Shamirova prahová schéma zdieľania tajomstva

Peter Chvojka, doc. RNDr. Ladislav Satko, PhD*
STU FEI Katedra matematiky
chvojka.p@gmail.com

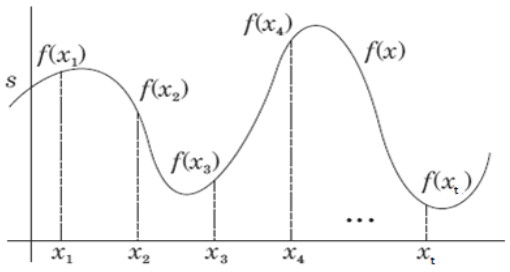
Abstrakt

Cieľom tejto práce je vybudovanie schémy podobnej Shamirovej prahovej schéme na okruhu zvyškových tried Z_m, *v prípade, že* m *je zložené kladné celé číslo. Taktiež sa budeme zaoberať perfektnosťou a monotónnosťou schémy.*

1. Úvod

Shamirova schéma na zdieľanie tajomstva bola jednou z prvých schém s (*t, n*)-prahovou
prístupovou štruktúrou. Často býva základom pre viacero ďalších schém, pretože je jednoduchá na pochopenie a výpočtové procesy dôveryhodnej osoby a aj kombinátora nie sú časovo ani pamäťovo náročné. Výhodou tejto schémy je, že neobmedzuje prahovú hodnotu počtu podielov *t* potrebných na rekonštrukciu kľúča a počet účastníkov *n* môže ľubovoľne stúpať bez opätovného prerozdelenia podielov ostatných účastníkov. Shamirova schéma neumožňuje odhaliť podvádzajúceho účastníka a je určená pre rovnocenných účastníkov.

Hlavná myšlienka konštrukcie pri tejto schéme spočíva v tom, že ľubovoľná skupina *t* účastníkov z celkovej *n* prvkovej skupiny môže zrekonštruovať kľúč. Pri tom sa využíva poznatok, že polynóm
stupňa *t* – 1 je jednoznačne určený *t* rôznymi bodmi.



Obr. 1. Polynóm

Na riešenie schém zdieľania tajomstva máme viacero možností a jednou z nich je využitie Lagrangeovho interpolačného polynómu, ktorý je riešením nasledujúcej úlohy: Nech je daných *t* rôznych bodov (x_i, y_i) pre $i = 1, 2, \ldots, t$. Nájdite polynóm $f(x)$ taký, že $f(x_i) = y_i$ pre $i = 1, 2, \ldots, t$. Riešením môže byť polynóm:

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

Lagrangeov interpolačný polynóm môžeme používať v ľubovoľnom konečnom poli *GF(q)*. My sa budeme zaoberať len prípadom, keď $q = p$, kde p je prvočíslo. Teda budeme pracovať v konečnom poli Z_p zvyškových tried podľa prvočíselného modulu p.
Nech počet všetkých účastníkov schémy je n a nech prístupovou množinou je každá množina, ktorá má aspoň t účastníkov. Úlohou dôveryhodnej osoby je najskôr vybrať kľúč K z množiny kľúčov $\mathcal{K}$, kde množina kľúčov $\mathcal{K} = Z_p$, pričom $p > n$. Dôveryhodná osoba, okrem kľúča $K = a_0$, náhodne vygeneruje koeficienty $a_1, a_2, \ldots, a_{t-1} \in Z_p$ pre polynóm stupňa $t - 1$. Polynóm vyzerá nasledovne:

$$f(x) = K + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \qquad (2)$$

Po získaní inicializačného polynómu dôveryhodná osoba vypočíta podiely pre účastníkov schémy. Vyberie n navzájom rôznych nenulových čísel $x_1, x_2, \ldots, x_n$ zo Z_p a následne vypočíta podiely s_i na kľúči pre jednotlivých účastníkov $P_1, P_2, \ldots, P_n$ podľa vzťahu:

$$s_i = f(x_i) = K + a_1 x_i + a_2 x_i^2 + \ldots + a_{t-1} x_i^{t-1} \qquad (3)$$

Účastník P_i pre $i = 1, 2, \ldots, n$ dostane svoj podiel ako dvojicu (x_i, s_i). Súkromná informácia účastníka P_i, teda podiel, je hodnota s_i. Hodnoty $x_1, x_2, \ldots, x_n$ sú obvykle verejne známe. V praxi sa obvykle používa $x_i = i$. Po doručení podielov jednotlivým účastníkom, úloha dôveryhodnej osoby končí.

* Vedúci práce

Pri *(t, n)*-prahovej schéme pre jednoznačnú rekonštrukciu kľúča potrebujeme poznať minimálne *t* podielov na kľúči *K*. Nech poznáme *l* podielov, pričom $l \geq t$. Potom sa môžeme pokúsiť zostaviť polynóm *t – 1* stupňa pomocou opísaného Lagrangeovho interpolačného polynómu. Je zrejmé, že v prípade *l > t* platí:

$$a_t = a_{t+1} = \ldots = a_{l-1} = 0$$

Pre jednoduchosť označíme podiely, ktoré máme k dispozícii (x_i, s_i), $i = 1, 2, \ldots, l$.

$$f(x) = \sum_{i=1}^{l} s_i \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} = \sum_{i=1}^{t} s_i \left(\prod_{1 \leq j \leq t; j \neq i} \frac{x - x_j}{x_i - x_j} \right) = \sum_{i=1}^{n} s_i \left(\prod_{1 \leq j \leq n; j \neq i} \frac{x - x_j}{x_i - x_j} \right) \quad (4)$$

Absolútny člen a_0 tohto polynómu je kľúč $K = a_0 = f(0)$. Z toho vyplýva, že nie je pre nás podstatný celý polynóm, ale len hodnota a_0. Keď dosadíme $x = 0$ do predchádzajúcej rovnice dostaneme výraz:

$$K = f(0) = \sum_{i=1}^{t} s_i \left(\prod_{1 \leq j \leq t; j \neq i} \frac{-x_j}{x_i - x_j} \right) = \sum_{i=1}^{n} s_i \left(\prod_{1 \leq j \leq n; j \neq i} \frac{-x_j}{x_i - x_j} \right) \quad (5)$$

V prípade, že je prvá súradnica bodov x_i verejne známa, môžeme si súčin v poslednej zátvorke vypočítať dopredu. Toto sa využíva pri overovaní perfektnosti Shamirovej schémy a uvedený súčin (keď tajný kľúč skladá všetkých *n* účastníkov schémy) označujeme ako S_{x_i} . Teda:

$$S_{x_i} = \prod_{1 \leq j \leq n; j \neq i} \frac{-x_j}{x_i - x_j} \quad (6)$$

Existuje aj ďalší spôsob výpočtu, ako môže množina účastníkov *l* zrekonštruovať kľúč $K = a_0$. Keďže poznáme podiely účastníkov z minimálnej prístupovej štruktúry, môžeme si vyjadriť vzťah medzi koeficientmi polynómu a známymi podielmi pomocou sústavy rovníc.

$$\begin{array}{ccccccccc} K & + & a_1 x_1 & + & \ldots & a_{t-1} x_1^{t-1} & = & s_1 \\ K & + & a_1 x_2 & + & \ldots & a_{t-1} x_2^{t-1} & = & s_2 \\ \vdots & & \vdots & & \ddots & \vdots & & \vdots \\ K & + & a_1 x_t & + & \ldots & a_{t-1} x_t^{t-1} & = & s_t \end{array} \quad (7)$$

Túto sústavu je možné zapísať aj v maticovom tvare.

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} K \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_t \end{pmatrix} \quad (8)$$

Matica *A* tejto sústavy je Vandermondova matica, ktorá nezávisí od zvoleného polynómu, ani od podielov na kľúči, ale iba od známych $x_1, x_2, \ldots, x_t$. Pre determinant Vandermondovej matice platí:
$\det A = (x_2 - x_1)(x_3 - x_1) \ldots (x_t - x_1)(x_3 - x_2)(x_4 - x_2) \ldots (x_t - x_2) \ldots (x_t - x_{t-1})$

$$\det A = \prod_{i,j=1; j<i}^{t} (x_i - x_j) \quad (9)$$

Determinant Vandermondovej matice v prípade prvočíselného modulu nebude nikdy nulový. Sústava rovníc bude mať vždy len jedno riešenie.

Teraz si ukážeme rekonštrukciu kľúča pomocou Lagrangeovho interplačného polynómu. Pre náš prípad uvažujme o prahovej (3, 5)-schéme v Z_{11}, teda $t = 3$, $n = 5$ a $p = 11$. Dôveryhodná osoba vyberie kľúč $K = a_0 = 2$ a koeficienty $a_1 = 9$, $a_2 = 7$. Dostaneme polynóm:

$$f(x) = 7x^2 + 9x + 2$$

Potom dôveryhodná osoba vypočíta podiely pre účastníkov schémy x_i. Súradnice x_i budú verejné a bude platiť $x_i = i$. Druhú súradnicu odošle účastníkom. Tí dostanú nasledujúce podiely: $s_1 = 7$, $s_2 = 4$, $s_3 = 4$, $s_4 = 7$, $s_5 = 2$.

Keď sa budú prvý traja účastníci pokúšať zrekonštruovať kľúč pomocou Lagrangeovho interpolačného polynómu, dosadia do vzorca $x = 0$. Dostanú kľúč:

$$7\frac{(0-2)(0-3)}{(1-2)(1-3)} + 4\frac{(0-1)(0-3)}{(2-1)(2-3)} + 4\frac{(0-1)(0-2)}{(3-1)(3-2)} =$$
$$10 + 10 + 4 = 2 (\mathrm{mod}\ 11)$$

Všetci piati účastníci budú rekonštruovať kľúč podobne:

$$7\frac{(0-2)(0-3)(0-4)(0-5)}{(1-2)(1-3)(1-4)(1-5)} + 4\frac{(0-1)(0-3)(0-4)(0-5)}{(2-1)(2-3)(2-4)(2-5)} +$$
$$4\frac{(0-1)(0-2)(0-4)(0-5)}{(3-1)(3-2)(3-4)(3-5)} + 7\frac{(0-1)(0-2)(0-3)(0-5)}{(4-1)(4-2)(4-3)(4-5)} +$$
$$2\frac{(0-1)(0-2)(0-3)(0-4)}{(5-1)(5-2)(5-3)(5-4)} = 2 + 4 + 7 + 9 + 2 = 2 (\mathrm{mod}\ 11)$$

Ako vidno hodnoty S_{x_i} sa dajú vypočítať dopredu:

$$S_{x_1} = 5\,,\ S_{x_2} = 1\,, S_{x_3} = 10\,, S_{x_4} = 6\,, S_{x_5} = 1\,.$$

Cieľom tejto práce je vybudovanie schémy podobnej Shamirovej prahovej schéme na okruhu zvyškových tried Z_m, v prípade, že *m* je zložené kladné celé číslo. V takom prípade niektoré prvky zo Z_m nemajú inverzný prvok vzhľadom na násobenie. Napr. nech Z_m je Z_6, $m = 3*2$. Prehľad násobenia je urobený v Cayleyho multiplikatívnej tabuľke. Z tejto tabuľky je zrejmé, že prvky 2 a 3 nemajú inverzné prvky. V modulárnej aritmetike platí, že prvky z danej množiny Z_m, ktoré sú súdeliteľné s modulom *m* nemajú v množine Z_m inverzný prvok vzhľadom na násobenie. Aj naďalej predpokladáme, že účastníci schémy budú očíslovaní hodnotami i_j z množiny $Z_m = \{0,1,2, \ldots, m-1\}$, pritom pre jednoduchosť budeme účastníkov schémy stotožňovať s ich indexmi. Teda o množine účastníkov

schémy $M = \{i_1, i_2, \ldots, i_n\}$ budeme predpokladať, že M je podmnožinou Z_m. Navyše, z typografických dôvodov , pri písaní vzorcov "prečíslujeme" množinu M do tvaru $M = \{1, 2, \ldots m\text{-}1\}$.

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tab. 1. Cayleyho multiplikatívna tabuľka v Z_6

Okruh Z_m je vzhľadom na sčítanie komutatívna grupa, ale vzhľadom na násobenie je to iba pologrupa, v ktorej množina prvkov nesúdeliteľných s faktorom m tvorí multiplikatívnu podgrupu Z^*_m. Preto, ak sa pokúsime o modifikáciu Shamirovej schémy, narazíme na nasledujúce problémy:

1. **Problém:** Pri určenom prahu, nemusí každá skupina účastníkov, ktorej početnosť je väčšia, alebo rovná prahu, byť schopná zrekonštruovať kľúč. Problém je v tom, že rozdiely čísel priradených účastníkom, ktoré sa vyskytujú v menovateľoch koeficientov Lagrangeovho polynómu, nemusia mať v Z_m inverzný prvok. Ak budeme kľúč rekonštruovať pomocou Lagrangeovho interpolačného polynómu potom v prípade, že v menovateli jedného zo súčinov S_{x_i} bude číslo súdeliteľné s m, tak kľúč nebude zrekonštruovaný, keďže nebude k tomuto číslu existovať inverzný prvok. Podobná situácia nastane aj keď sa pokúsime kľúč zrekonštruovať riešením matice. Z toho vyplýva, že nebude možné náhodné prideľovanie prvkov pre výpočet podielov z množiny Z_m, ale bude sa musieť použiť systematický výber.
2. **Problém:** Môže sa stať, že istá skupina účastníkov schémy bude autorizovanou množinou, pritom jej nadmnožina autorizovanou nebude. To by dávalo celkom pekný príklad nemonotónnej prístupovej štruktúry.
3. **Problém:** Dá sa očakávať, že takéto schémy nebudú perfektné schémy zdieľania tajomstva.

Pri modifikácii Shamirovej prahovej schémy budeme uvažovať hlavne o funkcii dílera, ktorý musí zabezpečiť vybranie jednotlivých účastníkov schémy tak, aby schéma, vzhľadom na ich očíslovanie, bola funkčná. V ďalšej časti sa budeme zaoberať problémami 1) – 3), ktoré budeme riešiť hlavne v tom prípade keď $m = xy$ je súčinom dvoch prvočísel.

Najskôr sa budeme zaoberať takým očíslovaním účastníkov schémy, pri ktorom rozdielom ľubovoľnej dvojice pridelených čísel nevznikne číslo súdeliteľné s prvočíslami, ktorých súčinom je číslo m. Ak číslo m je súčinom konečného počtu prvočísel a číslo x je z nich najmenšie, tak Z_m je rozdelené na x zvyškových tried podľa modulu x. Je zrejmé, že díler nemôže prideliť rôznym účastníkom schémy čísla z tej istej triedy podľa modulu x, lebo ich rozdiel by bol deliteľný x-om a teda súdeliteľný s modulom m. Teda účastníkov môžeme očíslovať maximálne x číslami, aby rozdielom ľubovoľnej dvojice čísel nevzniklo číslo súdeliteľné s m. Táto podmienka je zrejmá z existencie zvyškových tried podľa modulu x. Teda díler musí nutne prideliť čísla, ktoré reprezentujú rôzne zvyškové triedy podľa modulu x. Z toho vyplýva, že množina čísel pridelených na očíslovanie účastníkov schémy môže mať maximálne x prvkov. Najjednoduchší spôsob ako tieto čísla prideliť, je zobrať prvých x čísel zo Z_m počnúc od 1, alebo zobrať ľubovoľných x čísel idúcich za sebou, lebo tie predstavujú rôzne zvyškové triedy podľa modulu x. Nestačí však zvoliť čísla, ktoré reprezentujú rôzne zvyškové triedy podľa modulu x, ale musia byť z rôznych zvyškových tried aj podľa modulu y.

Príklad: Nech Z_m je Z_{15}, $m = 5*3$, $x = 3$.

Zvyškové triedy v Z_{15} podľa modulu *3*

1	2	3
4	5	6
7	8	9
10	11	12
13	14	

Zvyškové triedy v Z_{15} podľa modulu *5*

1	2	3	4	5
6	7	8	9	10
11	12	13	14	

V stĺpcoch tabuliek uvádzame prvky zo Z_{15} rozdelené do jednotlivých tried podľa modulu 3 a 5. V tabuľkách nefiguruje *0,* lebo tá sa nepridelíuje žiadnemu účastníkovi schémy Maximálne množiny M čísel, ktoré je možné prideľovať účastníkom, tvoríme tak, že ich vyberáme z rôznych tried ekvivalencie podľa modulu 3. Musíme však prihliadať na fakt, aby to neboli prvky z jednej triedy ekvivalencia podľa modulu 5. Potom môžeme voliť $M = \{1, 2, 3\}$. Iné možnosti pridelenia sú napr. $\{1, 8, 12\}$, $\{7, 8, 9\}$. V tomto prípade nie je napr. možné zobrať trojicu obsahujúcu čísla 1 a 11 aj keď sú v rôznych zvyškových triedach podľa modulu *3* ale ich rozdiel je súdeliteľný s 5. Podobne 4 a 14 atď. Môžeme si všimnúť, že ide o posúvanie prvkov 1 a 11 a 1 a 6 po diagonále.

Ukážeme si rekonštrukciu kľúča pre (2, 3)-prahovú schému v Z_{15}, pričom rekonštruovať kľúč budú všetci traja účastníci v prípade, že volíme čísla účastníkov pomocou množiny $M = \{1, 2, 3\}$. Dôveryhodná osoba vyberie kľúč $K = a_0 = 3$ a koeficient $a_1 = 5$. Dostaneme polynóm:

$$f(x) = 5x + 3$$

Podiely účastníkov sú: $s_1 = 8$, $s_2 = 13$, $s_3 = 3$. Rekonštrukciou kľúča dostanú:

$$8\frac{(0-2)(0-3)}{(1-2)(1-3)} + 13\frac{(0-1)(0-3)}{(2-1)(2-3)} + 3\frac{(0-1)(0-2)}{(3-1)(3-2)} =$$

$$9 + 6 + 3 = 3 (\mathrm{mod} 15)$$

Uvažujme o prípade, že sa o rekonštrukciu kľúča pokúsi tá istá skupina účastníkov , ktorá bude rozšírená

o účastníka, ktorému je pridelené číslo 6. Jeho podiel je $s_6 = 3$. Rekonštrukcia kľúča bude nasledovná:

$$8\frac{(0-2)(0-3)(0-6)}{(1-2)(1-3)(1-6)}+13\frac{(0-1)(0-3)(0-6)}{(2-1)(2-3)(2-6)}+$$
$$3\frac{(0-1)(0-2)(0-6)}{(3-1)(3-2)(3-6)}+3\frac{(0-1)(0-2)(0-3)}{(6-1)(6-2)(6-3)}=$$
$$\frac{12}{5}+6+6+\frac{1}{5}$$

Táto skupina kľúč nezrekonštruuje, lebo k 5 neexistuje inverzný prvok v Z_{15} vzhľadom na násobenie. Z toho vyplýva, že takáto schéma je príkladom nemonotónnej schémy.

V ďalšej časti sa budeme zaoberať pridelením čísel účastníkom v Z_m, kde m je súčinom dvoch rôznych prvočísel x a y, pri ktorom rozdielom niektorých dvojíc v menovateli koeficienta S_{xi} vznikne číslo súdeliteľné s m, ale vykráti sa s čitateľom. Ak M je maximálna množina čísel pridelených účastníkom schémy, tak čitateľ koeficienta S_{xi} obsahuje len prvky z množiny M. To znamená, že množina M musí obsahovať čo najviac násobkov čísiel x a y. Je potrebné si uvedomiť, že najprísnejšie podmienky na množinu M sú kladené, ak ľubovoľná dvojica má zrekonštruovať kľúč. V tomto prípade, ak v menovateli vznikne číslo súdeliteľné s x, tak v čitateli musí byť násobok čísla x, alebo ak v menovateli vznikne číslo súdeliteľné s y, tak v čitateli musí byť násobok čísla y. Z toho vyplýva, že množina M bude obsahovať iba niektoré násobky čísiel x a y. Pri väčších počtoch účastníkov, potrebných na rekonštrukciu kľúča sa bude dať množina M za istých podmienok zväčšiť a to v prípade, že v čitateli bude navyše násobok čísla x alebo y.

Ďalším dôležitým faktom je, že na množine Z_m rozdielom ľubovoľného násobku čísla x s ľubovoľným násobkom čísla y nikdy nevznikne číslo deliteľné x – om alebo y – om, pričom do úvahy neberieme nulový násobok, lebo nulu neprideľujeme a taktiež rozdielom ľubovoľného násobku čísla x *(y)* s iným násobkom čísla x *(y)* nikdy nevznikne číslo deliteľné y – om (x – om). Vyplýva to z toho, že všetky násobky čísla x predstavujú inú zvyškovú triedu vzhľadom na y a naopak všetky násobky čísla y predstavujú inú zvyškovú triedu vzhľadom na x.

Teraz si ukážeme postup tvorby množiny M najskôr pre $t = 2$ a potom pre $t > 2$. Súčasne si opisovaný postup vysvetlíme na Z_{33}.

Množina M je maximálna množina pre daný prah.

Predpoklad: Nech $m = x * y$, $x < y$.

Postup tvorby množiny M:

Vieme, že do M môžu byť zaradené len násobky x a y. Spomedzi týchto násobkov musíme vylúčiť tie čísla $v \in Z_m$, pre ktoré existujú $z \in M$ a $1 \le c \le x$ také, že $v - z = c\,x^n$ pre $n \ge 2$. Toto vylučovanie robíme po každom pridaní nového prvku. Z toho vyplýva, že jedna z možností pre tvorbu množiny M je nasledujúca:

Zoberieme násobky čísla x až po x^2, potom násobky x^2 po x^3 a tak pokračujeme až po x^n, kde $x^n < x * y$. Takýmto výberom zabezpečíme, že rozdielom ľubovoľných dvoch násobkov čísla x nedostaneme mocninu čísla x, lebo inak by sme museli v čitateli zabezpečiť mocninu x, čo nie je možné urobiť vždy. Keďže $x < y$ násobky y zaradíme do M všetky, lebo Z_m určite obsahuje len násobky prvej mocniny y. Z takto vytvorenej množiny M ľubovoľná dvojica zrekonštruuje kľúč. Prvkov, ktoré sú násobkom x je viac ako tých, čo sú násobkom y. Uvedená množina M je maximálna, z ktorej sa dajú očíslovať dvojice účastníkov, lebo čísla, ktoré sú násobkom y padnú do rôznych tried ekvivalencie podľa modulu x, ktoré sú v tvare: $x*k+1$, $x*k+2$, … , $x*k+(x-1)$ a násobky x predstavujú padnú do poslednej triedy ekvivalencie $x*k$. Keďže v množine Z_m ostali iba čísla $x*k+1$, $x*k+2$, … , $x*k+(x-1)$, tak ich pridaním do množiny M by sme vedeli zobrať dvojicu, ktorej rozdiel je $x*k$ a čitateľ násobok čísla x by neobsahoval.

V nasledujúcej časti budeme používať toto označenie:

M – maximálna množina čísel pre daný prah t

V – množina vylúčených čísel pre daný prah t

Z – množina zostávajúcich čísel

$Z_m = M \cup V \cup Z \cup \{0\}$

Pre náš konkrétny príklad teda platí:

Z_{33}, $m = 3*11$, $x = 3$, $y = 11$.

$M = \{3, 6, 9, 18, 27, 11, 22\}$

Vylúčené čísla: $V = \{12, 15, 21, 24, 30, 2, 20, 29, 4, 13, 31\}$

$12 - 3 = 9$, $15 - 6 = 9$, $21 - 3 = 18$, $24 - 6 = 18$, $30 - 3 = 27$, $11 - 2 = 9$, $20 - 11 = 9$,

$29 - 11 = 18$, $22 - 4 = 18$, $22 - 13 = 9$, $31 - 22 = 9$.

$Z = \{1, 5, 7, 8, 10, 14, 16, 17, 19, 23, 25, 26, 28, 32,\}$

Je zrejmé, že z množiny M môžeme podiely prideľovať aj pre prahové schémy pre $t > 2$, lebo rovnako ako pri dvoch účastníkoch dôjde k vykráteniu čitateľa s menovateľom. Podobne z množiny M, ktorá je maximálna pre prah t, budeme môcť prideľovať podiely účastníkom pre prahy väčšie ako t. Z toho vyplýva, že keď budeme do množiny M pridávať nový prvok, je potrebné preskúmať najhorší možný prípad s týmto prvkom.

Postupne budeme zvyšovať prah účastníkov, ktorí budú schopní zrekonštruovať kľúč a snažiť sa čo najviac zväčšiť množinu M. Ako už bolo spomenuté prvkov, ktoré sú násobkom x je viac ako tých, čo sú násobkom y. Preto bude jednoduchšie zabezpečiť, aby náhodne vybraná t – tica obsahovala násobok čísla x. Z toho dôvodu budeme najskôr vkladať prvky, ktoré predstavujú novú triedu ekvivalencie vzhľadom na y, čím zabezpečíme, že rozdielom nového prvku s ľubovoľným prvkom z M nevznikne číslo deliteľné y. Prvý nový prvok môžeme pridať pri t účastníkoch, pri ktorých platí $t=x+1$, lebo máme $x - 1$ prvkov, ktoré sú násobkom y, pridaním jedného prvku budeme mať x – tý prvok a posledný prvok bude určite násobok čísla x, čo je dôležité preto, lebo rozdielom nového prvku s jedným zo zvolených prvkov vznikne číslo deliteľné x. Takto som zvolil najhorší možný prípad, keď som sa snažil vybrať t - ticu, ktorá neobsahuje násobok čísla x.

Z toho vyplýva, že v každom kroku je možné pridať maximálne jeden nový prvok, inak viem zobrať takú skupinu, ktorá neobsahuje násobok čísla *x*. Takto pokračujeme až dovtedy kým mi ostanú čísla, ktorých zvyšková trieda v množine *M* vzhľadom na *y* už je. Pridať nový prvok bude možné iba pri takom prahu *t*, ktorý mi zabezpečí aspoň jeden násobok čísla *y*. Pri tom treba dávať pozor na to, že rozdielom viacerých čísel môže vzniknúť číslo deliteľné *y* a čitateľ obsahuje len jeden násobok čísla *y*. Potom bude potrebné zvýšiť prah *t*, ktorý zabezpečí, že ľubovoľná *t* – tica obsahuje viac násobkov čísla *y*.

Vráťme sa k nášmu príkladu.
Nový prvok je možné pridať až pri $t = x+1$, čiže $t = 3+1 = 4$.
Pri $t = 3$ to nie je možné, lebo keď pridám ľubovoľný prvok, môžem zobrať čísla 11 a 22 a rozdielom mi určite vznikne číslo deliteľné tromi.
Teraz si rozpíšeme aké triedy ekvivalencie podľa modulu 11 máme zastúpené v *M*.
$3 \in 11k+3$, $6 \in 11k+6$, $9 \in 11k+9$, $18 \in 11k+7$, $27 \in 11k+5$,
$11 \in 11k$, $22 \in 11k$.
Pre $t = 4$ pridáme prvok patriaci do novej triedy ekvivalencie podľa mod 11 napr. $1 \in 11k+1$.
Vylúčime prvky 10 (10 – 1 = 9), 19 (19 – 1 = 18), 28 (28 – 1 = 27).
$M = \{3, 6, 9, 18, 27, 11, 22, 1\}$
$V = \{12, 15, 21, 24, 30, 2, 20, 29, 4, 13, 31, 10, 19, 28\}$
$Z = \{5, 7, 8, 14, 16, 17, 23, 25, 26, 32\}$

Pre $t = 5$ pridáme napr. $8 \in 11k+8$.
Vylúčime prvky 17 (17 – 8 = 9), 26 (26 – 8 = 18).
$M = \{3, 6, 9, 18, 27, 11, 22, 1, 8\}$
$V = \{12, 15, 21, 24, 30, 2, 20, 29, 4, 13, 31, 10, 19, 28,17,26\}$
$Z = \{5, 7, 14, 16, 23, 25, 32\}$

Pre $t = 6$ pridáme napr. $32 \in 11k+10$ – zároveň je to posledná nová trieda ekvivalencie podľa modulu 11 aká nám v *Z* ostala.
Vylúčime prvky 5 (32 – 5 = 27), 14 (32 – 14 = 18), 23 (32 – 23 = 9).
$M = \{3, 6, 9, 18, 27, 11, 22, 1, 8, 32\}$
$V = \{12, 15, 21, 24, 30, 2, 20, 29, 4, 13, 31, 10, 19, 28, 17, 26, 5, 14, 23\}$
$Z = \{7, 16, 25\}$

Množina *M* je maximálna aj pre prahy $t = 7$, $t = 8$.
Pri prahu $t = 9$ môžeme pridať napr. 24. V takom prípade budeme mať prahovú schému (9, 11) a tým máme istotu že jeden prvok bude 9, 18 alebo 27. Prvky 12,15, 21,30 pridať nemôžeme lebo by mohol rozdielom vzniknúť číslo 11 alebo 22.

Pre $t = 9$ pridáme 24.
$M = \{3, 6, 9, 18, 27, 11, 22, 1, 8, 32, 24\}$
$V = \{12, 15, 21, 30, 2, 20, 29, 4, 13, 31, 10, 19, 28, 17, 26, 5, 14, 23\}$
$Z = \{7, 16, 25\}$
Pre t = 10 sa množina M nemení, lebo pridaním ľubovoľného prvku môže vzniknúť rozdiel 11 alebo 22.

Pre $t = 11$ môžeme pridať ďalší prvok, lebo zvýšením prahu sme zabezpečili, zobratie aspoň jedného prvku z triedy ekvivalencie $11k$ podľa modulu 11. Pridáme napr. $7 \in 11k+7$.
Vylúčim prvky 16 (16 – 7 = 9), 25 (25 – 7 = 18).
$M = \{3, 6, 9, 18, 27, 11, 22, 1, 8, 32, 24, 7\}$
$V = \{12, 15, 21, 30, 2, 20, 29, 4, 13, 31, 10, 19, 28, 17, 26, 5, 14, 23, 16, 25\}$

Ďalej postupujeme analogicky až po $t = 32$ a $M = Z_{33} - \{0\}$.

Ďalej uvažujme Z_m, kde *m* sa dá napísať ako mocnina jedného prvočísla x^n.
Postup tvorby *M* pre $t = 2$ je podobný ako v predchádzajúcom prípade. Zoberieme násobky čísla *x* až po x^2, potom násobky x^2 po x^3 a tak pokračujeme až po x^{n-1}a doplníme prvými $n-1$ prvkami zo Z_m. Z množiny Z_m musíme vylúčiť tie čísla $v \in Z_m$, pre ktoré existujú $z \in M$ a $1 \leq c \leq x$ také, že $v - z = c\,x^n$ pre $n \geq 2$. Toto vylučovanie robíme po každom pridaní nového prvku. Nový prvok môžem pridať až keď platí $t = x+1$ a vždy pridávam prvok, ktorého trieda ekvivalencie podľa modulu *x* v množine *M* je najmenej zastúpená. Množina *M* nebudeme môcť rozšíriť pri prahoch $t = x + 1 + x*c$, kde $c \in N$, lebo v týchto prípadoch môže rozdielom vzniknúť niekoľko čísel deliteľných *x* a teda budeme musieť zabezpečiť, že ľubovoľná skupina obsahuje viacero násobkov čísla x.
Príklad:
Z_{27}, $m = 3^3$, $x = 3$.
$M = \{3, 6, 9, 18, 1, 2\}$
Vylúčené čísla: $V = \{12, 15, 21, 24, 10, 19, 11, 20\}$
12 – 3 = 9, 15 – 6 = 9, 21 – 3 = 18, 24 – 6 = 18,
10 – 1 = 9, 19 – 1 = 18, 11 – 2 = 9, 20 – 2 = 18.
$Z = \{4, 5, 7, 8, 13, 14, 16, 17, 22, 23, 25, 26\}$

Pre $t = 3$ množina *M* sa nemení, keď pridáme ľubovoľný prvok môže vzniknúť rozdielom číslo patriace do triedy ekvivalencie $3k$ podľa modulu 3, preto musím zabezbečiť skupinu, ktorá obsahuje aspoň jedno číslo z tejto triedy ekvivalencie $3k$.
(Môžem zobrať 1, 2, a nové pridané číslo napr. 4, 4 – 1 = 3.)

Pre $t = 4$ pridáme 4.
$M = \{3, 6, 9, 18, 1, 2, 4\}$
$V = \{12, 15, 21, 24, 10, 19, 11, 20, 13, 22\}$
$Z = \{4, 5, 7, 8, 14, 16, 17, 23, 25, 26\}$

Pre $t = 5$ pridáme 5.
$M = \{3, 6, 9, 18, 1, 2, 4, 5\}$
$V = \{12, 15, 21, 24, 10, 19, 11, 20, 13, 22, 14, 23\}$
$Z = \{7, 8, 16, 17, 25, 26\}$

Pre $t = 6$ množina M sa nemení, keď pridáme ľubovoľný prvok môžu vzniknúť dve čísla z triedy ekvivalencie $3k$ podľa modulu 3 súčasne, preto musím zabezbečiť skupinu, ktorá obsahuje aspoň dve čísla z tejto triedy ekvivalencie $3k$.
Napr. 7 – 1 = 6, 7 – 4 = 3.

Pre $t = 7$ pridáme 7.
M = {3, 6, 9, 18, 1, 2, 4, 5, 7}
V = {12, 15, 21, 24, 10, 19, 11, 20, 13, 22, 14, 23, 16, 25}
Z = {8, 17, 26}

Pre $t = 8$ pridáme 8.
M = {3, 6, 9, 18, 1, 2, 4, 5, 7, 8}
V = {12, 15, 21, 24, 10, 19, 11, 20, 13, 22, 14, 23, 16, 25, 17, 26}

A analogicky postupujeme ďalej až po $t = 26$, $M = Z_{27}$ - {0}.
.

Zaoberali sme sa aj vytvorením maximálnej množiny prvkov M pre prah $t = 2$, pričom prvky vyberáme z množiny Z_m, kde modul m je súčinom dvoch mocnín prvočísel $m = x^p * y^q$.

Pri uvedených postupoch využívame poznatok:
Ak $a \neq xk \wedge b \neq xk \wedge p \neq q$ potom
$$ax^p - bx^q = x^q(ax^{p=q} - b) \Rightarrow ax^{p=q} - b \neq xk$$

V ďalšej časti si na príklade ukážeme, že schémy na Z_m, kde m nie je prvočíslo, nie sú perfektné. Najskôr sa budeme zaoberať prípadom, kde do úvahy berieme prvky zo Z_m, ktoré predstavujú navzájom rôzne triedy ekvivalencie podľa modulu všetkých faktorov m. Nech je daná prahová schéma (3,5) na Z_{35}, kľúč $K = a_0 = 4$ a koeficienty $a_1 = 7$, $a_2 = 1$. Polynóm vyzerá nasledovne:
$f(x) = x^2 + 7x + 4$
Potom dôveryhodná osoba vypočíta podiely pre účastníkov schémy. Súradnice x_i budú verejné a bude platiť $x_i = i$. Druhú súradnicu odošle účastníkom. Tí obdržia nasledujúce podiely: $s_1 = 12$, $s_2 = 22$, $s_3 = 34$, $s_4 = 13$, $s_5 = 29$.
Nech sa kľúč pokúsia zrekonštruovať prvý, druhý a piaty účastník. Potom dostanú:

$$12\frac{(0-2)(0-5)}{(1-2)(1-5)} + 22\frac{(0-1)(0-5)}{(2-1)(2-5)} + 29\frac{(0-1)(0-2)}{(5-1)(5-2)} =$$
$$30 + 10 + 34 = 4 \pmod{35}$$

Zistime teraz, či je daná schéma perfektná a či naozaj $t - 1$ účastníkov nezíska aspoň minimálnu informáciu o kľúči. Nech sa pokúsia zrekonštruovať kľúč len prvý a piaty účastník. Vedia, že minimálny počet podielov potrebných na zrekonštruovanie kľúča je 3 a $x_2 = 2$ je verejné, preto si môžu dopredu vypočítať hodnotu $S_{x_2} = 10$. K zisteniu kľúča K im chýba iba súradnica y_5.

$$12\frac{(0-2)(0-5)}{(1-2)(1-5)} + y_2\frac{(0-1)(0-5)}{(2-1)(2-5)} + 29\frac{(0-1)(0-2)}{(5-1)(5-2)} =$$
$$30 + 10y + 34 = 29 + 10y \pmod{35}$$

Naši účastníci sa pokúsia zmenšiť množinu kľúčov postupným dosadzovaním za y. Ich výstupy budú nasledovné:

y	0	1	2	3	4	5	6	7	8	9	10	11
K	29	4	14	24	34	9	19	29	4	14	24	34
y	12	13	14	15	16	17	18	19	20	21	22	23
K	9	4	14	24	34	9	24	34	9	19	29	4
y	24	25	26	27	28	29	30	31	32	33	34	
K	34	9	19	29	4	14	24	34	9	19	29	

Tab. 2.

Množina kľúčov sa zredukovala z 35 na 7 a teda schéma nie je perfektná.
Schéma nie je perfektná v prípade, že jeden z účastníkov má $x_i = i$ súdeliteľné s m. Z toho vyplýva, že perfektnosť schémy je možné dosiahnuť vylúčením týchto účastníkov. Potom však maximálny počet účastníkov nie je najmenší faktor p čísla m, ale $p - 1$(trieda ekvivalencie pk nemôže byť zahrnutá).
V prípade, že do úvahy berieme maximálne množiny najskôr pre $t = 2$, tak napr. v Z_{35} dostaneme M = {5,10,15,20,25,7,14,21,28}. Aby bola schéma perfektná, tak ľubovoľný člen Lagrangevho interpolačného polynómu nemôže po vykrátení obsahovať ani jeden násobok čísla 5 a ani 7. Preto môžeme brať do úvahy buď zvlášť iba násobky 5 alebo iba násobky 7. Ak berieme do úvahy iba násobky 5, nemôžeme zobrať 25, lebo po vykrátení ostane jedna 5 v čitateli. Teda dostaneme dve množiny M_1={5,10,15,20} a M_2 = {7,14,21,28}. Tieto množiny sú maximálne aj pre vyššie prahy a pre počet ich prvkov tak ako v predchádzajúcom prípade platí $p - 1$, kde p je najmenší faktor m. Perfektnosť schémy zaručíme výberom prvých mocnín násobkov čísla p alebo q, kde $m = p^a q^b$.
V prípade schém (m-1, m-1) na Z_m sú dané schémy perfektné (v každom člene Lagrangeovho interpolačného polynómu dôjde k vykráteniu všetkých čísiel súdeliteľných s m).

Odkazy na literatúru

[1] Stinson, D., R., "An Explication of Secret Sharing Schemes", Designs, Codes and Cryptography, Vol. 2, 1992, pp. 357-390.
[2] Matejíček, Ľ., "Multiúrovňové schémy zdieľania tajomstva", Diplomová práca, 2003