Schemi democratici di secret sharing da ipersuperfici su campi finiti

CrypTO Conference
Torino, 25-26 Maggio 2023

M. Ceria; con A. Aguglia e L. Giuzzi

Secret sharing

Secret sharing: procedura crittografica per la gestione dell'accesso ad un segreto da parte di un gruppo di persone.

I partecipanti, membri di questo gruppo, posseggono una **parte del segreto** detta **share**.

Come ricostruire il segreto? I partecipanti devono combinare i loro shares.

Secret sharing

Come ricostruire il segreto? I partecipanti devono combinare i loro shares.

Ma... va bene un gruppo qualsiasi per trovare il segreto?

No no, solo qualche gruppo deputato può ritrovare il segreto: gli **access set**.

Access structure: insieme degli access set minimali per inclusione.

Esempi

Supponiamo di avere un segreto q-ario s, con q potenza di un primo.

$(n, m)_q$ threshold secret sharing scheme

Segreto diviso in n shares distribuiti a n partecipanti.

Se m partecipanti combinano gli share possono ottenere s, ma se ci provano in $m - 1$ o meno, non solo non trovano s ma non hanno su di esso alcuna informazione.

Secret sharing

Possiamo costruire degli schemi di secret sharing a partire da **codici lineari** .

E quindi parliamo di teoria dei codici!!!

Codici lineari

Notation

$\mathbb{F}_q$: campo finito di cardinalità q
$\mathbb{F}_q^n$: spazio vettoriale n-dimensionale su $\mathbb{F}_q$.
Codice (n, M) **su** $\mathbb{F}_q$: $C \subseteq \mathbb{F}_q^n$ di cardinalità M.
Se C **sottospazio** di $\mathbb{F}_q^n$, si tratta di un **codice lineare**; se $\dim_{\mathbb{F}_q}(C) = k$ allora C è un codice lineare $[n, k]$.

Come rappresentare C?

- **Matrice Generatrice**: matrice $k \times n$ G t.c. righe $=$ base per C.
- **Parity-check** : matrice $(n - k) \times n$ che chiamiamo H t.c.

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid H\mathbf{x}^T = \mathbf{0}\}$$

Codice duale di C: codice $C^\perp$ cui generatrice è H.

Secret sharing da codici

Segreto: la prima componente di una parola.
Shares: le altre componenti della parola

Esempio di Massey

$q = 2^m$, $n = 5, k = 3$; parity-check $H := \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$.

Parola $(v_1, ..., v_5)$; segreto v_1, mentre i partecipanti A, B, C, D ottengono $A \leftarrow v_2$, $B \leftarrow v_3$, $C \leftarrow v_4$ e $D \leftarrow v_5$.

$v_1 + v_2 + v_3 = 0 = v_2 + v_4 + v_5$ e quindi anche

$v_1 + v_3 + v_4 + v_5 = 0$.

Access structure: $\{\{A, B\}, \{B, C, D\}\}$.

Parole minimali

C codice di lunghezza n. Per ogni parola $\mathbf{c} \in C$ e $1 \leq i \leq n$ il **supporto** di $\mathbf{c}$ è l'insieme $\mathrm{supp}(\mathbf{c}) := \{i : c_i \neq 0\}$ posizioni con componenti non nulle.

$\mathbf{c}, \mathbf{c}' \in C$ diciamo che $\mathbf{c}' \preccurlyeq \mathbf{c}$ se $\mathrm{supp}(\mathbf{c}') \subseteq \mathrm{supp}(\mathbf{c})$. E $\mathbf{c}$ è **minimale** per C se $\mathbf{c}' \preccurlyeq \mathbf{c}$ implica che esiste $\alpha \in \mathbb{F}_q$ t.c. $\mathbf{c}' = \alpha\mathbf{c}$.

Ogni parola di C è una combinazione lineare di parole minimali.

Parole minimali e secret sharing

Sia G una matrice generatrice di un codice $[n, k; q]$, C Nel SSS basato su C, un insieme di shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determina il segreto se e solo se esiste una parola

$$\mathbf{c} = (1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$$

nel **codice duale** $C^{\perp}$ con $c_{i_j} \neq 0$ per almeno un j,
$1 \leq i_1 < \ldots < i_m \leq n - 1$ and $1 \leq m \leq n - 1$.

Parole minimali e secret sharing

Se esiste una parola come $\mathbf{c}$ in $C^{\perp}$, il vettore

$$g_0 = \sum_{j=1,\ldots,m} x_j g_j$$

con $x_j \in \mathbb{F}_q$, $1 \leq j \leq m$. E allora il segreto s si trova calcolando

$$s = \sum_{j=1,\ldots,m} x_j t_{i_j}$$

Torniamo all'esempio di Massey

$q = 2^m$, $n = 5, k = 3$; matrice parity-check

$$H := \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Parola: $(v_1, ..., v_5)$; segreto v_1, e i partecipanti A, B, C, D ottengono $A \leftarrow v_2$, $B \leftarrow v_3$, $C \leftarrow v_4$ and $D \leftarrow v_5$.

$v_1 + v_2 + v_3 = 0 = v_2 + v_4 + v_5$ quindi $v_1 + v_3 + v_4 + v_5 = 0$.

Il codice duale si deduce facilmente usando H che lo genera.
Le parole minimali sono $\mathbf{c} = (1, 1, 1, 0, 0)$, $\mathbf{c}' = (1, 0, 1, 1, 1)$, e quindi la struttura d'accesso è $\{\{A, B\}, \{B, C, D\}\}$.

Difficile trovare le parole minimali!

E' **difficile** trovare l'insieme di tutte le parole minimali di un codice lineare arbitrario su di un campo finito.

La difficoltà si traduce nella difficolta di trovare strutture di accesso che siano buone.

Buone?

Ci interessano **schemi di secret sharing democratici**, dove ogni partecipante è coinvolto nello stesso numero di access set minimali.

Possiamo fare qualcosa di buono con i codici proiettivi.

Codici proiettivi

Un **sistema proiettivo** $[n, r+1]_q$ è una collezione V di n punti non necessariamente distinti nello spazio proiettivo $\mathrm{PG}(r, q)$ su $\mathbb{F}_q$.

Prendiamo un sistema di riferimento in $\mathrm{PG}(r, q)$, con coordinate omogenee $(X_0, X_1, \ldots, X_r)$, e costruiamo una matrice G prendendo, come colonne, le coordinate dei punti di V, normalizzati.
Il codice $C(V)$ che ha G come generatrice si chiama **codice generato a partire da** V.

Codici proiettivi

Lo spettro delle intersezioni di V con gli iperpiani di $\mathrm{PG}(r,q)$ ci dà la lista dei pesi del codice associato; gli **higher weights** di $C(V)$ sono dati da

$$d_k(C) = n - \max\{|V \cap \pi| : \pi \textbf{ sottosp. proiett di codim. k in } \mathrm{PG}(r,q)\}$$

$d_1(C(V))$ è la minima distanza di $C(V)$.

Condizione sufficiente affinché un codice lineare C di parametri $[n,k]$ su $\mathbb{F}_q$ sia minimale:

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}, \tag{1}$$

con $w_{\min}$ e $w_{\max}$ peso minimo e massimo di una parola non nulla di C.

Varietà Hermitiane e quasi Hermitiane

Correlazione di geometria proiettiva: bijezione dei sottospazi che rovescia l'inclusione.
Polarità: correlazione di ordine 2 (Hermitiana se associata ad una forma sesquilineare Hermitiana).

Varietà Hermitiana

Una varietà Hermitiana non singolare $H(r, q^2)$ in $\mathrm{PG}(r, q^2)$ è l'insieme di punti assoluti di una polarità Hermitiana di $\mathrm{PG}(r, q^2)$.

Varietà Quasi-Hermitiana

insieme di punti con stessa cardinalità e numeri di intersezione con gli iperpiani rispetto ad una varietà Hermitiana.

Il nostro codice proiettivo

In $\mathrm{PG}(r, q^2)$ con coordinate omogenee $(X_0, X_1, \ldots, X_r)$, prendiamo lo spazio affine $\mathrm{AG}(r, q^2)$ cui iperpiano all'infinito Σ_∞ ha equazione $X_0 = 0$. Allora $\mathrm{AG}(r, q^2)$ ha coordinate affini $(x_1, x_2, \ldots, x_r)$ dove $x_i = X_i/X_0$ for $i \in \{1, \ldots, r\}$. Prendiamo la varietà algebrica $\mathcal{B}$ avente equazione affine

$$x_r^q - x_r + \alpha^q(x_1^{2q} + \ldots + x_{r-1}^{2q}) - \alpha(x_1^2 + \ldots + x_{r-1}^2) = (\beta^q - \beta)(x_1^{q+1} + \ldots + x_{r-1}^{q+1})$$

con $\alpha \in \mathbb{F}_{q^2}^*$, $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ e

q dispari:

$\rightarrow$ r dispari e $4\alpha^{q+1} + (\beta^q - \beta)^2 \neq 0$

$\rightarrow$ r pari e $4\alpha^{q+1} + (\beta^q - \beta)^2$ non-quadrato in $\mathbb{F}_q$;

$q > 2$ pari:

$\rightarrow$ r dispari

$\rightarrow$ r pari e $Tr(\alpha^{q+1}/(\beta^q + \beta)^2)$ nulla.

I punti di $\mathcal{B}$ formano le colonne della generatrice del nostro codice proiettivo.

Varietà Quasi-Hermitiane

Se incolliamo l'insieme dei punti affini di $\mathcal{B}$ con la varietà Hermitiana degenere

$$\mathcal{F} = \{(0, X_1, \ldots, X_r) \colon X_1^{q+1} + \cdots + X_{r-1}^{q+1} = 0\}$$

otteniamo una varietà quasi-Hermitiana $\mathcal{H} = (\mathcal{B} \cap AG(r, q^2)) \cup \mathcal{F}$.

Studiamo i numeri di intersezione di $\mathcal{B}$ con gli **iperpiani** in questo modo:

- consideriamo l'intersezione di un iperpiano Σ con $\mathcal{H}$.
- togliamo da questa intersezione i punti all'infinito contenuti in $\mathcal{F}$ ed aggiungiamo le possibili intersezioni di Σ con $\mathcal{B}_\infty := \mathcal{B} \cap \Sigma_\infty$.

Studiamo poi le intersezioni con le **rette** in $\mathrm{PG}(r, q^2)$.

Caso $r \geq 3$ e q dispari

L'ipersuperficie $\mathcal{B}$ di $\mathrm{PG}(r, q^2)$, $r \geq 3$ contiene
$q^{2r-1} + q^{r-1} + (q^{2(r-1)} - q^2)/(q^2 - 1) + 1$ punti se r dispari o
$q^{2r-1} + (q^{2(r-1)} - q^2)/(q^2 - 1) + 1$ punti se r pari.

Possibili **cardinalità di intersezione con gli iperpiani**:

- r dispari:

$$n_1 = q^2 \frac{(q^{2(r-2)} - 1)}{q^2 - 1} + q^{r-1} + 1, \qquad n_2 = q^{2r-3} - q^{r-2} + q^{r-3} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_3 = q^{2r-3} + \frac{q^{2(r-2)} - q^2}{q^2 - 1} + 1, \qquad n_4 = q^{2r-3} + q^{r-1} - q^{r-2} + q^{r-3} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_5 = q^{2r-3} + q^{r-1} + \frac{q^{2(r-2)} - q^2}{q^2 - 1} + 1;$$

- r pari:

$$n_1 = q^2 \frac{(q^{2(r-2)} - 1)}{q^2 - 1} + 1, \qquad n_2 = q^{2r-3} - q^{r-1} + q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_3 = q^{2r-3} + \frac{q^{2(r-2)} - q^2}{q^2 - 1} - q^{r-2} + 1, \qquad n_4 = q^{2r-3} + \frac{(q^{2(r-2)} - q^2)}{q^2 - 1} + 1,$$

$$n_5 = q^{2r-3} + \frac{q^{2(r-2)} - q^2}{q^2 - 1} + q^{r-2} + 1.$$

Caso $r \geq 3$ e q pari

L'ipersuperficie $\mathcal{B}$ ha $q^{2r-1} + q^{2(r-2)} + \ldots + q^2 + 1$ punti di $\mathrm{PG}(r, q^2)$ e le seguenti **cardinalità di intersezione con gli iperpiani**:

- r dispari:

$$n_1 = \frac{q^{2(r-1)} - 1}{q^2 - 1}, \qquad n_2 = q^{2r-3} - q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_3 = q^{2r-3} + \frac{q^{2(r-2)} - 1}{q^2 - 1}, \qquad n_4 = q^{2r-3} + q^{r-1} - q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_5 = q^{2r-3} + \frac{q^{2(r-1)} - 1}{q^2 - 1};$$

- r pari:

$$n_1 = \frac{q^{2(r-1)} - 1}{q^2 - 1}, \qquad n_2 = q^{2r-3} - q^{r-1} + q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_3 = q^{2r-3} + \frac{q^{2(r-2)} - 1}{q^2 - 1}, \qquad n_4 = q^{2r-3} + q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_5 = q^{2r-3} + \frac{q^{2(r-1)} - 1}{q^2 - 1}.$$

E LE RETTE?

Se intersechiamo con le rette troviamo l'higher weight della forma $d_{r-1}(C)$.

Sia ℓ una **retta** di $\mathrm{PG}(r, q^2)$. Allora le possibili cardinalità di intersezione per $\ell \cap \mathcal{B}$ sono come segue:

$$0, 1, 2, q-1, q, q+1, q+2, 2q-1, 2q, q^2+1$$

Ora che abbiamo le sezioni, possiamo studiare il **codice proiettivo** associato a $\mathcal{B}$!

Codici con 5 pesi

Sia q una potenza di primo dispari. Allora i punti di $\mathcal{B}$ in $\mathrm{PG}(r, q^2)$, $r > 3$ determinano un **codice proiettivo minimal e q-divisibile** $C(\mathcal{B})$ di lunghezza $N = q^{2r-1} + q^{r-1} + (q^{2(r-1)} - q^2)/(q^2 - 1) + 1$ per r dispari, o $N = q^{2r-1} + (q^{2(r-1)} - q^2)/(q^2 - 1) + 1$ per r pari, dimensione $r + 1$ e pesi non nulli:

- r dispari:

$$w_5 = q^{2r-1} - q^{2r-3} + q^{2(r-2)}, \qquad w_4 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-2} - q^{r-3},$$

$$w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1},$$

$$w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1} + q^{r-2} - q^{r-3}, \qquad w_1 = q^{2r-1};$$

- r pari:

$$w_5 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} - q^{r-2}, \qquad w_4 = q^{2r-1} - q^{2r-3} + q^{2(r-2)},$$

$$w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-2},$$

$$w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1} - q^{r-2}, \qquad w_1 = q^{2r-1}.$$

Codici con 5 pesi

Sia q una potenza di primo pari. Allora, i punti di $\mathcal{B}$ in $PG(r, q^2)$, $r \geq 3$ determinano un **codice proiettivo q-divisibile** $C(\mathcal{B})$ di lunghezza $N = q^{2r-1} + q^{2(r-2)} + q^{2(r-3)} + \ldots + q^2 + 1$, dimensione $r + 1$ e pesi non nulli:

- r dispari:

$$w_5 = q^{2r-1} - q^{2r-3}, \qquad w_4 = q^{2r-1} - q^{2r-3} + q^{2r-4} - q^{r-1} + q^{r-2},$$

$$w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)},$$

$$w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-2}, \qquad w_1 = q^{2r-1};$$

- r pari:

$$w_5 = q^{2r-1} - q^{2r-3}, \qquad w_4 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} - q^{r-2},$$

$$w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)},$$

$$w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1} - q^{r-2}, \qquad w_1 = q^{2r-1}.$$

Il caso $q = 3$

I punti di $\mathcal{B}$ in $\mathrm{PG}(3, q^2)$, con q potenza di primo dispari, determinano un **codice proiettivo minimale** $C(\mathcal{B})$ di lunghezza $N = q^5 + 2q^2 + 1$, pesi non nulli

$$w_1 = q^5, \quad w_2 = q^5 - q^3 + 2q^2 + q - 1, \quad w_3 = q^5 - q^3 + 2q^2,$$

$$w_4 = q^5 - q^3 + q^2 + q - 1, \quad w_5 = q^5 - q^3 + q^2,$$

e weight enumerator $w(x) := \sum_i A_i x^i$, dove

$$A_0 = 1,\ A_{w_1} = q^2 - 1,\ A_{w_2} = (q^6 - q^5 + q^3)(q^2 - 1),\ A_{w_3} = (q^4 - q^2)(q^2 - 1),$$

$$A_{w_4} = (q^5 - q^3)(q^2 - 1),\ A_{w_5} = 2q^2(q^2 - 1)$$

e tutti i restanti A_i sono 0.

Schema democratico, finalmente!

Sia $r \geq 3$ e q una potenza di primo dispari. Nello schema di secret sharing basato sul codice duale $C(\mathcal{B})^{\perp}$, ci sono q^{2r} **access sets minimali** e n participanti dove

- $n = q^{2r-1} + q^{r-1} + \frac{(q^{2(r-1)} - q^2)}{q^2 - 1}$, r dispari;
- $n = q^{2r-1} + \frac{(q^{2(r-1)} - q^2)}{q^2 - 1}$, r pari.

In aggiunta, **ogni participante** P_i, $\forall i = 1 \ldots n$, è coinvolto in esattamente $(q^2 - 1)q^{2(r-1)}$ **su** q^{2r} **access sets minimali**.

Grazie per l'attenzione!