IC - Seminar nr. 4 — 20 mai 2019

Partajarea secretelor

Schema lui Shamir

n utilizatori $u_1, u_2, \dots u_n$

$2 \le k \le n$ prag

$S \longrightarrow \hat{i}_1, \hat{i}_2 \dots \hat{i}_n$

S secret; $\hat{i}_1, \hat{i}_2 \dots \hat{i}_n$ subsecrete

a.î. [$\forall k$ utilizatori pot găsi ușor secretul; $\forall k-1$ utilizatori nu pot găsi ușor secretul]

I Setup

Fie p nr. prim. (mare) $p > m$

160 biți

secretul $S \in \mathbb{Z}_p$

Se generează un polinom de grad maxim $k-1$, având coeficienții puși în $\mathbb{Z}_p$ a.î.

$P(0) = S$

$P(x) = a_{k-1}x^{k-1} + \dots + a_1 x + \boxed{S}$

subsecretele $\hat{i} = P(i) \bmod p, \ \forall i = \overline{1,m}$

II Reconstrucție a secretului S având k subsecrete

$A \subseteq \{1, \dots m\}$

$|A| = k$

$S = P(0) \overset{\text{LAGRANGE}}{=} \sum_{i \in A} \hat{i} \prod_{\substack{j \in A \\ j \neq i}} \frac{\hat{j}}{j-i} \bmod p$

! $\hat{\frac{j}{j-i}} = j \cdot (j-i)^{-1} \bmod p$

Exercitiu

$1^{-1}=1$ $5^{-1}=9$ $9^{-1}=5$
$2^{-1}=6$ $6^{-1}=2$ $10^{-1}=10$
$3^{-1}=4$ $7^{-1}=8$
$4^{-1}=3$ $8^{-1}=7$

(4p) ① Exemplificați Schema lui Shamir pt $m=5$, $K=3$, $p=11$

I. Generați secretul S, i_j, $j=\overline{1,m}$

II. 3 subsecrete i_1, i_3, i_5 → S

(3p) ② Dem că dacă $S_1 \to i_1^1, i_2^1 \dots i_m^1$

$S_2 \to i_1^2, i_2^2 \dots i_m^2$

K, m, p fixați

$S_1+S_2 \to i_1^1+i_1^2, i_2^1+i_2^2, \dots i_m^1+i_m^2$

(2p) ③ Prezentați o procedură de actualizare a subsecretelor K, m, p

$S \to i_1, \dots i_m$

$i_1' \quad i_m'$

(fără a reconstrui secretul S

fără a expune subsecretele inițiale)

(2p) ④ Prezentați o metodă prin care un utilizator își poate verifica că subsecretul său, i_j, este corect. ($i_j = P(j)$ fără a expune $P(X)$)

Indicație: Folosiți o funcție one-way cu proprietatea homomorfă

$f: \mathbb{Z}_p \to \mathbb{Z}_{p'}$, $f(a+b)=f(a)+f(b)$ Ex: $f(x)=\alpha^x \bmod p'$

Sunt date $P(i), k, m, p$ și fiecare cu

Rezolvare $m=5, k=3, p=11$

I fie P polinom de gradul 2, $P(X)=X^2+2X+7 \Rightarrow S=7$

$i_1 = P(1) \bmod 11 = (1\cdot1+2\cdot1+7) \bmod 11 = 10$

$i_2 = P(2) \bmod 11 = (2\cdot2+2\cdot2+7) \bmod 11 = 15 \bmod 11 = 4$

$i_3 = P(3) \bmod 11 = (3\cdot3+2\cdot3+7) \bmod 11 = 22 \bmod 11 = 0$

$i_4 = P(4) \bmod 11 = (4\cdot4+2\cdot4+7) \bmod 11 = 31 \bmod 11 = 9$

$i_5 = P(5) \bmod 11 = (5\cdot5+2\cdot5+7) \bmod 11 = 42 \bmod 11 = 9$

II Lagrange i_1, i_3, i_5, $A=\{1,3,5\}$

$$P(0) = \sum_{i\in A} i_i \left(\prod_{\substack{j\in A \\ j\neq i}} j\cdot(j-i)^{-1} \right) \bmod p = i_1 \cdot 3\cdot(3-1)^{-1}\cdot 5\cdot(5-1)^{-1} + i_3\cdot 1\cdot(1-3)^{-1}\cdot 5\cdot(5-3)^{-1} + i_5\cdot 1\cdot(1-5)^{-1}\cdot 3\cdot(3-5)^{-1} \bmod 11$$

645
645
7095

$$= 10\cdot3\cdot2^{-1}\cdot5\cdot4^{-1} + 0\cdot1\cdot9^{-1}\cdot5\cdot2^{-1} + 9\cdot1\cdot7^{-1}\cdot3\cdot9^{-1} \bmod 11$$

$$= 10\cdot3\cdot6\cdot5\cdot3 + 0 + 9\cdot1\cdot8\cdot3\cdot5 \bmod 11$$

$$= 2700 + 1080 \bmod 11 = 3780 \bmod 11 = 343\cdot11+7 \bmod 11 = 7 = S$$

(2) $S_1 \leftarrow i_1^1, i_2^1, \dots i_m^1$

$S_2 \leftarrow i_1^2, i_2^2, \dots i_m^2$

$S_1+S_2 \leftarrow i_1^1+i_1^2, \dots i_m^1+i_m^2$

fie $S' \leftarrow i_1^1+i_1^2, \dots i_m^1+i_m^2$

$\forall i\in A,\ i_i^1 \prod_{\substack{j\in A\\ j\neq i}} \frac{j}{j-i} + i_i^2 \prod_{\substack{j\in A\\ j\neq i}} \frac{j}{j-i} = (i_i^1+i_i^2) \prod_{\substack{j\in A\\ j\neq i}} \frac{j}{j-i}$

$$= \left(\sum_{i\in A} i_i^1 \prod_{\substack{j\in A\\ j\neq i}} \frac{j}{j-i} \right) + \left(\sum_{i\in A} i_i^2 \prod_{\substack{j\in A\\ j\neq i}} \frac{j}{j-i} \right) = \sum_{i\in A} (i_i^1+i_i^2) \prod_{\substack{j\in A\\ j\neq i}} \frac{j}{j-i}$$

$\Leftarrow$ $S_1 + S_2 = S'$

(3) $S \to i_1, \dots i_m$

$i'_1 \quad i'_2$

$S \to i_1, i_2, \dots, i_m$

$S' \to i_m, i_{m-1}, \dots i_1$

$S+S \to i_1+i_m, i_2+i_{m-1}, \dots i_m+i_1$

$2S$

deci $i'_i = (i_i + i_{m-i+1}) \cdot 2^{-1}$

$\Rightarrow S' = (S+S) \cdot 2^{-1} = 2 \cdot S \cdot 2^{-1} = S$

$i'_i = (i_i + i_{(i+1) \bmod m}) \cdot 2^{-1}$ pt $i < m$

$i'_m = (i_m + i_1) \cdot 2^{-1}$

$\sum_{i \in A} i'_i$

$i'_i = i_i + p \cdot k^{-1} \cdot \prod_{\substack{j \in A \\ j \neq i}} \frac{j}{j-i}$

$\sum_{i \in A} i'_i \prod_{\substack{j \in A \\ j \neq i}} \frac{j}{j-i} = \sum_{i \in A} i_i \prod_{\substack{j \in A \\ j \neq i}} \frac{j}{j-i} + k \cdot p \cdot k^{-1} \bmod p = (S+p) \bmod p = S$

③. $i_i^{0\,1}$

④ dacă i se dă $\alpha = \sum_{j=1}^{k-1} a_{j-1} x^{j-1}$ $\mod p' = f(a_{j-1}, x^{j-1})$, $j<k$

utilizatorul poate verifica dacă $\prod_{j<k} f(a_{j-1}, x^{j-1}) \equiv f(i_i^0)$

$$\| $$

$$f\left(\prod_{j<k} a_{j-1}\, i^{j-1}\right) = f(P(i)) = f(i_i^1)$$

③ $S \to i_1 \dots i_m$ ~~$k \cdot l = p \Rightarrow l = p \cdot k^{-1}$~~

$$i_i^{1\,1} = i_i^1 + \vec{k} \cdot \prod \frac{j-i}{j}$$

$$\Rightarrow \sum_{i\in A} i_i \prod_{\substack{j\in A \\ j\neq i}} \frac{j}{j-i} = \sum_{i\in A} i_i \prod_{\substack{j\in A \\ j\neq i}} \frac{j}{j-i} + k^{-1} \cdot K \quad ?$$

~~$i_i^{1\,1} = K i_i^0$~~

$$i_i^{1\,1} = i_i^1 + i^{-1} \prod \frac{j-i}{j}$$

$$\to \sum_{i\in A} i_i^1 \prod_{\substack{j\in A \\ j\neq i}} \frac{0}{j-i} = \sum_{i\in A} i_i \prod_{\substack{j\in A \\ j\neq i}} + \sum_{i\in A} i^{-1} \mod p$$

$$\| \ \alpha \bmod p$$

$= S$

$$i_i^{1\,1} = i_i^0 + i_{i0+1}^0 \cdot$$