Sdílení tajemství

Andrew Kozlík

KA MFF UK

Sdílení tajemství mezi dvěma lidmi

Příklad: Sdílení tajného 6místného PINu mezi dvěma lidmi.

- Naivní řešení:
  - PIN: 5 4 8 1 7 2
  - $Díl_1$: 5 4 8 _ _ _
  - $Díl_2$: _ _ _ 1 7 2
  - Problém: Samotný držitel dílu má informaci o PINu, která jej zužuje na 10^3 možných hodnot z celkových 10^6.

- Lepší řešení:
  - $Díl_1$: Zvolíme náhodně celé číslo z $[0, 10^6)$.
  - $Díl_2 \equiv PIN - Díl_1 \pmod{10^6}$.
  - Potom $PIN = (Díl_1 + Díl_2) \bmod 10^6$.
  - Samotný $Díl_1$ neobsahuje žádnou informaci o PINu.
  - Samotný $Díl_2$ neobsahuje žádnou informaci o PINu, protože má rovnoměrné rozdělení na $[0, 10^6) \cap \mathbb{Z}$ bez ohledu na hodnotu PINu.

Sdílení tajemství mezi třemi lidmi

Příklad: Sdílení tajného 6místného PINu mezi třemi lidmi.

- $Díl_1$: Zvolíme náhodně celé číslo z $[0, 10^6)$.
- $Díl_2$: Zvolíme náhodně celé číslo z $[0, 10^6)$.
- $Díl_3 \equiv PIN - Díl_1 - Díl_2 \pmod{10^6}$.

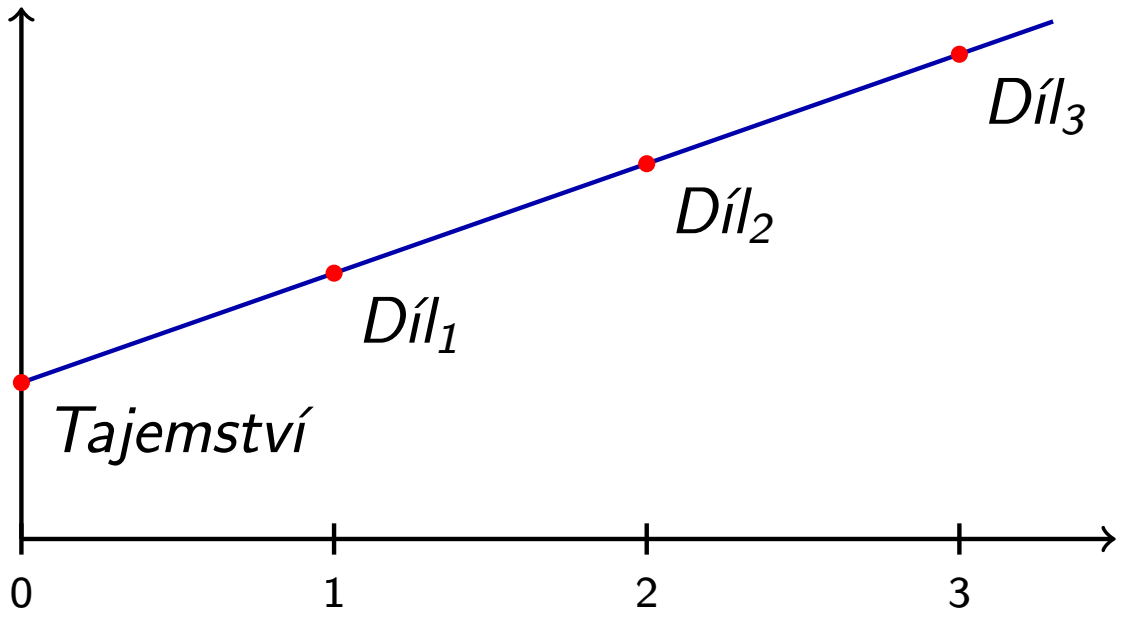
Příklad: Sdílení tajného 6místného PINu mezi třemi lidmi tak, aby jej libovolní dva mohli určit.

- Naivní řešení:
  - PIN: 5 4 8 1 7 2
  - $Díl_1$: 5 4 8 1 _ _
  - $Díl_2$: 5 4 _ _ 7 2
  - $Díl_3$: _ _ 8 1 7 2

- Lepší řešení:
  Shamirovo schéma sdílení tajemství.

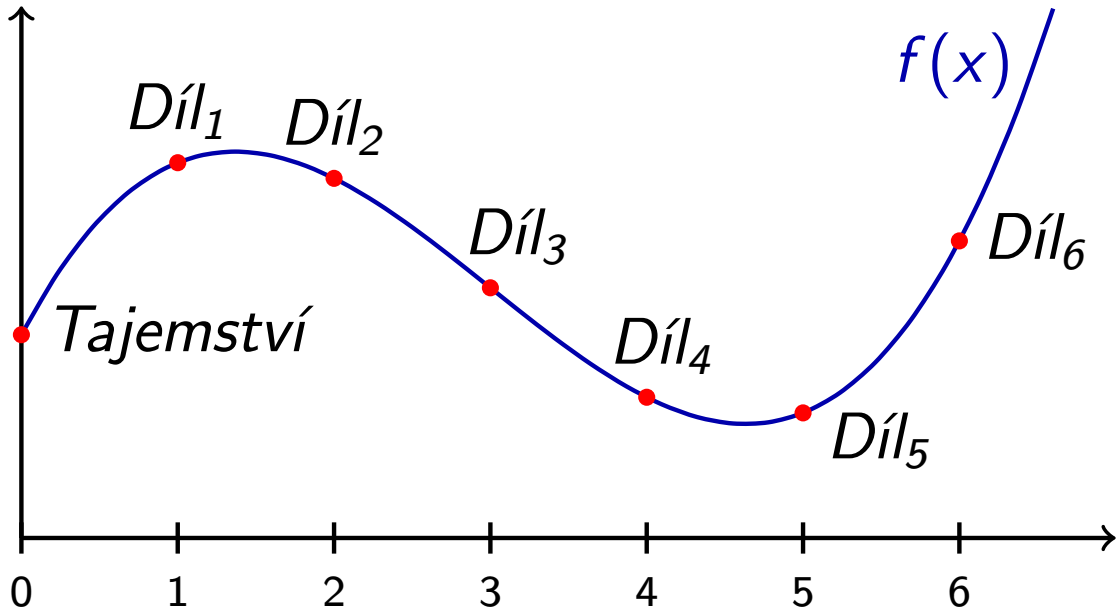
Příklad: Schéma sdílení tajemství 2-z-3

- $f(x) = ax + b$ je funkce (nad konečným tělesem).
- a je náhodně volený prvek tělesa, b je tajemství.
- Velikost konečného tělesa musí pojmout hodnotu tajemství, např. $\mathbb{Z}_{1000003}$, a počet účastníků + 1.
- Účastník $x \in \{1, \ldots, 3\}$ obdrží bod $(x, f(x))$.
- Libovolné 2 díly (body) jednoznačně určují tajemství.
- Ilustrace



Příklad: Schéma sdílení tajemství 4-z-6

- f je polynom stupně 3 (nad konečným tělesem).
- Tajemství je hodnota absolutního členu $f(0)$.
- Ostatní koeficienty polynomu jsou voleny náhodně s rovnoměrným rozdělením.
- Účastník $x \in \{1, \ldots, 6\}$ obdrží bod $(x, f(x))$.
- Libovolné 4 díly (body) jednoznačně určují tajemství.
- Ilustrace



Lagrangeův interpolační polynom

Věta

Nechť $M = \{(x_1, y_1), \ldots, (x_k, y_k)\} \subseteq \mathbb{F}^2$ *je množina bodů taková, že* $\{x_1, \ldots, x_k\}$ *jsou po dvou různé.*
Potom nad tělesem $\mathbb{F}$ *existuje právě jeden polynom stupně nejvýše* $k-1$*, který prochází všemi body z* M

$$f(x) = \sum_{i=1}^{k} y_i \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j}.$$

Důkaz.

1. Všimněme si, že polynom nabývá správných hodnot:
   Dosadíme-li x_ℓ za x, kde $1 \leq \ell \leq k$, tak
   - pro $i = \ell$ máme součin jednotek,
   - pro $i \neq \ell$ se vyskytne nula v součiniteli, kde $j = \ell$.

   Tedy $f(x_\ell) = y_\ell$.

Lagrangeův interpolační polynom

Důkaz (pokračování).

2. Polynom f je stupně nejvýše $k-1$.
3. Jednoznačnost.
   - Nechť g je polynom stupně nejvýše $k-1$ nad $\mathbb{F}$, který prochází všemi body z M.
   - Potom $f-g$ je polynom stupně nejvýše $k-1$ nad $\mathbb{F}$.
   - $f-g$ má k po dvou různých kořenů $\{x_1, \ldots, x_k\}$.
   - Jediný polynom stupně nejvýše $k-1$, který má k kořenů, je nulový polynom.
   - Tedy $f = g$.

Shamirovo schéma sdílení tajemství

Úloha:

- Nechť $\mathbb{F}$ je konečné těleso a $1 \leq k \leq n < |\mathbb{F}|$ jsou celá čísla.
- Chceme rozdělit tajemství $s \in \mathbb{F}$ mezi n účastníků tak, aby:
  - každá podmnožina k účastníků mohla jednoznačně určit s,
  - každá podmnožina $(k-1)$ účastníků neměla žádnou informaci o s.
    (Pro s má každá hodnota z $\mathbb{F}$ stejnou pravděpodobnost.)
- k nazýváme *práh*, anglicky *threshold*.

Rozdělení tajemství:

- Definujeme $a_0 = s$.
- Pro $1 \leq i < k$ zvolíme náhodně $a_i \in \mathbb{F}$ s rovnoměrným rozdělením pravděpodobnosti.
- Definujeme $f(x) = \sum_{i=0}^{k-1} a_i x^i$.
- Každému účastníkovi $x \in \{1, \ldots, n\}$ dáme bod $(x, f(x))$.

Shamirovo schéma sdílení tajemství

Složení tajemství:

- Máme podmnožinu účastníků s díly $\{(x_1, y_1), \ldots, (x_k, y_k)\}$.
- Spočteme hodnotu interpolačního polynomu v 0:

$$s = f(0) = \sum_{i=1}^{k} y_i \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x_j}{x_j - x_i}.$$

Bezpečnost:

- Mějme podmnožinu $k-1$ účastníků s díly $M = \{(x_1, y_1), \ldots, (x_{k-1}, y_{k-1})\}$.
- Potom pro každého kandidáta $s' \in \mathbb{F}$ existuje právě jeden polynom stupně nejvýše $k-1$, který prochází body $M \cup \{(0, s')\}$.
- Každý z těchto polynomů má stejnou pravděpodobnost.

Poznámky

- Volba tělesa:
  - $\mathbb{Z}_p$, kde $p \geq n+1$ a $p \geq$ počet možných tajemství.
  - Rozdělovat tajemství po bajtech a použít těleso $\mathrm{GF}(256)$.
- Při rozdělování můžeme místo koeficientů zvolit náhodně $k-2$ bodů, interpolovat a dopočítat zbývající body.
- Rozšiřitelnost: Lze přidávat nové díly i po vytvoření počáteční sady dílů.
- Díly jsou zhruba stejně velké, jako původní tajemství.