Secret Sharing

Petr Veselý (454919)

M0170 Kryptografie

13. 5. 2016

Osnova

- Motivace
- Sdílení mezi dvěma účastníky
- Shamirovo (k, n)-prahové schéma
- Blakleyho (k, n)-prahové schéma
- Definice
- Vlastnosti schémat
- Hierarchická schémata
- Tassovo schéma
- Shrnutí

Motivace

Sdílení mezi dvěma účastníky

- **Tajemství *S***
- $S = 0100101011001011\ 0101001010100111$

- **Naivní metoda**
- $T_1 = 0100101011001011$
- $T_2 = 0101001010100111$

Sdílení mezi dvěma účastníky

- **Tajemství *S***
- $S = 0100101011001011\ 0101001010100111$

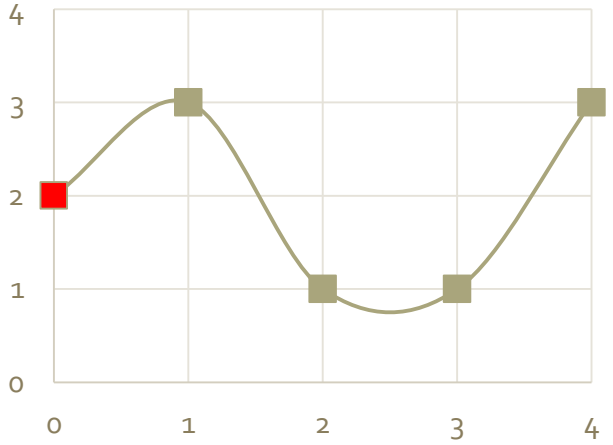
- **Naivní metoda**
- $T_1 = 0100101011001011$
- $T_2 = 0101001010100111$

- **Bezpečná metoda**
- $R = 1101001011010100\ 1011010010010010$
- $T_1 = R$
- $T_2 = S \oplus R$

- Zobecnění pro více účastníků…

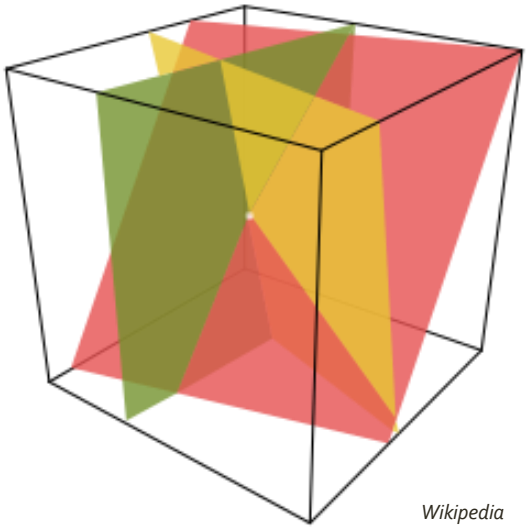
Shamirovo (k, n)-prahové schéma (1979)

- **Náhodný polynom st. k-1, konst. člen je tajemství**
- $f(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + S$
- n účastníků dostane hodnoty $f(1), \ldots f(n)$
- k hodnot jednoznačně určí polynom
- V praxi se používá polynom nad $GF(p)$, $p > S$.
- Lagrangeova interpolace: $L(0) = \sum_{j=0}^{k} f(x_j) \prod_{\substack{m=0 \\ m \neq j}}^{k} \frac{x_m}{x_m - x_j}$



Blakleyho (k, n)-prahové schéma (1979)

- **Bod A v k-rozměrném prostoru, jeho první souřadnice je tajemství S**
- $A[S, a_1, \dots, a_{k-1}]$
- n účastníků dostane n rovnic (vhodně vybraných) nadrovin, v jejichž průsečíku A leží
- k nadrovin se protne v bodu A



Wikipedia

Formální definice

- **Přístupová struktura (access structure)**
- $\Gamma \subseteq 2^P$, kde $P = \{p_1, p_2, \dots, p_n\}$
- množina všech množin účastníků, které jsou schopné určit tajemství S

- **Monotónní přístupová struktura**
- $B \subseteq \mathrm{C} \ \wedge B \in \Gamma \Rightarrow C \in \Gamma$

- **(k, n)-prahové schéma**
- $\Gamma = \{M \in 2^P;\ |M| \geq k\}$

Vlastnosti schémat sdílení tajemství

- **Perfektní bezpečnost (perfect secrecy)**
- $\mathrm{P}(S|B \notin \Gamma) = \mathrm{P}(S)$

- **Informační poměr (information rate)**
- $\rho = \log|T| / \log|S|$

- **Ideální schéma (ideal scheme)**
- $\rho = 1$

Hierarchická schémata

All animals are equal, but some are more equal than the others

Prezident, dva ze tří generálů, tři z šesti plukovníků

- (6, 10)-prahové schéma?

Hierarchická schémata

All animals are equal, but some are more equal than the others

Prezident, dva ze tří generálů, tři z šesti plukovníků

- **Hierarchické prahové schéma**
- účastníci rozděleni do l disjunktních podskupin (úrovní), $P = \bigcup_{i=1}^{l} U_i$
- je definována monotónní posloupnost prahů $0 < k_1 < k_2 < \cdots < k_l$.
- Přístupová struktura je tvořena všemi množinami účastníků, v nichž je alespoň k_j účastníků z $\bigcup_{i=1}^{j} U_i$ pro každé $1 \leq j \leq l$, tedy

$$\Gamma = \left\{ V \subseteq P; \left| V \cap \left(\bigcup_{j=1}^{i} U_j \right) \right| \geq k_i \; \forall i \in \{1, \ldots, l\} \right\}.$$

Hierarchická schémata - naivní přístup

All animals are equal, but some are more equal than the others

Prezident, dva ze tří generálů, tři z šesti plukovníků

Prezident 28
Generál 7
Plukovník 1

- (45, 55)-prahové schéma?

- Ito, Saito, Nishizeki [ISN89]: **Pro každou monotónní přístupovou strukturu existuje** takové rozdělení počtů podílů mezi účastníky, že počet podílů držených množinou účastníků dosáhne prahu pouze tehdy, je-li množina prvkem přístupové struktury

Tassovo schéma

- **Hierarchické schéma podobné Shamirovu schématu**
- $f(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + S$ nad GF(p)
- $U_0, \ldots, U_m$ hierarchie účastníků (disj. množiny)
- $0 < k_0 < k_2 < \cdots < k_m = k$ příslušné prahy

- V každé úrovni U_i dostane účastník u podíl počítaný jako $\boldsymbol{P^{(k_{i-1})}(u)}$, kde $P^{(k_{i-1})}$ je $\boldsymbol{k_{i-1}}$**-tá derivace**

- **Příklad:** $k_0 = 2, k_1 = 4, k_2 = 6$
- U_0 $P(u)$
- U_1 $P^{(2)}(u)$
- U_2 $P^{(4)}(u)$

Tassovo schéma – rekonstrukce tajemství

- **Birkhoffova interpolace**
- Definujme vektor…
$$\boldsymbol{r} = (1;\ x, x^2, \dots, x^{k-1})$$
- …a vektor koeficientů polynomu $P(x)$
$$\boldsymbol{a} = (S, a_1, a_2, \dots, a_{k-1})$$
- Podíl tajemství $P^{(k_i-1)}(u)$ je skalárním součinem vektoru $\mathbf{r}^{(k_i-1)}(u)$, který známe, a vektoru $\mathbf{a}$, který chceme zjistit
- To vede k řešení soustavy lineárních rovnic

- **Příklad:** $k_0 = 2, k_1 = 4, k_2 = 6$
- $\boldsymbol{r} = (1;\ x, x^2, x^3, x^4, x^5)$
- $\boldsymbol{r^{(2)}} = (0, 0, 2, 6x, 12x^2, 20x^3)$
- $\boldsymbol{r^{(4)}} = (0, 0, 0, 0, 24, 120x)$

Shrnutí

- Existuje řada efektivních schémat sdílení tajemství
- Prahová schémata, hierarchická schémata
- Perfektní bezpečnost

Zdroje

- [Sha79] Adi Shamir. How to share a secret. In *Commun. ACM*, 22(11):612-613, 1979.
- [Bla79] G R Blakley. Safeguarding cryptographic keys. In *National Computer Conference Proceedings, vol 48*, pages 313-317. AFIPS, 1979.
- [ISN89] M. Ito, et al., Secret sharing scheme realizing general access structure. In *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 72, pp. 56-64, 1989.
- [Tas07] Tamir Tassa. Hierarchical threshold secret sharing. In *Journal of Cryptology*, 20(2):237-264, 2007.