EVOLVING SECRET SHARING:

distribuire segreti in un mondo che cambia

Scuola Ortogonale, II ciclo

GIANFRANCO VITIELLO (Università degli Studi di Salerno)

Mentore: Prof. ROBERTO DE PRISCO

IV Weekend Ortogonale, Procida 14-17 Maggio 2026

elicsir

Elevating Italian Computer Science Innovation and Research

Table of Contents

Formalizzazione

1 Concetti preliminari

Definizione

Uno schema di secret sharing Π, sull'insieme di partecipanti $\mathcal{P}_n$, e sull'insieme di segreti $\mathcal{S}$ (con $|\mathcal{S}| \geq 2$) è una coppia di algoritmi PPT *(Share,Recon)* tale che:

Share:

Input: $s \in \mathcal{S}$

Output: $sh_1, \ldots, sh_n$

Recon:

Input: $\{sh_i\}_{i \in A}$, con $A \subseteq \mathcal{P}_n$

Output: $s' \in \mathcal{S}$ tale che **correttezza** e **sicurezza** soddisfatte.

Insiemi qualificati e struttura di accesso

Un sottoinsieme di partecipanti A si dice **qualificato** se abilitato al recupero della chiave s con gli share di cui dispone; altrimenti, viene detto **non qualificato**.

Definizione

Una **struttura di accesso** $\mathcal{A} \subset 2^{\mathcal{P}_n}$ è la collezione di tutti i sottoinsiemi qualificati.

NOTA: nel seguito della trattazione verranno considerate solo strutture di accesso **monotone**.

Definizione

Per ogni segreto $s \in \mathcal{S}$ e per ogni insieme qualificato $A \in \mathcal{A}$, risulta

$$Recon(\{sh_i\}_{i \in A}) = s$$

Quanto alla proprietà di sicurezza, ci sono diverse nozioni della stessa.

Sicurezza perfetta

Per ogni sottoinsieme **non qualificato** $B \notin \mathcal{A}$ e per ogni coppia di segreti $s_1, s_2 \in \mathcal{S}$, la distribuzione di probabilità $\{sh_i^1\}_{i \in B}$ e $\{sh_i^2\}_{i \in B}$ sui corrispondenti segreti è la stessa.

Sicurezza computazionale

Per ogni sottoinsieme **non qualificato** $B \notin \mathcal{A}$ e per ogni coppia di segreti $s_1, s_2 \in \mathcal{S}$, la distribuzione di probabilità $\{sh_i^1\}_{i \in B}$ e $\{sh_i^2\}_{i \in B}$ sui corrispondenti segreti è la stessa a meno di un fattore trascurabile.

Esempio semplice: Secret-sharing additivo

Costruzione

Sia s il segreto che si vuole condividere ed sia n il numero di partecipanti. Il dealer darà al partecipante P_i lo share r_i scelto uniformemente a caso in $\mathbb{Z}$ per $i = 1, \ldots, n-1$; P_n, invece, riceverà:

$$r_n = s - \sum_{i=1}^{n-1} r_i$$

Schemi a soglia

1 Concetti preliminari

Il secret-sharing additivo non è altro che un caso specifico degli schemi a soglia, introdotti da Shamir nel 1979.

Costruzione p.1

Share: prende il input il segreto s, il numero di partecipanti n e la soglia t. Sceglie un polinomio $f(x)$ di grado $t-1$, a coefficienti in $\mathbb{Z}_p$ e tale che $f(0) = s$:

$$f(x) = s + r_1 x + r_2 x^2 + \cdots + r_{t-1} x^{t-1}$$

dove $r_1, r_2, \ldots, r_{t-1}$ sono scelti uniformemente a caso in $\mathbb{Z}_p$, con p primo sufficientemente grande. P_i riceve lo share:

$$r_i = f(i) \quad \text{per } i = 1, \ldots, n$$

Costruzione p.2

Recon: prende in input un insieme di share S. Se $|S| < t$, restituisce $\perp$; altrimenti, ricostruisce s tramite interpolazione di Lagrange:

$$s = \sum_{j=1}^{t} r_{i_j} \prod_{\substack{k=1 \\ k \neq j}}^{t} \frac{i_k}{i_k - i_j} \pmod{p}$$

Struttura di accesso generale

Nel 1996, Ito et al. dimostrarono il seguente risultato.

Teorema

Sia $\mathcal{P}_n$ un insieme di partecipanti. Per ogni $\mathcal{U} \subseteq 2^{\mathcal{P}_n}$ tale che:

$$A \in \mathcal{U}, \quad A \subseteq A' \subseteq \mathcal{P}_n \Rightarrow A' \in \mathcal{U}$$

esiste uno schema di secret-sharing con struttura di accesso $\mathcal{U}$.

Problema

1 Concetti preliminari

Domanda: come si misura l'efficienza di uno schema di secret sharing?

Risposta: rapportando la dimensione dello share massimo rispetto a quella del segreto (in bit). Idealmente, tale valore è 1.

Tipologie

Un criterio di classificazione degli schemi di secret-sharing riguarda le garanzie di sicurezza che si vogliono ottenere:

- perfectly private secret sharing;
- computationally private secret sharing;
- ramp secret sharing;
- robust secret-sharing;
- verifiable secret-sharing.

Table of Contents

Evolving access structure

Definizione informale

Una struttura di accesso in evoluzione $\mathcal{A} \subset 2^{\mathcal{P}_n}$ è una collezione (anche infinita) di sottoinsiemi di $\mathcal{P}_n$, il quale nel tempo aumenta di cardinalità.

Anche in questo scenario è possibile definire schemi a soglia.

Problema

2 Evolving secret-sharing

Domanda: se il numero di partecipanti non è noto a priori, come si può determinare l'efficienza di uno schema *evolving*?

Risposta: calcolando la dimensione dello in funzione di t (prossimo partecipante).

Strutture di accesso (k, ∞)

Komargodski et al. hanno dimostrato il seguente:

Teorema

Per ogni $k, l \in \mathbb{N}$, esiste uno schema di secret sharing per strutture di accesso evolving con soglia k e lunghezza del segreto l bit in cui per ogni $t \in \mathbb{N}$ la dimensione dello share del $t-$esimo partecipante è:

$$(k-1) \cdot \log_2 t + poly(k, l) \cdot o(\log_2 t)$$

Strutture di accesso $(2, \infty)$

Per strutture di accesso $(2, \infty)$ con $|\mathcal{S}| \geq 2$ bit, Komargodski et al. hanno provato:

Teorema (Upper Bound)

Esiste uno schema di secret sharing per strutture di accesso $(2, \infty)$ in cui la dimensione dello share del t-esimo partecipante è superiormente limitata da:

$$\log_2 t + \log_2 \log_2 t + 2 \cdot \log_2 \log_2 \log_2 t + 6$$

Inoltre, gli stessi autori hanno dimostrato un lower bound di $\log_2 t + \log_2 \log_2 t - O(1)$, rendendo la costruzione **quasi ottimale**.

Strutture di accesso $(3, \infty)$

Quindi, stando al teorema esposto poc'anzi, per schemi $(3, \infty)$ la dimensione dello share del $t-$esimo partecipante risulta:

$$2 \cdot \log_2 t + \textit{poly}(3, l) \cdot o(\log_2 t)$$

Domanda: È possibile fare di meglio?

Risposta

2 Evolving secret-sharing

Schema di secret-sharing $(3, \infty)$

Costruzione p.1

Sia s il segreto che si vuole condividere, e siano $r_i^{\{i\}}$ e $r_i^{\{i,k\}}$, per $i = 1, 2, \ldots$ e $k = 1, \ldots, i-1$ valori uniformi. I partecipanti, nel momento in cui entrano a far parte dello schema, ottengono uno share in accordo alla seguente regola di distribuzione:

Schema di secret-sharing $(3, \infty)$

Costruzione p.2

$p_1 \leftarrow r_1^{\{1\}}$

$p_2 \leftarrow r_2^{\{2\}}, r_2^{\{1,2\}}$

$p_3 \leftarrow r_1^{\{1\}} \oplus r_2^{\{1,2\}} \oplus s, \;\; r_3^{\{3\}}, \;\; r_3^{\{1,3\}}, \;\; r_3^{\{2,3\}}$

$p_4 \leftarrow r_1^{\{1\}} \oplus r_2^{\{1,2\}} \oplus s, \;\; r_1^{\{1\}} \oplus r_3^{\{1,3\}} \oplus s, \;\; r_2^{\{2\}} \oplus r_3^{\{2,3\}} \oplus s, \;\; r_4^{\{4\}}, \;\; r_4^{\{1,4\}}, \;\; r_4^{\{2,4\}}, \;\; r_4^{\{3,4\}}$

$\ldots$

$p_i \leftarrow \{r_j^{\{j\}} \oplus r_k^{\{j,k\}} \oplus s\}$, per $j < k < i$, $\;\; r_i^{\{i\}}$ e $r_i^{\{i,j\}}$, per $j < i$.

Problema

2 Evolving secret-sharing

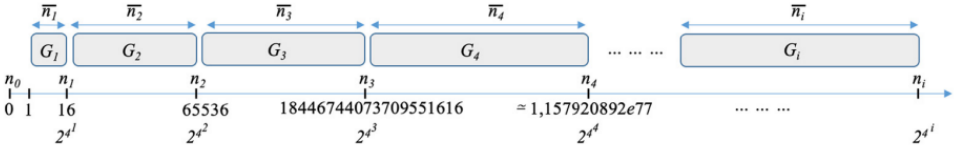
La lunghezza dello share cresce quadraticamente in base al numero di n di partecipanti: per niente efficiente.

Intuizione: usare questo schema come building block per un nuovo schema.

Idea

2 Evolving secret-sharing

Dividere i partecipanti per generazioni in base al momento in cui entrano a far parte dello schema. La generazione $i-$esima verrà indicata con G^i, per $i \geq 1$. Sia $n_0 = 0$ ed $n_i = 2^{4^i}$: la generazione G^i parte dal partecipante $n_{i-1} + 1$ e termina con il partecipante n_i. Quindi, si indicherà con $\overline{n}_i = n_i - n_{i-1}$ la cardinalità della generazione $i-$esima. Graficamente:



Proposta

2 Evolving secret-sharing

È possibile definire un nuovo schema con evolving access structure (più efficiente) basato su due schemi di secret-sharing:

- $\mathcal{S}^{\infty}$, visto poc'anzi;
- $\mathcal{S}^{i}$, schema per strutture di accesso di dimensione fissata $(3, N^{i})$, con $N^{i} = \overline{n}_{i} + 1$, per $i \geq 1$.

Schema di Asmuth-Bloom

2 Evolving secret-sharing

Costruzione

Siano p_0, p_1, p_{N^i} primi pubblici tali che $p_{N^i} \cdot \ldots \cdot p_{N^i-k} \cdot p_0 < p_1 \cdot \ldots \cdot p_k$.

Share: su input $s \in \mathbb{Z}_{p_0}$, calcola un intervallo I, sceglie uniformemente a caso α tale che $s' = \alpha \cdot s \in I$. Dà in output $sh_j = s' \mod p_j$ per $j = 1, \ldots, N^i$;

Recon: su input $\{sh_j\}_{j \in A}$, risolve

$$\begin{cases} x \equiv sh_1 \mod p_1 \\ \vdots \\ x \equiv sh_{N^i} \mod p_{N^i} \end{cases}$$

e dà in output la soluzione $s = x \mod p_0$;

Schema finale

Intuizioni fondamentali:

1. ad ogni generazione g viene associato un valore pseudocasuale RS^g;
2. per ogni generazione, si genera uno share in più da tramandare a tutti i partecipanti delle generazioni successive.

Descrizione formale

2 Evolving secret-sharing

Sia $g(n)$ la funzione di membership che su input n ne restituisce la generazione di appartenenza.

Costruzione p.1

Share: su input $s \in S$ e le stringhe casuali $RS^1, RS^2, ..., RS^{g-1}$, calcola:

- lo share sh_g^∞ usando l'algoritmo $Share$ di $\mathcal{S}^\infty$;
- gli share $sh_1^g, sh_2^g, ..., sh_{\overline{n}_g}^g, sh_E^g$ usando l'algoritmo $Share$ di $\mathcal{S}^g$;
- gli share mascherati $RS^j \oplus sh_E^g$, per $j = 1, ..., g-1$;
- una stringa casuale RS^g.

Composizione dello share

2 Evolving secret-sharing

Sia t il $t-$esimo partecipante, la cui generazione è $g = \lceil \log_4(\log t) \rceil$ e il cui indice generazionale è i. Lo share di t è costituito da cinque parti:

P1: sh_g^{∞};

P2: $sh_E^1, sh_E^2, \ldots, sh_E^{g-1}$;

P3: sh_i^g;

P4: $RS^1 \oplus sh_E^g, RS^2 \oplus sh_E^{g_j}, \ldots, RS^{g-1} \oplus sh_E^g$;

P5: RS^g.

NOTA: per $g = 1$, **P2** e **P4** assenti.

Descrizione formale

2 Evolving secret-sharing

Costruzione p.2

Recon: su input $A \subseteq \mathcal{P}_t$ restituisce un segreto $s' \in S$ in accordo alle proprietà di **correttezza** e **sicurezza**.

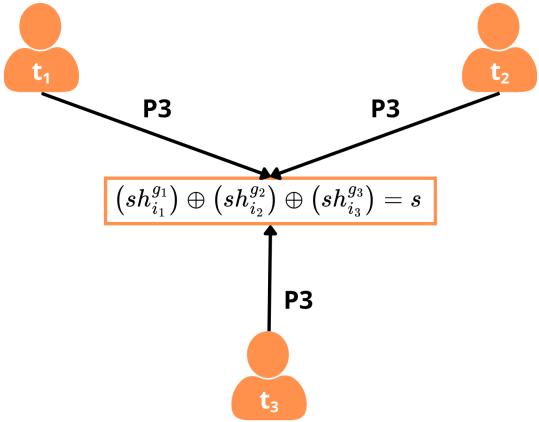
NOTA: se A è un sottoinsieme qualificato, sono possibili quattro scenari per la ricostruzione del segreto.

Ricostruzione

2 Evolving secret-sharing

Siano t_1, t_2, t_3 elementi di $\mathcal{P}_n$
Scenario 1: $g(t_1) = g(t_2) = g(t_3)$

LEGENDA:
i_1 = indice associato a t_1 nella propria generazione $g(t_1) = g_1$
i_2 = indice associato a t_2 nella propria generazione $g(t_2) = g_2$
i_3 = indice associato a t_3 nella propria generazione $g(t_3) = g_3$

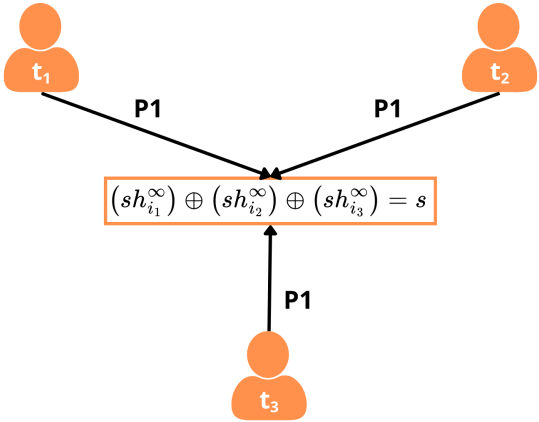


Ricostruzione

2 Evolving secret-sharing

Siano t_1, t_2, t_3 elementi di $\mathcal{P}_n$
Scenario 2: $g(t_1) \neq g(t_2) \neq g(t_3)$

LEGENDA:
i_1 = indice associato a t_1 nella propria generazione $g(t_1) = g_1$
i_2 = indice associato a t_2 nella propria generazione $g(t_2) = g_2$
i_3 = indice associato a t_3 nella propria generazione $g(t_3) = g_3$

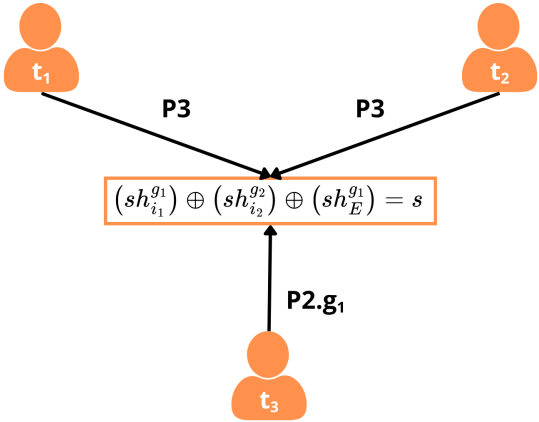


Ricostruzione

2 Evolving secret-sharing

Siano t_1, t_2, t_3 elementi di $\mathcal{P}_n$
Scenario 3: $g(t_1) = g(t_2) \neq g(t_3)$

LEGENDA:
i_1 = indice associato a t_1 nella propria generazione $g(t_1) = g_1$
i_2 = indice associato a t_2 nella propria generazione $g(t_2) = g_2$
i_3 = indice associato a t_3 nella propria generazione $g(t_3) = g_3$

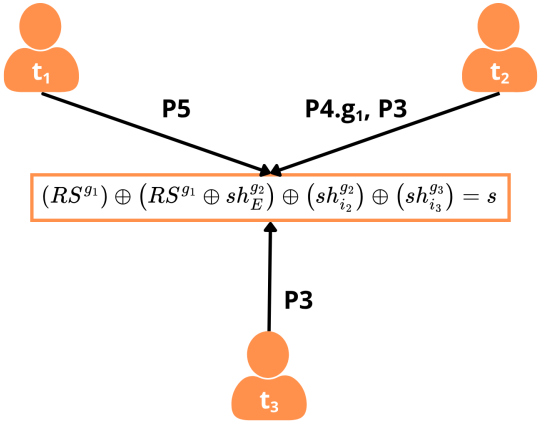


Ricostruzione

2 Evolving secret-sharing

Siano t_1, t_2, t_3 elementi di $\mathcal{P}_n$
Scenario 4: $g(t_1) \neq g(t_2) = g(t_3)$

LEGENDA:
i_1 = indice associato a t_1 nella propria generazione $g(t_1) = g_1$
i_2 = indice associato a t_2 nella propria generazione $g(t_2) = g_2$
i_3 = indice associato a t_3 nella propria generazione $g(t_3) = g_3$



Sicurezza

2 Evolving secret-sharing

Grazie ai seguenti fattori:

1. uso della casualità;
2. sicurezza dello schema $(3, \infty)$;
3. sicurezza dello schema $(3, N^i)$;
4. totale indipendenza dei due schemi;

si può dimostrare che un insieme proibito di dimensione massima (pari a 2), non è comunque in grado di ricavare informazioni circa il segreto.

Analisi della dimensione dello share

2 Evolving secret-sharing

La dimensione dello share per il $t-$esimo partecipante è al più:

$$
\begin{aligned}
c \cdot (\log_4 \log_2 t)^2 + \quad & \text{(P1)} \\
\frac{\sqrt[z]{4}}{3} \cdot \log_2 t + \quad & \text{(P2)} \\
\sqrt[z]{4} \cdot \log_2 t + \quad & \text{(P3)} \\
\log_2 p \cdot (\log_4 \log_2 t) \quad & \text{(P4 e P5)}
\end{aligned}
$$

NOTA: z è la costante da cui dipende la dimensione dell'intervallo in cui cercare numeri primi, ragion per cui è nell'interesse del dealer sceglierlo grande.

Analisi della dimensione dello share

2 Evolving secret-sharing

Mettendo tutto assieme:

$$\frac{4}{3}\sqrt[z]{4}\log_2 t + c \cdot (\log_4 \log_2 t)^2 + \log_2 p \cdot (\log_4 \log_2 t)$$

dal teorema di Komargodski:

$$2 \cdot \log_2 t + poly(3, l) \cdot o(\log_2 t)$$

Analisi della dimensione dello share

2 Evolving secret-sharing

Mettendo tutto assieme:

$$\frac{4}{3}\sqrt[z]{4}\log_2 t + \cancel{c \cdot (\log_4 \log_2 t)^2} + \cancel{\log_2 p \cdot (\log_4 \log_2 t)}$$

dal teorema di Komargodski:

$$2 \cdot \log_2 t + \cancel{poly(3,l) \cdot o(\log_2 t)}$$

Analisi della dimensione dello share

2 Evolving secret-sharing

Si supponga che:

$$\left(\frac{4}{3} \cdot \sqrt[z]{4}\right) \log_2 t < \left(\frac{4}{3} + \epsilon\right) \log_2 t$$

da cui:

$$\epsilon > \frac{4}{3} \cdot \left(\sqrt[z]{4} - 1\right)$$

per z tendente all'infinito:

$$\left(\frac{4}{3} + \epsilon\right) \log_2 t < 2 \cdot \log_2 t$$

(ad oggi ancora il miglior risultato disponibile per questa tipologia di schema)

Table of Contents

Conclusioni

3 Conclusioni

Con questa presentazione abbiamo visto che:

- definizioni e proprietà generali di uno schema di secret-sharing;
- esempi di schemi con evolving access structure;
- stato dell'arte del $(3, \infty)$ secret sharing con annesso studio di correttezza e sicurezza.

Riferimenti

3 Conclusioni

[1] A. Beimal, *Secret-Sharing Schemes: A Survey*, IWCC 2011, pp. 11-46;

[2] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Designs, Codes and Cryptography 1992, pp. 357-390;

[3] A. Shamir, *How to Share a Secret*, Communications of the ACM 1979, Volume 22, No. 22, pp. 612-613;

[4] S. Krenn and T. Lorünser, *An Introduction to Secret Sharing*, SpringerBriefs in Information Security and Cryptography 2023;

[5] M. Ito et al., *Multiple Assignment Scheme for Sharing Secret*, Journal of Cryptology 1993, Volume 6, pp. 15-20;

[6] I. Komargodski, *How to Share a Secret, Infinitely*, IEEE Transactions on Information Theory 2018, Volume 64, No. 6, pp. 4179-4190;

[7] P. D'Arco et al., *Secret sharing schemes for infinite sets of participants: A new design technique*, Theoretical Computer Science 2011, pp. 149-161;

[8] Q. Cheng et al., *A Construction of Evolving 3-threshold Secret Sharing Scheme with Perfect Security and Smaller Share Size*, arXiv:2410.13529v1, 17 October 2024;

EVOLVING SECRET SHARING

Grazie per l'attenzione!
Domande?