Partajarea secretelor - schema lui Shamir

O schemă de partajare a secretelor împarte un *secret* în *subsecrete* care sunt distribuite unor utilizatori. Secretul poate fi reconstruit numai de anumite grupuri stabilite a priori, grupuri ce formează *structura* (*autorizată*) *de acces* a schemei de partajare. Schemele de partajare a secretelor au fost introduse independent de Blakley [1] şi Shamir [2], ca o soluţie pentru stocarea cheilor criptografice. Schemele de partajare a secretelor pot fi folosite în orice situaţie în care accesul la o resursă importantă trebuie să fie partajat. Accesul la un depozit bancar sau lansarea rachetelor nucleare sunt două astfel de exemple.

În primele scheme de partajare a secretelor, numai numărul de utilizatori prezenţi era important pentru reconstrucţia secretului - este vorba de aşa numitele scheme *prag*, în care toţi utilizatorii au aceeaşi importanţă. În cele ce urmează, n va reprezenta numărul total de utilizatori (utilizatori ce vor fi identificaţi prin numere de la 1 la n) iar k (unde k satisface $2 \leq k \leq n$) va reprezenta numărul minim de participanţi prezenţi pentru a putea reconstrui secretul. Informal, o *schemă prag de partajare a secretelor* este o metodă de a genera $(S, (I_1, \ldots, I_n))$ astfel încât

- (*corectitudine*) - pentru orice $A \subseteq \{1, 2, \ldots, n\}$, $|A| = k$, problema determinării elementului S, fiind date $\{I_i \mid i \in A\}$, este "uşoară";
- (*securitate*) - pentru orice $A \subseteq \{1, 2, \ldots, n\}$, $|A| = k - 1$, problema determinării elementului S, fiind date $\{I_i \mid i \in A\}$, este "grea".

Elementul S va fi numit *secret* iar elementele $I_1, \ldots, I_n$ vor fi numite *subsecretele* lui S.

Schema lui Shamir [2] se bazează pe *interpolare polinomială* - fiind date k perechi $(x_1, y_1), \ldots, (x_k, y_k)$ unde $x_i \neq x_j$ pentru orice $1 \leq i < j \leq k$, există un unic polinom $P(x)$ de grad $k - 1$ astfel încât $P(x_i) = y_i$, pentru orice $1 \leq i \leq k$.

- Secretul S este ales ca un element arbitrar dintr-un corp (cum ar fi $\mathbf{Z}_p$, unde p este un număr prim); se generează un polinom P de grad $k-1$ având coeficienţi din corpul respectiv, astfel încât $P(0) = S$ (adică, coeficientul liber este secretul);

- Subsecretele $I_1, \ldots, I_n$ sunt generate ca $I_i = P(x_i)$, $1 \leq i \leq n$, unde $x_1, \ldots, x_n$ sunt valori publice distincte două câte două (putem alege chiar $x_i = i$, $\forall 1 \leq i \leq n$) - atenţie, calculele se fac în corpul respectiv;

- Având subsecretele $\{I_i | i \in A\}$, pentru un grup A cu $|A| = k$, secretul poate fi obţinut folosind formula lui Lagrange (atenţie, calculele se fac în corpul respectiv) ca[1]

$$S = \sum_{i \in A} (I_i \cdot \prod_{j \in A \setminus \{i\}} \frac{x_j}{x_j - x_i}).$$

  În cazul $x_i = i$, $\forall 1 \leq i \leq n$, secretul poate fi obţinut ca

$$S = \sum_{i \in A} (I_i \cdot \prod_{j \in A \setminus \{i\}} \frac{j}{j - i}).$$

Tema va avea două părţi:

1. Generarea secretului şi a subsecretelor sale - dându-se n şi k, se generează mai întâi p prim, apoi secretul S aleator în $\mathbf{Z}_p$ şi subsecretele sale, $I_1, \ldots, I_n$, calculate ca mai sus;

2. Reconstrucţia secretului - dându-se n, k, p şi k perechi (i, I_i), se calculează secretul S, folosind formula lui Lagrange, ca mai sus.

References

[1] G. R. Blakley. Safeguarding cryptographic keys. In *National Computer Conference, 1979*, volume 48 of *American Federation of Information Processing Societies Proceedings*, pages 313–317, 1979.

[2] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[1] Într-un corp, expresia $\frac{a}{b}$ denotă ab^{-1}, unde $b \neq 0$. În particular, în $\mathbf{Z}_p$, când p este prim, expresia $\frac{a}{b}$ denotă ab^{-1} `mod` p, unde b^{-1} reprezintă inversul multiplicativ al lui b modulo p (în cazul $b \neq 0$).