Secret Sharing folosind interpolare Birkhoff

Radu Miron

5 iulie 2018

UAIC FII Iasi

Continut

Interpolarea Birkhoff

Definiție

- $X = \{x_1, ..., x_{n+1}\}, E = \{e_{i,j} | e_{i,j} \in \{0, 1\}, i = 1, n+1; j = 0, m\}$, $C = \{c_{i,j} \in \Re | e_{i,j} = 1\}$, $G = \{g_0, g_1, ..., g_n\}$
- polinomul P de grad n care verifică ecuațiile

$$P^{(k)}(x_i) = c_{i,k}$$

- **¿ ¿** soluție unică **? ?**

Condițiile lui Polya

$M_r =$ numărul de 1-uri de pe primele $r+1$ coloane ale matricei E
Atunci, condiția *necesară* pentru a avea soluție unică este:

$$M_r \geq r+1, \forall r \in \{0, 1, ..., m\}$$

Polinomul de interpolare

Fie $G = \{1, x, x^2\}$, deci $g_0(x) = 1, g_1(x) = x, g_2(x) = x^2$. Presupunem că X și E sunt următoarele : $X = \{1, 2, 3\}$,

$$E = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

iar datele sunt $p(1) = 15, p(2) = 29, p'(3) = 23$. Căutăm polinomul $p(x) = a_2x^2 + a_1x + a_0$ ce satisface $p(1) = 15, p(2) = 29, p'(3) = 23$.

$$A(E, X, G) = \begin{pmatrix} g_0(x_1) & g_1(x_1) & g_2(x_1) \\ g_0(x_2) & g_1(x_2) & g_2(x_2) \\ g_0'(x_3) & g_1'(x_3) & g_2'(x_3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 0 & 1 & 6 \end{pmatrix}$$

$$A(E, X, G_0) = \begin{pmatrix} p(x_1) & g_1(x_1) & g_2(x_1) \\ p(x_2) & g_1(x_2) & g_2(x_2) \\ p'(x_3) & g_1'(x_3) & g_2'(x_3) \end{pmatrix} = \begin{pmatrix} 15 & 1 & 1 \\ 29 & 2 & 4 \\ 23 & 1 & 6 \end{pmatrix}$$

Polinomul de interpolare

Observăm că $det(A(E,X,G)) = 3, det(A(E,X,G_0)) = 21, det(A(E,X,G_1)) = 15, det(A(E,X,G_2)) = 9$. Conform formulei de interpolare Birkhoff, polinomul căutat va fi

$$p(x) = \sum_{j=0}^{2} \frac{D(E,X,G_j)}{D(E,X,G)} g_j(x) = 7 + 5x + 3x^2.$$

Scheme de partajare ierarhice conjunctive

Definitie

- $U =$ mulțime de n participanți, împărțită pe nivele disjuncte $U = \bigcup_{i=0}^{m} U_i$, unde fiecare nivel are un anumit prag. Fie $K = \{k_i\}_{i=0}^{m}$ un șir crescător de numere întregi pozitive, $0 \leq k_0 \leq k_1 \leq ... \leq k_m$.
- structura de acces a schemei (K, n) ierahice este:

$$\Gamma = \{V \subset U : |V \cap (\bigcup_{j=0}^{i} U_j)| \geq k_i, \forall i \in \{0, 1, ..., m\}\}$$

Schema lui Tassa

1. Dealer-ul selectează aleator polinomul $P \in F_{k-1}[x]$, unde

$$P(x) = \sum_{i=0}^{k-1} a_i x^i, \quad a_0 = S$$

2.Dealerul atribuie fiecărui participant $u \in U$ un element al corpului F.

3..Dealer-ul distribuie participanților share-uri în următorul mod:
Fiecare participant de pe nivelul i din ierarhia de nivele, $u \in U_i$, $0 \leq i \leq m$ primește share-ul $P^{(k_{i-1})}(u)$, adică derivata polinomului P de ordinul nivelului anterior.

Proprietati

- liniaritatea schemei lui Tassa
- liniaritatea schemei lui Shamir
- proprietățile schemei lui Shamir datorate liniarității
- ¿ ¿ proprietățile schemei lui Tassa datorate liniarității **? ?**

Schemă dealer-free

Schemă dealer-free

- probleme
- soluții

Schemă dealer-free

- fiecare participant generează random un număr x_i, cu $x_i \in F_q$ și va distribui secretul său cu schema lui Tassa
- participantul P_i transmite participanților de pe nivelul U_k share-ul $s_{i,j,k} = p_i^{(k-1)}(u_{k,j})$
- la final, utilizatorul j de pe nivelul k va avea share-ul: $S_{j,k} = s_{1,j,k} + s_{2,j,k} + ... + s_{n,j,k}$.
- noul secret va fi $S = x_1 + x_2 + ... + x_n$.

Micșorarea pragului

Micșorarea pragului

- probleme
- soluții

Schema de micșorare a pragului i

1. Jucătorii selectează un id j, astfel încât j să nu se afle în mulțimea identităților jucătorilor implicați în schemă. Fiecare calculează constanta folosită pentru polinomul de interpolare Lagrange, $P = \sum \gamma_i share(i)$:

$$\gamma_i = \prod_{1 \leq k \leq t, i \neq k} \frac{j-k}{i-k}$$

2. Jucătorul P_i își va înmulți share-ul său $f(id_i)$ cu γ_i. Mai apoi, va "splita" secretul său în t porțiuni:

$$\gamma_i f(id_i) = \phi_{1i} + \phi_{2i} + ... + \phi_{ti}, 1 \leq i \leq t$$

3. Jucătorii schimbă între ei valorile ϕ_{ij}. Valoarea ϕ_{ij} reprezintă valoarea trimisă de jucătorul j către jucătorul i astfel,

$$\sigma_i = \phi_{i1} + \phi_{i2} + ... + \phi_{it}$$

va fi ceea ce va deține jucătorul P_i și va pune la comun cu restul jucătorilor care reconstruiesc secretul.

4. Jucătorii adună valorile γ_k, $1 \leq k \leq t$ și caluleaza

$$f(j) = \sum_{k=1}^{t} \sigma_k$$

5. Fiecare P_i combină share-ul său privat $f(i)$ cu $f(j)$ după următoarea formulă:

$$f_0(i) = f(j) - j(\frac{f(i) - f(j)}{i - j})$$

6. Polinomul f_0 este un polinom de gradul $t - 2$, cu $f_0(0) = f(0)$. Va rezulta că pragul $t - 2$ este noul prag al schemei.

Schema de micșorare a pragului

1. Jucătorii selectează un id j, astfel încât j să nu se afle în mulțimea identităților jucătorilor implicați în schemă. Fie $P_1, P_2, ..., P_t$ cei t jucători care doresc să refacă un secret. Apoi fiecare calculează constanta folosită pentru polinomul de interpolare Birkhoff:

$$\gamma_i = \sum_{k=0}^{t-1} a_{i,k} j^k$$

unde $a_{l,k} = (-1)^{l-1+k} \frac{det(A_{l-1,k}(E,X,G))}{det(A(E,X,G))}$ este calculat de participantul corespunzător liniei perechii i_l, j_l din E, cu $l = 1, ..., r$, iar $A_{l-1,k}(E, X, G)$ reprezintă matricea $A(E, X, G)$ din care am eliminat linie l și coloana $k + 1$.

Concluzii!!!