$A(x) = \sum_{j=1}^{m+1} \left(a_j \prod_{1 \leq h \leq m+1, h \neq j} \frac{x - x_h}{x_j - x_h} \right)$$

Questo teorema mi assicura che il polinomio di grado massimo $t-1$ è unico e fornisce una formula che può essere usata per calcolare il polinomio a(x) (creato dal Dealer) dati i punti (x_{i_j}, y_{i_j}).
La formula è la seguente:

$$a(x) = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \mod p$$

Un gruppo B di t partecipanti ora può calcolare $a(x)$ utilizzando la formula di interpolazione. Anzi è possibile semplificare il calcolo, in quanto i partecipanti non hanno bisogno di conoscere tutto il polinomio a(x): è sufficente per loro dedurre il termine costante $k = a(0)$. Per questo, possono calcolare la seguente espressione, che viene ottenuta sostituendo $x = 0$ nella formula di interpolazione di Lagrange:

$$k = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_j} - x_{i_k}} \right) \mod p$$

Definiamo:

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

con $1 \leq j \leq t$, allora avremo:

$$k = \sum_{j=1}^{t} b_j y_{i_j} \mod p$$

Quindi, la chiave è una combinazione lineare modulo p di t share qualsiasi.

[2] Sviluppato in appendice

1.3.1 Esempio

Riprendiamo l'esempio 1: I partecipanti $\{P_1, P_3, P_5\}$ possono calcolare $\{b_1, b_2, b_3\}$ mediante la formula

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

che nell'esempio diventa:

$$b_1 = \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} \mod 17$$

$$= 3 \times 5 \times (-2)^{-1} \times (-4)^{-1} \mod 17 = 4.$$

Allo stesso modo si ottiene $b_2 = 3$ e $b_3 = 11$. Allora, assegnate rispettivamente le share 8, 10 e 11 si ottiene

$$k = 4 \times 8 + 3 \times 10 + 11 \times 11 \mod 17 = 13$$

come prima.

Anche in questo caso, come per il primo metodo di risoluzione, se un sottoinsieme B di $t-1$ partecipanti cerca di calcolare k non avrà successo. Infatti, fissiamo un valore $y_0 \in Z_p$ come chiave k, dove la chiave nel sistema a soglia di Shamir è $k = a_0 = a(0)$. Inoltre, poichè i partecipanti sono $t-1$, il polinomio $a(x)$ avrà $t-1$ valori noti in Z_p. Ora applicando il teorema precedente, c'è un unico polinomio $a_{y_0}(x)$ tale che:

$$y_{i_j} = a_{y_0}(x_{i_j})$$

con $1 \leq j \leq t-1$ e tale che

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

Cioè, esiste un unico polinomio $a_{y_0}(x)$ interpolatore per le $t-1$ share conosciute a B, e che presenta y_0 come chiave (come termine noto).
Poichè questo è vero per qualsiasi valore $y_0 \in Z_p$, nessun valore di k può essere escluso e quindi qualsiasi gruppo di $t-1$ partecipanti non può ottenere informazioni su k.

1.3.2 Esempio

Riprendendo gli esempi precedenti supponiamo che P_1 e P_3 vogliano provare a calcolare k. P_1 ha come share 8 mentre P_3 ha come share 10. Allora per ogni possibile valore y_0 della chiave, esiste un unico polinomio $a_{y_0}(x)$ che assume il valore 8 in $x = 1$, 10 in $x = 3$ e il valore y_0 in $x = 0$. Usando la formula di interpolazione il polinomio diventa:

$$a_{y_0}(x) = 6y_0(x-1)(x-3) + 13x(x-3) + 13x(x-1) \mod 17.$$

Perciò l'insieme $\{P_1, P_3\}$ non ha modo di scoprire il polinomio corretto e quindi di avere qualche informazione su k.

1.4 Schema a soglia (t,t)

Un caso particolare dello schema a soglia di Shamir è il caso in cui $w = t$. Questo semplice schema funziona considerando qualsiasi set di chiavi $K = Z_m$ e di share $S = Z_m$ (per questo schema non è necessario che m sia primo e neanche che m sia $\geq w + 1$).

Per condividere la chiave $k \in Z_m$, D svolge i passi seguenti:

- D sceglie segretamente e casualmente $t - 1$ elementi di Z_m:

$$y_1, ..., y_{t-1}$$

- D calcola:

$$y_t = k - \sum_{i=1}^{t-1} y_i \mod m$$

- Per $1 \leq i \leq t$ D distribuisce le share y_i ai P_i.

Quindi in questo caso sono necessari tutti i t partecipanti per calcolare k che verrà ricavata dalla formula:

$$k = \sum_{i=1}^{t} y_i \mod m.$$

E qualsiasi sottoinsieme di $t - 1$ partecipanti non può ricavare il valore di k. Infatti se consideriamo un sottoinsieme di partecipanti $P \setminus \{P_i\}$ con $1 \leq i \leq t - 1$, le share in loro possesso sono

$$y_1, ..., y_{i-1}, y_{i+1}, ..., y_{t-1}$$

e sommando riescono a trovare

$$k - y_i$$

Tuttavia non conoscendo il valore random y_i non ottengono nessuna informazione sulla chiave k.

1.4.1 Esempio

Supponiamo $p = 10$ e $t = 4$ e le share date a ciascun partecipante $y_1 = 7$, $y_2 = 2$, $y_3 = 4$ e $y_4 = 2$. La chiave k sarà:

$$k = 7 + 2 + 4 + 2 \mod 10 = 16 \mod 10 = 5.$$

Supponiamo ora che siano solo i primi tre partecipanti ad unirsi per trovare la chiave k. Loro sanno che $y_1 + y_2 + y_3 \mod 10 = 3$ ma non conoscono il valore di y_4. Ci saranno quindi corrispondenze tra i 10 possibili valori di y_4 e i 10 possibili valori di k:

$$y_4 = 0 \Leftrightarrow k = 3,$$

$$y_4 = 1 \Leftrightarrow k = 4,$$

$$\ldots$$

$$y_4 = 9 \Leftrightarrow k = 2,$$

nessuno dei quali dà informazioni su k.

1.5 Vulnerabilità dello schema di Shamir e soluzione di Ben-Or e Rabin

Il sistema di condivisione di segreti di Shamir assume che sia i partecipanti che il Dealer siano onesti. Nella realtà invece può succedere che il Dealer sia corrotto e assegni share incoerenti ai partecipanti, in modo che un sottogruppo non riesca a ricostruire la chiave k. Oppure gli stessi partecipanti possono rivelare uno share falso nella fase della condivisione e quindi venire a conoscenza degli altri share in modo da ottenere solo per se stessi la chiave k.

Il protocollo per individuare i partecipanti disonesti è stato introdotto da Rabin e Ben-Or. Il loro lavoro espande il protocollo di condivisione dei segreti, quando più della metà dei partecipanti sono onesti e quando esiste un canale di comunicazione appropriato, in modo tale che qualsiasi calcolo multipartitico venga effettuato solo dalle parti oneste. Partendo dal presupposto che ogni partecipante può trasmettere un messaggio a tutti gli altri partecipanti e che ogni coppia di partecipanti sia in grado di comunicare in segreto, Rabin e Ben-Or presentano un protocollo di condivisione di segreti verificabile, e dimostrano che qualsiasi accordo multipartitico può essere raggiunto se la maggioranza dei giocatori sono onesti. La segretezza raggiunta è incondizionata e non si basa su alcun presupposto di intrattabilità computazionale.

Tal Rabin e Michael Ben-Or hanno perfezionato il protocollo di Shamir introducendo una dimostrazione a zero-knowledge basata sull'uso di Check Vectors (o vettori di controllo) nel protocollo. (In crittografia un protocollo zero-knowledge o a conoscenza zero è un metodo interattivo utilizzato da un soggetto per dimostrare ad un altro soggetto di essere a conoscenza di un segreto, senza rivelare nient'altro oltre alla conoscenza dello stesso.)
Il protocollo di Shamir migliorato è il seguente:

Per ogni coppia di partecipanti A e B, il Dealer fissa due interi positivi $b_{AB}, y_{AB} \in Z_p$ e calcola

$$c_{AB} = b_{AB}y_{AB} + s_A \mod p$$

dove s_A è la share che riceve A. Ora D distribuisce ad A la coppia (s_A, y_{AB}) e a B la coppia (b_{AB}, c_{AB}).

$$D \to A(s_A, y_{AB})$$
$$D \to B(b_{AB}, c_{AB})$$

La seconda coppia è conosciuta come *check-vector*, cioè permette a B di verificare che la share comunicata da A sia corretta attraverso la formula precedente. É importante notare che i vettori sono tenuti nascosti da ogni partecipante, e solo nel momento della

condivisione delle share per la ricostruzione della chiave k, ogni partecipante A scambia la sua informazione privata con B.

$$A \to B(y_{AB})$$

$$B \text{ calcola } (c_{AB} - b_{AB}y_{AB}) \text{ e controlla che A condivida proprio } s_A$$

In questo modo B controlla che A condivida con il resto dei partecipanti proprio la share data dal Dealer e non una falsa.

Ma se è il dealer ad essere corrotto, egli potrebbe distribuire ad ogni partecipante $P_1, ..., P_w$ delle share $s_1, .., s_w$ in modo tale che quando i partecipanti $i_1, ..., i_t$ mettano insieme le loro share ottengano la chiave k mentre ricombinando le share dei partecipanti $j_1, ..., j_t$ si avrà come risultato una chiave $k' \neq k$.

$$D \to P_1(s_1)$$

$$D \to P_2(s_2)$$

$$...$$

$$D \to P_w(s_w)$$

Diremo che il Dealer è onesto se e solo se le due chiavi k e k' coincidono e a quel punto diremo che le share date ai partecipenti sono *coerenti*.

Per risolvere questo tipo di problema è nato il concetto di Sistema verificabile di condivisione di segreti ("Verifiable Secret Sharing" - VSS), introdotto da Chor, Goldwasser, Micali e Awerbuch. In questo schema di verifica il Dealer trasmette meno infomazioni possibili, rivelando solo qualche piccola infomazione sulle share, in modo che i partecipanti possano verificare che le loro share siano coerenti.

In particolare uno schema elegante di questo tipo è stato introdotto da Paul Feldman. In questo schema il Dealer prende un gruppo ciclico G con un generatore noto g, in modo che sia computazionalmente intrattabile ottenere il valore di x conoscendo g^x (ossia sia intrattabile il problema del logaritmo discreto.) Se $|G|$ è un primo p e il Dealer usa il polinomio

$$f(x) = k + a_1x + , ..., + a_{t-1}x^{t-1} \mod p,$$

allora pubblica $g, g^k, g^{a_1}, ..., g^{a_{t-1}}, g^{f(i_1)}, ..., g^{f(i_w)}$. In questo modo, ogni partecipante disponendo di una share $f(i_j)$ può controllare che la $g^{f(i_j)}$ calcolata autonomamente equivalga a quella pubblicata.

Capitolo 2

Schema a soglia di Blakley (t,w)

Mentre lo schema a soglia di Shamir si basa sull'interpolazione polinomiale, quello di Blakley si basa sulla geometria degli iperpiani.
Per implementare lo schema a soglia (t,w), ad ognuno degli w partecipanti viene data un'equazione in dimensione t di un iperpiano su un campo finito, in modo che tutti gli w iperpiani si intersechino in un unico punto. Il punto di intersezione è la chiave segreta k. Quando t partecipanti si uniscono, risolvono un sistema di equazioni per trovare la chiave.

La chiave è un punto in uno spazio di t dimensione, e le w share sono iperpiani affini passanti tutti per questo punto. Un iperpiano affine in uno spazio di dimensione t con coordinate in un campo finito F può essere descritto da una equazione lineare:

$$a_1x_1 + a_2x_2 + ... + a_tx_t = b.$$

Il punto di intersezione si trova intersecando qualsiasi t di questi iperpiani. La chiave k è definita come la prima coordinata del punto di intersezione.

- FASE INIZIALE
  Sia p primo e consideriamo il campo Z_p. Il Dealer genera un punto segreto x in Z_p, la cui prima coordinata è il valore della chiave k, e genera casualmente i valori delle altre coordinate nel campo Z_p. L'utente i-esimo otterrà l'equazione di un iperpiano:
  $$a_{i1}x_1 + a_{i2}x_2 + ... + a_{it}x_t = y_i$$
  contenente il punto x. Per lo schema (t,w) ci saranno w equazioni di iperpiani, quindi avremo un sistema lineare $w \times t$:
  $$Ax = y$$
  Infine il Dealer manda i valori $y_i, a_{i1}, ..., a_{it}$ al partecipante i-esimo.

- FASE DI COMBINAZIONE DELLE SHARE
  Supponiamo che una coalizione di utenti $S = \{P_{i1}, ..., P_{it}\}$ si uniscano per ricostruire la chiave k. Utilizzando le loro equazioni creeranno una matrice A_s tale che:
  $$A_s x = y_s,$$
  dove y_s è il vettore formato dalle share segrete dei partecipanti. La chiave cercata sarà la prima coordinata della soluzione di questo sistema di t equazioni in t incognite.

Finchè p è ragionevolmente grande, è facile che la matrice sia invertibile, ma non è garantito. Non è difficile trovare strategie di scelta dei valori a_i tali che la matrice sia sempre invertibile. Essenzialmente, questo è quello che accade nel metodo di Shamir. Le equazioni matriciali per i due metodi sono molto simili, per cui il metodo di Shamir può essere visto come un caso particolare del metodo di Blakley. Ma poichè il metodo di Shamir dà una matrice di Vandermonde, le equazioni hanno sempre soluzione. Il secondo vantaggio del metodo di Shamir è che ciascun partecipante deve ricordare meno informazioni.
Inoltre a differenza dello schema a soglia di Shamir quello di Blackley non viene ritenuto uno schema a soglia perfetto in quanto piú cresce il numero di partecipanti che si uniscono, piú decresce l'incertezza su dove si trovi il punto. Ad esempio i partecipanti sanno che il punto, quindi la chiave, si trova sul loro iperpiano e se si uniscono le share di $t-1$ partecipanti si individua anche la retta su cui si trova il punto.

Vediamo ora come si definiscono gli schemi a soglia perfetti e con quale criteri si valuta la sicurezza di questi schemi.

Capitolo 3

Struttura d'accesso

Nei capitoli precedenti, è stato descritto un metodo che permette ad ogni sottoinsieme di t partecipanti di ricavare la chiave k, unendo le loro share. Una situazione piú generale specifica esattamente quali sottoinsiemi di partecipanti saranno in grado di determinare la chiave k e quali no.

Sia $\Gamma = \{X \subseteq P : X$ recupera il segreto$\}$. I sottoinsiemi di Γ sono tutti abilitati a calcolare il segreto. Γ è chiamata *struttura d'accesso* ed i suoi sottoinsiemi sono chiamati *sottoinsiemi autorizzati.*

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 w partecipanti denotato con P, in modo tale che siano soddisfatte le seguenti proprietà:*

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

Uno schema a soglia (t,w) realizza la struttura d'accesso: $\Gamma_{(t,w)} = \{B \subseteq P : |B| \geq t\}$

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 k. Poichè B è un sottoinsieme autorizzato può determinare k. Perciò il sottoinsieme C può calcolare k ignorando le share dei partecipanti in $C - B$. Un insieme che contiene un insieme autorizzato, è ancora un insieme autorizzato. Allora avremo che 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* $C \in \Gamma$.

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

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

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

Poichè Γ è fatto di tutti i sottoinsiemi di P che sono ottenuti dagli insiemi della base Γ_0, ne segue che Γ è determinata univocamente da Γ_0. La sua espressione matematica è la seguente:

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

Nel caso di uno schema a soglia (t, w), la base è costituita da tutti i sottoinsiemi composti esattamente da t partecipanti.

3.0.1 Esempio

Sia $P = \{P_1, P_2, P_3, P_4\}$ e

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

Allora:

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

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

3.1 Regole di Distribuzione

In questa sezione daremo una definizione matematica formale di uno schema di condivisione di segreti perfetto e lo rappresenteremo con un insieme di regole di distribuzione.

Definizione 5. *Una regola di distribuzione è una funzione*

$$f : P \to S$$

dove P è l'insieme dei partecipanti e S 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 $1 \leq i \leq w$. Sia K l'insieme delle chiavi, per ogni $k \in K$ sia F_K l'insieme delle regole di distribuzione corrispondenti alla chiave avente valore k. L'insieme F_K è pubblico.
Successivamente definiamo:

$$F = \bigcup_{k \in K} F_K$$

dove F è l'insieme completo delle regole di distribuzione dello schema. Se $k \in K$ è il valore della chiave che D desidera condividere, allora D sceglierà una regola di distribuzione $f \in F_K$ che userà per distribuire le share. Questo è un modello generale con cui si può studiare uno schema di condivisione di segreti, infatti ogni schema può essere descritto specificando esattamente quale è la regola di distribuzione usata.

3.1.1 Definizione probabilistica di SSS

Sia K l'insieme dei segreti e sia p_K una distribuzione di probabilità su K, cioè p_K è la probabilità che una chiave k sia scelta dal Dealer. Inoltre per ogni $k \in K$, il Dealer D sceglierà una regola di distribuzione in F_K in accordo alla distribuzione di probabilità p_{F_K}. Date queste distribuzioni di probabilità è possibile calcolare la distribuzione di probabilità sulla lista delle share assegnata ad ogni sottoinsieme di partecipanti (autorizzati e non). Supponiamo $B \subseteq P$ e definiamo:

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

dove la funzione $f|_B$ denota la restrizione della regola di distribuzione f a B: $f|_B : B \to S$, definita come

$$f|_B(P_i) = f(P_i) \forall P_i \in B$$

Quindi $S(B)$è l'insieme di tutte le possibili distribuzioni di share assegnate ai partecipanti in B. La distribuzione di probabilità su $S(B)$, denotata con $p_S(B)$, è calcolata come segue. Sia $g_B \in S(B)$. Allora:

$$p_{S(B)}(g_B) = \sum_{k \in K} \left(p_K(k) \sum_{\{f \in F_K : f|_B = g_B\}} p_{F_K}(f) \right).$$

Inoltre:

$$p_{S(B)}(g_B|_k) = \sum_{\{f \in F_K : f|_B = g_B\}} p_{F_K}(f).$$

$\forall g_B \in S(B)$ e $k \in K$.

Ecco allora una definizione formale di SSS perfetto.

Definizione 6. *Supponiamo* Γ *sia una struttura d'accesso e*

$$F = \bigcup_{k \in K} F_K$$

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

- *Per ogni sottoinsieme autorizzato di partecipanti* $B \subseteq P$*, non esistono due regole di distribuzione* $f \in F_K$ *e* $f' \in F_{k'}$ *con* $k \neq k'$*, tale che* $f|_B = f'|_B$*. (Cioè ogni distribuzione di share ai partecipanti di un sottoinsieme autorizzato* B *determina univocamente il valore segreto di* k*.)*

- *Per ogni sottoinsieme non autorizzato di partecipanti* $B \subseteq P$ *e per ogni distribuzione di share* $g_B \in S(B)$ *si ha che*

  $$p_K(k|_{g_B}) = p_K(k)$$

  $\forall k \in K$*. (Ciò significa che la distribuzione di probabilità condizionata su* K*, data una distribuzione di share* $g|_B$ *per un sottoinsieme* B *non autorizzato, è la stessa distribuzione di probabilità su* K*. In altre parole la distribuzione di share a* B *non fornisce nessuna informazione sul valore della chiave.)*

3.2 Tasso di Informazione

Si può dimostrare (vedi [1], paragrafo 13, 2.1) che ogni struttura d'accesso monotona può essere realizzata da un SSS perfetto. Per quanto riguarda l'efficenza di uno schema di condivisione di segreti, può essere misurata attraverso il tasso di informazione.

Definizione 7. *Supponiamo di avere uno schema di condivisione dei segreti perfetto che realizza una struttura d'accesso* Γ*. Il* ***tasso d'informazione*** *per* P_i *è il seguente:*

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

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

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

Fino a che la chiave k deriva da un insieme finito di chiavi K, possiamo pensare di rappresentarla come una stringa di bit lunga $\log_2 |k|$, usando il codice binario per esempio. Allo stesso modo, le share date ai P_i sono rappresentate da stringhe di bit lunghe $\log_2 |S(P_i)|$. Intuitivamente, P_i riceve $\log_2 |S(P_i)|$ bit di informazioni, ma le informazioni contenute nella chiave sono $\log_2 |k|$ bit. Perciò ρ_i è il rapporto tra il numero di bit della share e il numero di bit della chiave.

Osservando lo schema a soglia di Shamir si nota che ha tasso d'informazione $\rho = 1$, che mostreremo essere il valore ottimale.

Teorema 2. *In ogni schema di condivisione di segreti perfetto che realizza una struttura d'accesso* Γ*,* $\rho \leq 1$*.*

Dimostrazione. Supponiamo di avere un SSS perfetto che realizza la struttura d'accesso Γ. Sia $B \in \Gamma_0$ e $P_j \in B$. Definiamo $B' = B \setminus \{Pj\}$. Sia $g \in S(B)$.
Ora, $B' \notin \Gamma$, cosí la distribuzione di share $g|_{B'}$, non fornisce alcuna informazione riguardo la chiave. Quindi, per ogni $k \in K$, c'è una regola di distribuzione $g^k \in F_K$ tale che $g^k|_{B'} = g|_{B'}$. Poichè $B \in \Gamma$ dev'essere che $g^k(P_j) \neq g^{k'}(P_j)$ se $k \neq k'$. Quindi

$$|S(P_j)| \geq |k|, \text{e } \rho_j \leq 1 \Longrightarrow \rho \leq 1$$

. □

Quando $\rho = 1$ si ha una situazione ottimale. Pertanto uno schema con tale tasso viene detto **ideale**. Lo schema a soglia di Shamir è uno schema ideale.

3.2.1 Esempio

Supponiamo che $P = \{P_1, P_2, P_3, P_4\}$ e $\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$.
Sia m un numero intero e supponiamo $k \in Z_m$. Il Dealer sceglie cinque valori (share) in Z_m, a_1, a_2, b_1, b_2, c_1, e li distribuisce nel seguente modo:

$$P_1 \leftarrow (a_1, b_1)$$

$$P_2 \leftarrow (a_2, c_1)$$

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

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

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 k.
Il sottoinsieme $\{P_1, P_2, P_4\}$ calcola:

$$k = a_1 + a_2 + (k - a_1 - a_2) \mod m$$

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

$$k = b_1 + b_2 + (k - b_1 - b_2) \mod m$$

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

$$k = c_1 + (k - c_1) \mod m$$

Abbiamo visto che ogni sottoinsieme autorizzato può calcolare k, 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 k, vediamo che neanche B, può calcolare k.

Definizione 8. *Un sottoinsieme $B \subseteq P$ è un* ***sottoinsieme non autorizzato massimale*** *se dato $B_j \in \Gamma$, $\forall B_j \supseteq B$ risulta che $B_j \neq B$.*

Allora è sufficente dimostrare che nessuno dei sottoinsiemi massimali non autorizzati può determinare informazioni su k. 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 k non può essere calcolato, perchè alcune parte di informazioni 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:

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

Poichè i valori di a_1, a_2, b_1, c_1 sono casuali e non conosciuti, k non può essere calcolato. Un sottoinsieme non autorizzato non ha nessuna informazione sul valore di k. Il tasso di informazione per questa struttura è:

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

3.2.2 Entropia sul tasso di informazione

Denotiamo con

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

il massimo tasso d'informazione per un SSS perfetto che realizza una specifica struttura d'accesso Γ. L'entropia 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 sulle chiavi k, l'entropia di questa distribuzione di probabilità è denotata $H(K)$. 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 K, induce una distribuzione di probabilità sulla lista delle share assegnate ai partecipanti in B. Denoteremo questa distribuzione di probabilità con con $p_S(B)$ e l'entropia di questa distribuzione di probabilità come $H(B)$. Diamo ora un'altra definizione di un SSS perfetto in termini di entropia, ma equivalente a quelle precedenti:

Definizione 9. *Supponiamo che Γ sia una struttura d'accesso ed F un insieme di regole di distribuzione. Allora F è un SSS perfetto che realizza la struttura d'accesso Γ, se soddisfa le seguenti proprietà:*

- *Per ogni sottoinsieme autorizzato di partecipanti $B \subseteq P$, $H(K|B) = 0$*
- *Per ogni sottoinsieme di partecipanti non autorizzato $B \subseteq P$, $H(K|B) = H(K)$*

Questa definizione spiega perchè lo schema a soglia di Blakley non è uno schema di condivisione di segreti perfetto. Infatti se un sottogruppo di utenti non autorizzato, (in uno schema a soglia (t, w) possono essere $t-1$ utenti) unisce le proprie share, l'incertezza sull'informazione segreta k diminuisce rispetto a quella di un sottogruppo di $1, 2, ..., t-2$ partecipanti.

Richiamiamo ora alcuni risultati sull'entropia:

Lemma 1. *Siano X, Y e Z variabili random. Allora seguono i risultati seguenti:*

$$\begin{aligned}
H(X,Y) &= H(X|Y) + H(Y) && (3.1)\\
H(X,Y|Z) &= H(X|Y,Z) + H(Y|Z) && (3.2)\\
H(X,Y|Z) &= H(Y|X,Z) + H(X|Z) && (3.3)\\
H(X|Y) &\geq 0 && (3.4)\\
H(X|Z) &\geq H(X|Y,Z) && (3.5)\\
H(X,Y|Z) &\geq H(Y|Z) && (3.6)
\end{aligned}$$

Lemma 2. *Supponiamo* Γ *una struttura d'accesso e* F *un insieme di regole di distribuzione che realizzano* Γ*. Sia* $B \notin \Gamma$ *e* $A \cup B \in \Gamma$*, dove* $A, B \subseteq P$*. Allora:*

$$H(A|B) = H(K) + H(A|B, K).$$

Lemma 3. *Supponiamo* Γ *una struttura d'accesso e* F *un insieme di regole di distribuzione che realizzano* Γ *e* $A \cup B \in \Gamma$*, dove* $A, B \subseteq P$*. Allora:*

$$H(A|B) = H(A|B, K).$$

Il prossimo teorema permette di stabilire un limite per il tasso d'informazione di certe strutture.

Teorema 3. *Supponiamo* Γ *una struttura d'accesso tale che:*

$$\{W, X\}, \{X, Y\}, \{W, Y, Z\} \in \Gamma$$

e

$$\{W, Y\}, \{X\}, \{W, Z\} \notin \Gamma.$$

Sia F *un SSS perfetto che realizza* Γ*. Allora:*

$$H(XY) \geq 3H(K)$$

Dimostrazione. Dai risultati precedenti avremo:

$$\begin{array}{rll}
H(K) & = H(Y|W,Z) - H(Y|W,Z,K) & \text{dal Lemma 2.} \\
& \leq H(Y|W,Z) & \text{da (4.4)} \\
& \leq H(Y|W) & \text{da (4.5)} \\
& = H(Y|W,K) & \text{dal Lemma 3.} \\
& \leq H(X,Y|W,K) & \text{da (4.6)} \\
& = H(X|W,K) + H(Y|W,X,K) & \text{da(4.2)} \\
& \leq H(X|W,K) + H(Y|X,K) & \text{da (4.5)} \\
& = H(X|W) - H(K) + H(Y|X) - H(K) & \text{dal Lemma 2.} \\
& \leq H(X) - H(K) + H(Y|X) - H(K) & \text{da (4.4)} \\
& = H(X,Y) - 2H(K) & \text{da(4.1)}
\end{array}$$

Da cui la conclusione $H(XY) \geq 3H(K)$ □

Corollario 1. *Supponiamo che* Γ *sia una struttura d'accesso che soddisfa le ipotesi del teorema precedente. Supponiamo inoltre che le chiavi siano tutte equiprobabili, allora*

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

Dimostrazione. Poichè le chiavi sono equiprobabili:

$$H(K) = \log_2 |K|.$$

Inoltre sappiamo che:

$$\begin{aligned} H(X,Y) &\leq H(X) + H(Y) \\ &\leq \log_2 |S(X)| + \log_2 |S(Y)|. \end{aligned}$$

Dal teorema precedente abbiamo: $H(XY) \geq 3H(K)$.
Allora ne segue:

$$\log_2 |S(X)| + \log_2 |S(Y)| \geq 3 \log_2 |K|.$$

Ora dalla definizione di tasso di informazione abbiamo:

$$\rho \leq \frac{\log_2 |K|}{\log_2 |S(X)|}$$

e

$$\rho \leq \frac{\log_2 |K|}{\log_2 |S(Y)|}$$

Allora ne segue:

$$\begin{aligned} 3 \log_2 |K| &\leq \log_2 |S(X)| + \log_2 |S(Y)| \\ &\leq \frac{\log_2 |K|}{\rho} + \frac{\log_2 |K|}{\rho} \\ &= 2\frac{\log_2 |K|}{\rho} \end{aligned}$$

Quindi $\rho \leq \frac{2}{3}$ □

Dunque lo schema descritto nel **Teorema 3.** non è ideale.

Appendice A

Matrice di Vandermonde

La matrice di Vandermonde è la matrice le cui righe (o colonne) hanno elementi, a partire da 1, in progressione geometrica: $a_{i,j} = \alpha_i^{j-1}$ oppure la trasposta $a_{i,j} = \alpha_j^{i-1}$.

$$\mathbf{V} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \dots & \alpha_m^{n-1} \end{pmatrix}$$

Teorema 4. *Una matrice quadrata di Vandermonde di ordine n ha determinante:*

$$det(V) = \prod_{1 \le i \le j \le n} (\alpha_j - \alpha_i)$$

La dimostrazione si può vedere sia per induzione sull'ordine di n oppure utilizzando la formula di Leibniz.

Dimostrazione. Per induzione vale per $n = 1$, supponiamolo vero per $n - 1$, il determinante di una matrice di ordine n può essere calcolato:

- sottraendo ad ogni colonna la colonna precedente moltiplicata per α_1

$$\mathbf{det}(\mathbf{V}) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2(\alpha_2 - \alpha_1) & \dots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ 1 & \alpha_3 - \alpha_1 & \alpha_3(\alpha_3 - \alpha_1) & \dots & \alpha_3^{n-2}(\alpha_3 - \alpha_1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n - \alpha_1 & \alpha_n(\alpha_n - \alpha_1) & \dots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{pmatrix}$$

- dividendo ogni riga j-esima (tranne la prima) per il termine $\alpha_j - \alpha_1$, portandolo fuori dalla matrice

$$\mathbf{det}(\mathbf{V}) = det \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ (\alpha_2 - \alpha_1)^{-1} & 1 & \alpha_2 & \dots & \alpha_2^{n-2} \\ (\alpha_3 - \alpha_1)^{-1} & 1 & \alpha_3 & \dots & \alpha_3^{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (\alpha_n - \alpha_1) & 1 & \alpha_n & \dots & \alpha_n^{n-2} \end{pmatrix} \prod_{j=2}^{n} (\alpha_j - \alpha_1) =$$

$$= det \begin{pmatrix} 1 & \alpha_2 & \dots & \alpha_2^{n-2} \\ 1 & \alpha_3 & \dots & \alpha_3^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-2} \end{pmatrix} \prod_{j=2}^{n} (\alpha_j - \alpha_1)$$

- infine applicando la formula del determinante per una matrice di Vandermonde di ordine $n-1$

$$det(V) = \left(\prod_{2 \le i < j \le n} (\alpha_j - \alpha_i) \right) \left(\prod_{1 = i < j \le n} (\alpha_j - \alpha_i) \right) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$$

□

Una dimostrazione alternativa invece potrebbe essere la seguente:

Dimostrazione. Il determinante di V è un polinomio sui coefficenti $\alpha_1, ..., \alpha_n$, e si annulla quando due righe sono uguali, ovvero quando $\alpha_j = \alpha_i$ con $i \neq j$. Ne consegue che il determinante è pari a un polinomio

$$P(\alpha_1, ..., \alpha_n) \text{ moltiplicato per } \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i);$$

secondo la classica formula di Leibniz, il grado del determinante su ogni variabile è $n-1$, quindi il polinomio P è una costante P_n.
Che questa costante sia esattamente 1 si può dimostrare per induzione, confrontando i coefficenti di $\alpha_{n,n} - 1$ ottenuti secondo la formula del determinante e secondo l'ipotesi induttiva. □

Scrivendo il determinante della matrice in questo modo ne segue:

Corollario 2. *Le matrici quadrate di Vandermonde hanno determinante nullo se e solo se hanno due coefficenti uguali $\alpha_i = \alpha_j$ con $i \neq j$, ovvero due righe uguali. In particolare, il rango di una generica matrice di Vandermonde è il minimo tra il numero di colonne e il numero di distinti coefficenti α_i (ovvero di righe distinte).*

Appendice B

Interpolazione di Lagrange

L'interpolazione di Lagrange è utilizzata per interpolare funzioni o dati ritenuti senza errore. Supponiamo di volere interpolare $n+1$ punti (x_i, y_i) con $i = 0, 1, 2, ..., n$ con un polinomio $P_n(x)$ di grado n:

$$P_n(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... = \sum_{i=0}^{n} a_i x^i$$

Il polinomio $P_n(x)$ ha $n+1$ coefficenti a_k. Interpolare un polinomio su un insieme di punti significa che il polinomio dovrà passare attraverso tutti questi punti (x_i, y_i) e questo implica, per ciascun punto x_i, la condizione:

$$P_n(x_i) = y_i.$$

Tale condizione su $n+1$ punti determina un sistema di $n+1$ equazioni:

$$P_n(x_0) = y_0$$

$$P_n(x_1) = y_1$$

$$...$$

$$P_n(x_n) = y_n$$

la cui soluzione a_k consente di determinare il polinomio $P_n(x)$. In forma matriciale il sistema di equazioni $Va = y$ si scrive:

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Il problema ha un' unica soluzione se la matrice non è singolare, cioè se il $det(V)$ è diverso da zero. Ma V è una matrice di Vandermonde e sarà singolare se ha due righe uguali, cioè se $x_i = x_j$ con $i \neq j$. In generale il determinante si può esprimere come

$$det(V) = \prod_{1 \leq i \leq j \leq n} (x_i - x_j).$$

Il sistema può presentare difficoltà se lo si risolve con i metodi tradizionali, Lagrange presenta un metodo alternativo, basato sul fatto che se ha soluzione questa è unica. Proviamo allora a costruire le soluzioni utilizzando un polinomio ausiliario $l_i(x)$ di grado n con le proprietà:

$$l_i(x_j) = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

La soluzione cercata si può esprimere come:

$$P_n(x) = \sum_{i=0}^{n} l_i(x) y_i$$

Si tratta quindi di costruire adeguatamente i polinomi $l_i(x)$. La condizione $l_i(x_j) = 0$ per $i \neq j$ si può semplicemente soddisfare con la scelta:

$$l_i(x) \propto \prod_{j=0; j \neq i}^{n} (x - x_j)$$

Con la condizione $l_i(x_i) = 1$ il polinomio deve essere normalizzato e perciò:

$$l_i(x) = \frac{\prod_{j=0; i \neq j}^{n} (x - x_j)}{\prod_{j=0; i \neq j}^{n} (x_i - x_j)}$$

Si ha quindi:

$$P_n(x) = \sum_{i=0}^{n} l_i(x) y_i$$

con

$$l_i(x) = \prod_{j=0; j \neq i}^{n} \frac{(x - x_j)}{(x_i - x_j)}$$

Poichè la soluzione è unica il polinomio è lo stesso che sarebbe risultato dalla soluzione dell'equazione matriciale.

Teorema 5 (Formula di interpolazione di Lagrange)**.**
Supponiamo p primo, $x_1, ..., x_{n+1}$ elementi distinti di Z_p e $a_1, ..., a_{n+1}$ elementi non necessariamente distinti di Z_p. Allora esiste un unico polinomio $A(x) \in Z_p[x]$ con grado massimo m, tale che $A(x_i) = a_i$, $1 \leq i \leq n+1$.
Il polinomio $A(x)$ è il seguente:

$$A(x) = \sum_{j=1}^{n+1} \left(a_j \prod_{1 \leq h \leq n+1, h \neq j} \frac{x - x_h}{x_j - x_h} \right)$$

La formula di interpolazione di Lagrange esiste anche in forma di due variabili:

Teorema 6 (Formula di interpolazione di Lagrange in due variabili)**.**
Supponiamo p primo, $x_1, ..., x_{n+1}$ elementi distinti di Z_p e $a_1, ..., a_{n+1} \in Z_p[x]$ sono polinomi di grado massimo n. Allora esiste un unico polinomio $A(x, y) \in Z_p[x, y]$ che ha grado massimo n (in x e y), tale che $A(x, y_i) = a_i(x)$, $1 \leq i \leq n+1$.
Il polinomio $A(x, y)$ è il seguente:

$$A(x, y) = \sum_{j=1}^{n+1} \left(a_j(x) \prod_{1 \leq h \leq n+1, h \neq j} \frac{y - y_h}{y_j - y_h} \right)$$

Bibliografia

[1] Douglas R. Stinson, Cryptography: Theory and Practise, Third Edition, Chapman&Hall/CRC, Boca Raton, 2005.

[2] Tal Rabin, Michael Ben-Or, *Verifiable Secret Sharing and Multiparty Protocols with Honest Majority*(extended abstract), Institute of Mathematics and Computer Science, The Hebrew University, Jerusalem, Israel, 1989.

[3] Russ Martin, *Introduction to Secret Sharing Schemes*, www.cs.rit.edu/∼rfm6038/Paper.pdf

[4] Pablo Azar, *Secret Sharing and Applications*, Harvard University, 2009, *thehcmr.org/issue*2_1/*secret_sharing.pdf*.

[5] John Johnson,*Construction of a Secret Sharing Scheme with Multiple Extra Functionalities*, Department of Computer Science, University of British Columbia, 2003.

[6] Srivatsan Narayanan, Ananth Raghunathan, and Pandu Rangan,*Lower Bounds for Round and Communication Complexities of Unconditional Verifiable Secret Sharing*, Dept. of Computer Science and Engineering, Indian Institute of Technology Madras.

[7] C. Shannon, A mathematical theory of communication, *Bell Systems Technical Journal,* 27 (1948),pp. 379-423, pp. 623-656.