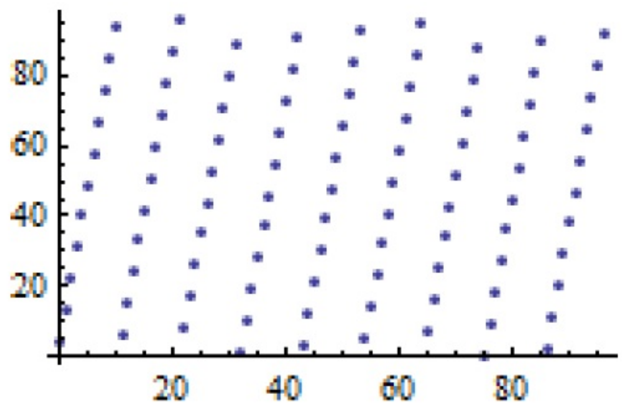
Schemi per la condivisione di segreti
(Secret sharing scheme)

Polinomi su $\mathbb{Z}_p$



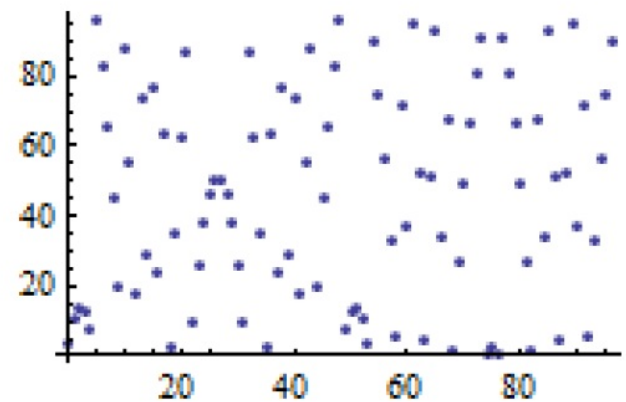


Grafico di una retta (mod 97)

Grafico di una parabola (mod 97)

Matematicamente si comportano come i polinomi sui reali

Un polinomio di grado d ha al più d radici

Un polinomio di grado $d-1$ è univocamente determinato

da d punti distinti $\quad x_i \neq x_j \, , \quad i \neq j$

$$(x_0, f(x_0)) \quad \dots \quad (x_{d-1}, f(x_{d-1})) \qquad f(x) = a_0 + a_1 x + \dots + a_{d-1} x^{d-1}$$

Matrice di Vandermonde (non singolare)

$$\begin{pmatrix} 1 & x_0 & \dots & x_0^{d-1} \\ 1 & x_1 & \dots & x_1^{d-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{d-1} & \dots & x_{d-1}^{d-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} = \begin{pmatrix} f(x_0) \\ f(x_1) \\ \vdots \\ f(x_{d-1}) \end{pmatrix}$$

$\exists !$ soluzione

nota dati gli x_i | incognite | noti

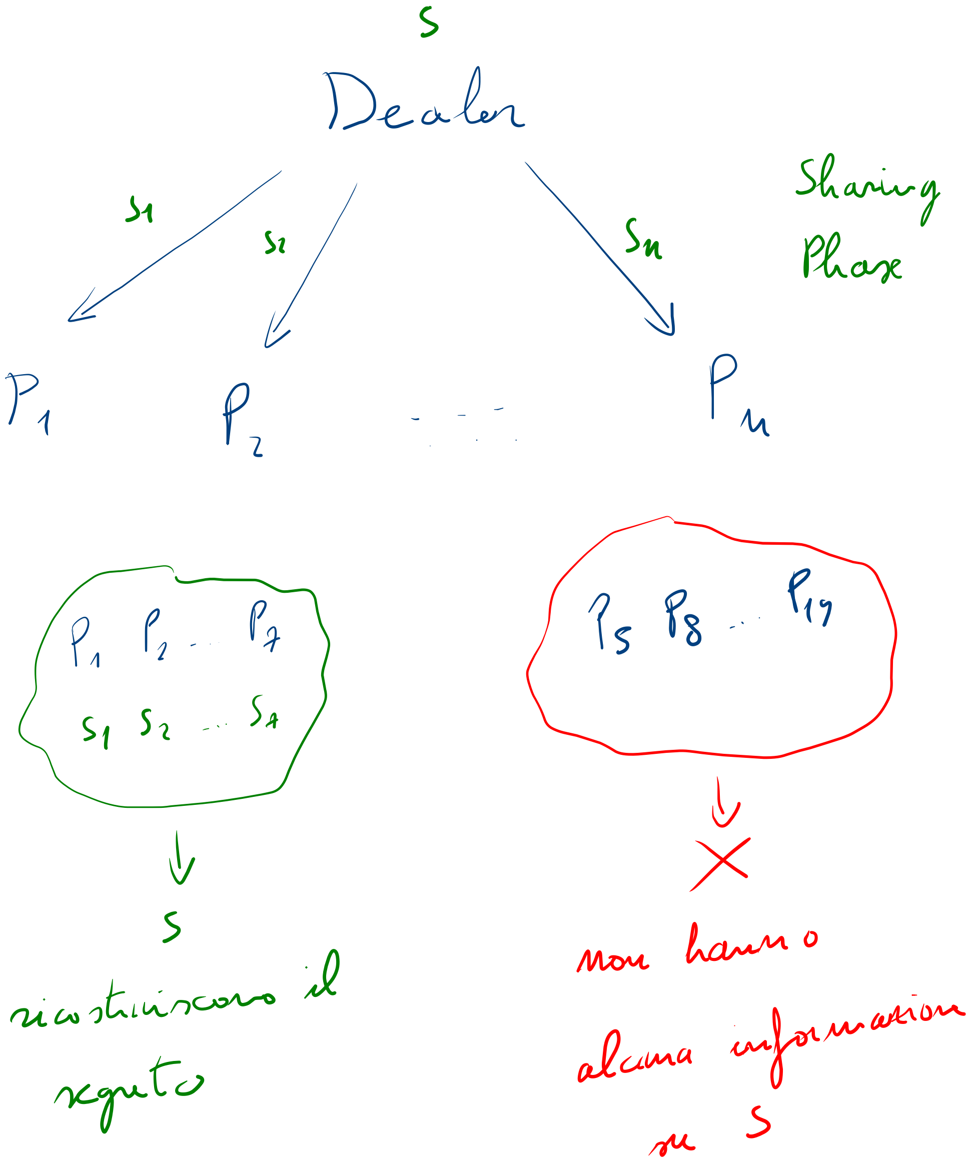
Come ricorderete, il polinomio interpolante può essere anche calcolato più efficientemente ed espresso attraverso la formula di Lagrange

$$f(x) = \sum_{i=0}^{d-1} f(x_i) \cdot L_i(x)$$

dove $\quad L_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{d-1} \frac{(x - x_j)}{(x_i - x_j)} \qquad x_i \neq x_j, \ \forall i \neq j$

Nota: $\quad L_i(x_i) = 1 \quad$ e $\quad L_t(x_i) = 0 \quad \forall t \neq i$

$\Rightarrow \quad f(x)$ vale esattamente $f(x_i)$ in ognuno degli x_i.



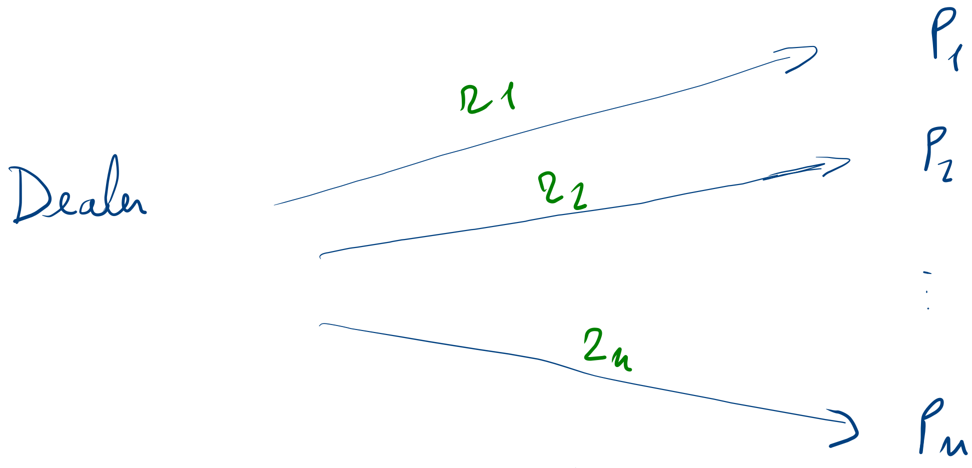
Il dealer vuole condividere un segreto S con gli n partecipanti in modo tale che

- sottoinsiemi qualificati ricostruiscano S
- sottoinsiemi proibiti non abbiano alcuna informazione su S

La Reconstruction Phase può essere condotta o dai partecipanti o tramite un combiner

Warm up

$s \in \{0,1\}^n$ stringa di n bit



$r_i \in_R \{0,1\}^n$

$i = 1, \dots, n-1$

$r_n = r_1 \oplus \dots \oplus r_{n-1} \oplus s$

Quando tutti i partecipanti mettono assieme le proprie share

$$s = \underset{P_1}{r_1} \oplus \underset{P_2}{r_2} \oplus \dots \oplus \underset{P_{n-1}}{r_{n-1}} \oplus \underbrace{(r_1 \oplus r_2 \oplus \dots \oplus r_{n-1} \oplus s)}_{P_n}$$

D'altra parte, qualsiasi sottoinsieme di partecipanti non ha alcuna informazione su S

- o i partecipanti dispongono di valori totalmente casuali, se P_n non è presente $\Rightarrow$ NO INFO

- oppure, se P_n è presente, manca almeno un z_i per "rimuovere la maschera" ad z_n e liberare S. Ma essendo $z_i \in_R \{0,1\}^n$, il segreto S può ancora essere qualsiasi valore in $\{0,1\}^n$ con prob. uniforme. $\Rightarrow$ NO INFO

Nota: lo schema può essere facilmente riprodotto in altri gruppi al posto di $(\{0,1\}^n, \oplus)$

e.g. $(\mathbb{Z}_n, +_n)$

Nella forma più generale, gli insiemi qualificati e proibiti di partecipanti definiscono una "struttura d'accesso" al segreto

$$\mathcal{A} = (Q, F) \quad \text{su} \quad P = \{1, 2, \dots n\}$$

Struttura d'accesso — Famiglia di insiemi qualificati — Famiglia di insiemi proibiti — insieme di partecipanti

Le strutture d'accesso di interesse sono quelle monotone

$$A \in Q \,, \quad A \subset B \implies B \in Q$$

I partecipanti in B possono sempre ricostruire usando solo quelli anche in A

Lo schema di Shamir

realizza una struttura d'accesso a soglia

$$Q = \{ S \subseteq \{1, \dots, n\} : |S| \geq t \}$$

Ogni sottoinsieme di almeno t partecipanti ricostruisce

$$F = \{ S \subseteq \{1, \dots, n\} : |S| < t \}$$

Ogni sottoinsieme di t-1 o meno partecipanti non ottiene alcuna informazione

Schema a soglia (t, n)

Sia $s \in \mathbb{Z}_p$ $(p$ primo, $p > n)$ ← devo avere almeno n punti distinti

Sharing Phase. Il Dealer sceglie unif. a caso un polinomio $a(x)$ di grado al più $t-1$, tale che $a(0) = s$. $\left\{ \begin{array}{l} a_0 = s \\ a_i \in_R \mathbb{Z}_p \end{array} \right.$

Per $i = 1, \dots, n$, invia $s_i = a(i)$ al partecipante P_i

Reconstruction Phase. Ogni sottoinsieme di t partecipanti Q ricostruisce il segreto dalle proprie share, usando l'interpolazione di Lagrange

Nota: non ricostruisco $a(x)$. Calcolo direttamente il suo valore in 0, i.e., $a(0)$.

$$s = \sum_{i \in Q} s_i \cdot \lambda_{Q,i} \qquad \lambda_{Q,i} = \prod_{j \in Q \setminus \{i\}} \frac{j}{j-i}$$

Correttezza. L'interpolazione di Lagrange garantisce che ogni sottoinsieme qualificato ricostruisca.

Sicurezza. Cosa garantisce che un sottoinsieme di al più $t-1$ partecipanti non ottiene alcuna info su $a(0)$?

Senza perdita di generalità, consideriamo $\{P_1 \dots P_{t-1}\}$

$$a(0)=s_0 \longrightarrow \qquad t\left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1^{t-1} \\ 1 & 2 & \cdots & 2^{t-1} \\ \vdots & & & \\ 1 & t-1 & & (t-1)^{t-1} \end{pmatrix}}^{t} \right. \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix}$$

Per ogni scelta di $s_0 \in \mathbb{Z}_p$ il sistema ammette un'unica soluzione

$\Downarrow$

Poiché i coefficienti $a_1, \dots a_{t-1}$ sono scelti unif. a caso $\Longleftarrow$

ogni valore di s_0 è equamente probabile.

Osservazione: lo schema iniziale è uno schema a soglia (n, n)

Può essere esteso per realizzare un (t, n)

- per ogni sottoinsieme di t partecipanti si usa uno schema (t, t) INDIPENDENTE DAGLI ALTRI

Inefficiente: P_i appartiene a $\binom{n-1}{t-1}$ sottoinsieme

e riceve $\binom{n-1}{t-1}$ share, una per sottoinsieme

Shamir dà una share a P_i!

Lo schema iniziale è utile per realizzare però strutture d'accesso generali (quando non sappiamo far meglio...)