Slovenská technická univerzita v Bratislave
FAKULTA ELEKTROTECHNIKY A INFORMATIKY
Študijný odbor: INFORMATIKA

Bc. Ľuboš Matejíček

Multiúrovňové schémy na zdieľanie tajomstva

Diplomová práca

máj, 2003
Vedúci diplomovej práce: doc. RNDr. Ladislav Satko, CSc.

Čestné prehlásenie

Čestne prehlasujem, že som diplomovú prácu vypracoval samostatne s použitím uvedenej literatúry.

Ľuboš Matejíček

V Novej Dubnici, 16. mája 2003

Anotácia

Slovenská technická univerzita v Bratislave
FAKULTA ELEKTROTECHNIKY A INFORMATIKY
Študijný odbor: INFORMATIKA
Výberový blok: Bezpečnosť informačných technológií

Autor: Bc. Ľuboš Matejíček
Diplomová práca: Multiúrovňové schémy na zdieľanie tajomstva.
Vedúci diplomovej práce: doc. RNDr. Ladislav Satko, CSc.
Máj, 2003

Diplomová práca opisuje vlastnosti schém na zdieľanie tajomstva. Zameriava sa prevažne na multiúrovňové schémy založené na Shamirovej prahovej schéme. Nájdeme v nej popísaný algoritmus dôveryhodnej osoby a algoritmus kombinátora vhodný pre tieto schémy. Opisuje predpoklady, na ktorých je založená bezpečnosť týchto schém.

V práci sme ukázali, že funkčnosť multiúrovňovej schémy je závislá na verejne známych parametrov schémy. Ich vhodná voľba je teda kľúčová pri konštrukcii schémy. Navrhli a implementovali sme algoritmus, pomocou ktorého je možné overiť, či schéma s takto zvolenými parametrami bude funkčná.

Nevýhodou tohto algoritmu je veľká časová náročnosť, ktorá vyplýva z toho, že algoritmus musí prechádzať cez všetky potenciálne minimálne prístupové množiny účastníkov a pre každú zvlášť posúdiť, či táto množina účastníkov dokáže zrekonštruovať kľúč.

Annotation

Slovak University of Technology, Bratislava
FACULTY OF ELECTRICAL ENGINEERING
AND INFORMATION TECHNOLOGY
Degree Course: INFORMATICS

Author: Bc. Ľuboš Matejíček
Thesis: Multilevel schemes for secret sharing
Supervisor: doc. RNDr. Ladislav Satko, CSc.
2003, may

This thesis deals with properties of secret sharing. It aims mostly at multilevel schemes based on Shamir threshold scheme. The algorithm of trusted authority and the algorithm of combiner are described as both are convenient for use with such schemes. Also, preconditions on which the security of secret sharing is based on are described.

We have proved that functionality of a multilevel scheme depends on publicly known scheme parameters. It means that proper selection of these parameters is crucial for construction of such scheme. We have designed and implemented the algorithm which allows us to verify whether a scheme using certain parameters shall be functional.

A drawback of this algorithm is its operational complexity caused by a fact that all potential minimal sets of participants must be traversed through and for each one of them it must be evaluated whether a given set is capable of reconstruction of the key.

Poďakovanie

Ďakujem doc. RNDr. Ladislavovi Satkovi, CSc. za odborné vedenie diplomovej práce, pri ktorom mi venoval veľa času a trpezlivosti.

Obsah

I Úvod **1**

1 Čo poskytujú schémy na zdieľanie tajomstva **1**

II Analýza problému **2**

2 Zoznámenie sa s problematikou **2**

2.1 Základné pojmy 2

2.2 Prístupová štruktúra 5

2.3 Algoritmus dôveryhodnej osoby a algoritmus kombinátora 6

2.4 Návrh schémy 7

2.5 Pohľad útočníka 8

3 Opis prístupovej štruktúry **10**

3.1 Kumulatívne schémy 10

3.2 Monotónne obvody a množina prístupových množín 11

3.3 Konštrukcia schémy so všeobecnou prístupovou štruktúrou 13

3.4 Množina neprístupových množín 15

4 Vybrané schémy na zdieľanie tajomstva **18**

4.1 Schéma založená na čínskej zvyškovej vete 18

4.2 Shamirova prahová schéma 20

4.3 Kumulatívna schéma odhaľujúca podvádzajúceho účastníka 24

5 Zdieľanie tajomstva v multiúrovňových schémach **30**

5.1 Označenie v multiúrovňových schémach 30

5.2 Rozšírenie schémy 31

5.3 Prístupová štruktúra multiúrovňovej schémy 32

5.4 Konštrukcia schémy 33
5.5 Voľba polynómu 34
5.6 Matica systému 37
5.7 Algoritmus dôveryhodnej osoby 41
5.8 Príklady 41
5.8.1 Príklad úspešnej rekonštrukcie 42
5.8.2 Príklad neúspešnej rekonštrukcie 43
5.8.3 Výpočet kľúča z podielov neprístupovej množiny 43

III Opis postupu riešenia 45

6 Súvis s diplomovým projektom 45

7 Špecifikácia požiadaviek 47
7.1 Analýza problému 47
7.2 Výber použitých nástrojov 47

8 Návrh 51
8.1 Návrh dialógu 51

9 Implementácia 53
9.1 Inštalácia knižníc 53
9.1.1 Inštalácia knižnice Qt zo súboru *.tar.bz2 53
9.1.2 Inštalácia knižnice Qt zo súboru *.rpm 54
9.1.3 Inštalácia knižnice GMP 55
9.2 Nastavenie ciest 55
9.3 Vytvorenie programu multilevel-scheme 56

IV Výsledky a ich zhodnotenie 57

Časť I

Úvod

1 Čo poskytujú schémy na zdieľanie tajomstva

Existuje viacero dôvodov, ktoré motivujú k zdieľaniu tajomstva medzi viacerými osobami. Najčastejšie je to nedostatok dôvery jednej osoby a komplikovaná dostupnosť spoľahlivej osoby. Schémy na zdieľanie tajomstva predstavujú mocný nástroj na decentralizáciu dôvery medzi viacerých účastníkov.

V praxi sa stretávame s úlohami, v ktorých poskytujeme nejaké informácie, alebo služby určitému okruhu osôb, ale iba ak o ne požiadajú spoločne, nie jednotlivo. Príkladom môže byť bankový účet zdieľaný tromi účastníkmi (klientmi). Získať kľúč (heslo) a takto manipulovať s peniazmi na účte umožníme, len ak sa o získanie kľúča spoločne pokúsia aspoň dvaja účastníci.

Jedným zo spôsob riešenie je využitie arbitrovaného protokolu. Dôveryhodná osoba (arbiter) najprv overí totožnosť účastníkov usilujúcich sa o získanie kľúča. Následne rozhodne, či je množina účastníkov oprávnená na jeho získanie. Ak áno kľúč im vydá. Slabinou tohto protokolu je dostupnosť dôveryhodnej osoby (spoľahlivosť protokolu). Bezpečnosť protokolu je založená na nemožnosti skorumpovať dôveryhodnú osobu.

Iný spôsob riešenia ponúkajú schémy na zdieľanie tajomstva. V schéme na zdieľanie tajomstva dôveryhodná osoba vyberie kľúč a podiely na kľúči. Podiely obsahujú informáciu o kľúči, ktorá bude rozdelená medzi účastníkov tak, aby kľúč mohli zložiť len vopred vybrané množiny účastníkov.

Spoľahlivosť schém na zdieľanie tajomstva nie je založená na neustálej dostupnosti dôveryhodnej osoby. Dôveryhodná osoba musí podiely po ich vybraní doručiť cez bezpečný kanál účastníkom. Jej úloha tým končí a dôveryhodná osoba by mala následne zabudnúť kľúč aj podiely účastníkov. Časový interval, kedy sa môže útočník pokúsiť o korupciu dôveryhodnej osoby, je potom len do odovzdania posledného podielu na kľúči.

Časť II

Analýza problému

2 Zoznámenie sa s problematikou

2.1 Základné pojmy

Pojem **schéma na zdieľanie tajomstva** (skrátene schéma) sa používa v dvoch významoch. V užšom význame opisuje len spôsob výberu kľúča a podielov dôveryhodnou osobou. Častejšie znamená tento pojem matematický model, obsahujúci okrem algoritmu dôveryhodnej osoby aj algoritmus kombinátora a samozrejme podrobný opis vlastností tohto modelu.

Pri schémach na zdieľanie tajomstva predpokladáme, že spôsob výberu kľúča a podielov na kľúči je verejne známy. Väčšinou tiež predpokladáme aj zverejnenie ostatných parametrov schémy[1]. Jedinými privátnymi údajmi v schéme býva kľúč a podiely na kľúči.

- **Dôveryhodná osoba** $\mathcal{D}$, niekedy aj centrálna autorita, alebo rozdávač *(mutually trusted authority, dealer, server)* – všeobecne dôveryhodná osoba, ktorá vyberá kľúč a podiely účastníkov na kľúči. Jej úlohou je aj doručenie podielov účastníkom.
- **Kľúč** *(secret, key)* $K \in \mathcal{K}$ zvolený dôveryhodnou osobou. Je zdieľaný účastníkmi. Jeho získanie znamená získať chránené aktíva (informácie, prístup...).
- **Množina účastníkov schémy** $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n\}$ *(set of participants)*, ktorí spoločne zdieľajú kľúč K. Dôveryhodná osoba nepatrí do množiny účastníkov schémy.
- Privátna informácia, ktorú účastník P_i obdržal od dôveryhodnej osoby, sa nazýva **podiel i-teho účastníka na kľúči** a označuje sa s_i. Množinu, z ktorej budeme podiel s_i účastníka P_i vyberať, označujeme $\mathcal{S}_i$. Ak podiely všetkých účastníkov vyberáme z tej istej množiny ($\mathcal{S}_1 = \mathcal{S}_2 = \ldots = \mathcal{S}_n$), potom túto množinu označíme $\mathcal{S}$.

[1] Algoritmus kombinátora, prístupová štruktúra, ...

- **Kombinátor** je osoba, ktorú účastníci poverili zhromažďovaním podielov účastníkov. Po zhromaždení niekoľkých podielov sa kombinátor pokúsi o rekonštrukciu kľúča. Obvykle je to jeden z účastníkov.

- **Prístupová množina***(qualified set, access subset)* – množina účastníkov, ktorí sú spoločne schopní zrekonštruovať kľúč K (ich podiely sú dostatočné na získanie kľúča).

- **Neprístupová množina***(forbidden set,non-access subset)* – množina účastníkov, ktorá nemá žiadnu informáciu o kľúči. (Zložením podielov účastníkov neprístupovej množiny nie je možné získať žiadnu novú informáciu o kľúči.)

- **Semiprístupová množina** *(semi-access subset)* – množina účastníkov, ktorá nie je ani prístupová, ale ani neprístupová. Zložením podielov tejto množiny nie je možné zrekonštruovať kľúč, ale dá sa o ňom zistiť nejaká informácia (dá sa zmenšiť množina potenciálnych kľúčov, alebo aspoň spresniť pravdepodobnosť výberu kľúča).

Každá množina účastníkov je buď *prístupová*, *neprístupová*, alebo *semiprístupová*. V schémach na zdieľanie tajomstva obvykle predpokladáme, že množina všetkých účastníkov schémy je prístupová. Prázdna množina účastníkov býva naopak neprístupová.

Na lepšie objasnenie používaných pojmov uvedieme dve jednoduché schémy.

Schéma 1.

Inicializačná fáza

Dôveryhodná osoba náhodne vyberie $(k \cdot n)$-bitový kľúč K a kľúč rozdelí na n častí (podielov) po k bitoch, ktoré sa distribuujú medzi účastníkov. Podiely sú doručené účastníkom cez bezpečný kanál.

Rekonštrukčná fáza

O zloženie kľúča[2] sa môže pokúsiť množina všetkých n účastníkov $\mathcal{P}$.

$$K = s_1|s_2|\ldots|s_n$$

Ak niektoré z podielov nepoznáme, môžeme sa ich pokúsiť uhádnuť. Počet kľúčov, ktoré prichádzajú úvahy po poznaní m podielov, je $2^{k(n-m)}$. Všetky sú rovnako pravdepodobné.

[2]Operácia | znamená zreťazenie

Ak chýba už len niekoľko podielov, môžu sa účastníci pokúsiť uhádnuť kľúč. Ich šanca uhádnuť kľúč sa s každým ďalším známym podielom zlepšuje. Toto je veľkou slabinou tejto schémy.

Prístupovou množinou účastníkov je množina všetkých účastníkov $\mathcal{P}$. Neprístupovou je prázdna množina účastníkov. Každá iná podmnožina množiny $\mathcal{P}$ je semiprístupová.

Schéma 2.

Karnin-Green-Hellmanova schéma

Inicializačná fáza

Nech $\mathcal{S}$ je konečná množina a $(\mathcal{S}, +)$ je aditívna grupa. Dôveryhodná osoba náhodne vyberie podiely všetkých účastníkov $s_1, \ldots, s_n \in \mathcal{S}$. Nech výber každého prvku množiny $\mathcal{S}$ za podiel s_i je rovnako pravdepodobný a výber jednotlivých podielov nezávislý. Potom dôveryhodná osoba vypočíta kľúč K z množiny $\mathcal{K} = \mathcal{S}$, podľa vzťahu

$$K = s_1 + s_2 + \cdots + s_n \tag{1}$$

a rozdá podiely účastníkom.

Rekonštrukčná fáza

Získať kľúč, ak poznáme podiely všetkých účastníkov, znamená len dosadiť do vzorca (1). Ak však nepoznáme čo i len jeden z podielov, je uhádnutie kľúča rovnako náročné, ako keby sme nepoznali žiadny podiel. Posledný podiel môže zmeniť súčet na akýkoľvek. Zmena na každý prvok z $\mathcal{K}$ je rovnako pravdepodobná.

Táto schéma je oveľa bezpečnejšia ako predchádzajúca. Prístupovou množinou je množina všetkých účastníkov $\mathcal{P}$. Každá iná množina účastníkov je neprístupová, semiprístupové množiny účastníkov neexistujú.

Mali by sme zodpovedať aj na otázku, či na výpočet kľúča sú potrebné skutočne všetky podiely na kľúči. Ak by súčet niekoľkých podielov sa rovnal neutrálnemu prvku vzhľadom na operáciu $+$, kľúč by sme mohli dostať aj bez znalosti týchto podielov. Bolo by dokonca možné, že priamo jeden z podielov sa bude rovnať kľúču. Je to však veľmi nepravdepodobné. Z pohľadu útočníka[3], ktorý by chcel nájsť kľúč, je pravdepodobnosť, že podiel s_i sa rovná kľúču, je rovnako nízka ako pravdepodobnosť, že podiel sa rovná ľubovoľnému náhodne vybranému číslu z $\mathcal{K}$.

Pozícia útočníka po získaní jedného podielu nie je teda o nič silnejšia, ako keby nepoznal žiaden podiel a začal náhodne generovať možné kľúče a overovať, či náhodou nenatrafil na ten pravý.

[3]Uvažujme, že schéma má viac ako jedného účastníka.

Ak útočník získa ľubovoľných $m < n$ podielov a sčíta ich, dostane nejaké číslo K', ktoré by mohlo byť potenciálne kľúčom. Pravdepodobnosť, že $K' = K$ je rovnako malá ako pravdepodobnosť, že súčet ľubovoľných m náhodne vybraných čísel sa bude rovnať kľúču. Je to však rovnako nízka pravdepodobnosť ako to, že uhádneme kľúč pri náhodnom výbere jediného čísla.

2.2 Prístupová štruktúra

Rozdelenie množín účastníkov na prístupové, semiprístupové a neprístupové predstavuje jednu z najpodstatnejších charakteristík schémy na zdieľanie tajomstva. Toto rozdelenie množín účastníkov opisuje *prístupová štruktúra*.

Množina prístupových množín $\Gamma \subseteq 2^{\mathcal{P}}$ obsahuje všetky prístupové množiny účastníkov v danej schéme. **Množina neprístupových podmnožín** $\Delta \subseteq 2^{\mathcal{P}}$ obsahuje neprístupové množiny účastníkov v danej schéme($\Gamma \cap \Delta = \emptyset$).

Dvojicu (Γ, Δ) voláme **prístupová štruktúra** *(access structure)*. Ak neexistujú semiprístupové množiny účastníkov (čiže $\Gamma \cup \Delta = 2^{\mathcal{P}}$), nazývame prístupovú štruktúru **úplná prístupová štruktúra** *(complete access structure)*. Naopak ak existuje aspoň jedna semiprístupová množina účastníkov, nazývame prístupovú štruktúru **neúplná** *(incomplete)*.

Schému s neúplnou prístupovou štruktúrou budeme nazývať **neúplná schéma** *(incomplete, non-perfect scheme)*. Schému s úplnou prístupovou štruktúrou budeme volať **perfektná schéma** *(perfect scheme)*. V tejto práci sa budeme zaoberať len perfektnými schémami (s výnimkou schémy 1 a 5). Na opis prístupovej štruktúry perfektnej schémy sa obvykle používa len množina prístupových množín Γ. Množina neprístupových množín je jej doplnkom $\Delta = 2^{\mathcal{P}} \setminus \Gamma$.

Ak v prístupovej štruktúre platí, že každá nadmnožina prístupovej množiny účastníkov je tiež prístupová ($\forall \mathcal{A}_1 \in \Gamma \ ; \ \mathcal{A}_1 \subseteq \mathcal{A}_2 \Rightarrow \mathcal{A}_2 \in \Gamma$) a každá podmnožina neprístupovej množiny je tiež neprístupová ($\forall \mathcal{B}_1 \in \Delta \ ; \ \mathcal{B}_1 \supseteq \mathcal{B}_2 \Rightarrow \mathcal{B}_2 \in \Delta$), potom hovoríme, že prístupová štruktúra je **monotónna**. Schémy, ktoré nemajú monotónnu prístupovú štruktúru, sa používajú iba v prípade, ak prístupová štruktúra (Γ, Δ) nie je verejne známa a zároveň počet účastníkov schémy je dostatočne veľký. V tejto práci sa obmedzíme len na monotónne prístupové štruktúry.

Množinou minimálnych prístupových množín voláme takú podmnožinu Γ^- množiny prístupových množín, ktorej prvkami sú všetky také prístupové množiny účastníkov $\mathcal{A}$, ktorých všetky (nevlastné) podmnožiny nie sú prístupové ($\mathcal{B} \subset \mathcal{A} \subseteq \mathcal{P} \ ; \ \mathcal{A} \in \Gamma^- \Rightarrow \mathcal{B} \notin \Gamma$).

Množinou maximálnych neprístupových množín nazývame takú podmnožinu Δ^+ množiny neprístupových množín, ktorej prvkami sú všetky také neprístupové množiny účastníkov $\mathcal{A}$, ktoré by pridaním čo i len jedného nového účastníka prestali byť neprístupové ($\mathcal{A} \subset \mathcal{B} \subseteq \mathcal{P}\ ;\ \mathcal{A} \in \Delta^+ \Rightarrow \mathcal{B} \notin \Delta$).

V monotónnych schémach množina prístupových množín Γ jednoznačne vyplýva z množiny minimálnych prístupových množín Γ^-. Množinu Γ nazývame **uzáver množiny** Γ^- *(closure)* a označujeme ju $\mathrm{cl}(\Gamma^-)$.

$$\Gamma = \mathrm{cl}(\Gamma^-) = \{C \subseteq \mathcal{P}\ :\ \exists B \subseteq C,\ B \in \Gamma^-\}$$

Uveďme príklad:
Nech $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ a nech

$$\Gamma^- = \{\ \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\ \}$$

potom

$$\Gamma = \Gamma^- \cup \{\ \{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}\, \{P_1, P_2, P_3, P_4\}\ \}$$

Ak je schéma monotónna, potom jej prístupovú štruktúru (Γ, Δ) môžme popísať aj pomocou dvojice (Γ^-, Δ^+). Tento popis je väčšinou jednoduchší a elegantnejší. Je to preto, lebo $\Gamma^- \subseteq \Gamma$,$\Delta^+ \subseteq \Delta$ a počty prvkov Γ^- a Δ^+ sú často aj rádovo menšie oproti pôvodným množinám.

Jadrom **core Γ** prislúchajúcim k prístupovej štruktúru (Γ, Δ) nazývame množinu účastníkov, ktorí sú v aspoň jednej minimálnej prístupovej množine

$$\mathrm{core}\,\Gamma = \bigcup_{P \in \Gamma^-} P$$

Ak pre danú štruktúru platí $\mathrm{core}\,\Gamma = \mathcal{P}$ hovoríme, že prístupová štruktúra je **zapojená**. V ďalšom texte budeme hovoriť len o zapojených prístupových štruktúrach.

2.3 Algoritmus dôveryhodnej osoby a algoritmus kombinátora

Pri využívaní schém na zdieľanie tajomstva v praxi predpokladáme, že úlohy dôveryhodnej osoby a kombinátora sú výpočtové procesy. Skúsme sa teda na chvíľu zamyslieť nad vstupmi, výstupmi a úlohou týchto procesov (popísaných pomocou algoritmov). Pri návrhu schémy predpokladáme, že oba algoritmy sú verejné.

Algoritmus dôveryhodnej osoby je algoritmus, ktorý vyberá kľúč a podiely všetkých účastníkov tak, aby dodržal rozdelenie na prístupové, semiprístupové a neprístupové množiny dané prístupovou štruktúrou[4]. Algoritmus využíva prvky náhodnosti (pri opakovanom spúšťaní by mal vygenerovať pokiaľ možno iné podiely na kľúči, prípadne kľúč). Často algoritmus umožňuje dopočítať podiely na kľúči k už známemu kľúču K.

Algoritmus kombinátora má za úlohu vhodne skombinovať podiely účastníkov, ktoré má k dispozícii a zrekonštruovať kľúč. Vstupom algoritmu sú podiely účastníkov na kľúči. Ak množina účastníkov, ktorých podiely poznáme, je prístupová, výstupom algoritmu je kľúč. Ak však množina účastníkov nie je prístupová, potom výstup algoritmu nie je definovaný. Pri návrhu schémy musíme zobrať do úvahy aj praktické hľadisko – algoritmus kombinátora pre výpočet kľúča z podielov prístupovej množiny nesmie mať priveľkú zložitosť (časovú, pamäťovú...).

Nech $S = \{s_1, \ldots, s_n\}$ je množina podielov na kľúči. Potom algoritmus kombinátora[5] môžeme matematicky vyjadriť ako funkciu

$$f : 2^S \to \mathcal{K} \cup \{\emptyset\}$$

2.4 Návrh schémy

Schéma na zdieľanie tajomstva je matematický model, ktorý by mal popísať:

- množinu $\mathcal{K}$, z ktorej sa vyberá kľúč K a podiely jednotlivých účastníkov,
- algoritmus dôveryhodnej osoby,
- prístupovú štruktúra (Γ, Δ),
- množiny $\mathcal{S}_1, \ldots, \mathcal{S}_n$, z ktorých sa vyberajú podiely $s_1, \ldots, s_n$ a spôsob ich výberu (výpočet, alebo náhodný výber s presne popísanou hustou pravdepodobnosti),
- algoritmus kombinátora (spôsob ako sa možno z podielov prístupovej množiny dopracovať ku kľúču.),

[4]Poslednou úlohou dôveryhodnej osoby je doručiť podiely príslušným účastníkom cez bezpečný kanál.

[5]Predpokladajme, že algoritmus kombinátora vráti $\emptyset$ v prípade, ak z podielov nie je možné zrekonštruovať kľúč.

- množstvo informácie, o kľúči, ktoré je možné (teoreticky) získať pre semiprístupové množiny účastníkov.

Neúplné schémy[6] by naviac mali popísať, ktoré množiny účastníkov sú semiprístupové ($\mathcal{C} \in 2^{\mathcal{P}} \setminus (\Gamma \cup \Delta)$) a opis informácie o kľúči, ktorú môže semiprístupová množina účastníkov získať.

V niektorých schémach kombinátor pri rekonštrukcii kľúča naviac dokáže odhaliť podvádzajúceho účastníka. **Podvádzajúci účastník** je taký účastník schémy, ktorý k rekonštrukcii kľúča neprispeje svojim podielom s_i, ktorý obdržal od dôveryhodnej osoby. Podvádzajúci účastník prispeje falšovaným podielom $s_i' \neq s_i$. Na základe sfalšovaného podielu kombinátor (s veľkou pravdepodobnosťou) nezrekonštruuje skutočný kľúč.

Schéma, ktorá dokáže odhaliť podvádzajúceho účastníka (prípadne viacerých), by mala obsahovať okrem algoritmu odhalenia aj vyčíslenú pravdepodobnosť, že odhalenie nebude úspešné. Algoritmy odhalenia podvodu obvykle pripúšťajú, že s nepatrnou pravdepodobnosťou sa podvod odhaliť nepodarí.

2.5 Pohľad útočníka

Možnosti útočníka

Potenciálny útočník si môže určiť za úlohu viacero cieľov, ako narušiť predpokladaný životný cyklus schémy. Predpokladajme, že útočník môže využívať:

- značnú výpočtovú silu, ktorá v dobe návrhu schémy ešte nemusela existovať,
- pokrok vo vývoji algoritmov (môže využiť vlastné alebo cudzie algoritmy, ktoré v dobe návrhu schémy nemuseli byť známe).

Klasikácia útočníkov

Útočníkom, ktorý útočí sa schému, môže samozrejme byť ktokoľvek. Pre bezpečnosť každej schémy je potrebný vhodný výber dôveryhodnej osoby. Táto určí všetky tajné (kľúč) a privátne (podiely účastníkov) informácie v schéme.

Ďalšou osobou, ktorá rozhodne nesmie byť skorumpovaná, je kombinátor. Ten pri rekonštrukcii prvý spozná kľúč a teda ho môže potencionálne zneužiť.

Niektoré schémy na zdieľanie tajomstva dokážu s vysokou pravdepodobnosťou odhaliť podvádzajúceho účastníka. Vďaka tomu sú oveľa bezpečnejšie a dajú sa

[6] Schémy s neúplnou prístupovou štruktúrou.

využiť aj v prostredí, v ktorom by niektorí účastníci schémy mohli byť skorumpovaní. Nevýhodou schém umožňujúcich odhalenie podvádzajúceho účastníka zvyčajne býva dlhší podiel na kľúči.

Vonkajší útočník sa môže pokúsiť vydávať sa za účastníka schémy. Ak prostredie, v ktorom schéma pracuje, umožňuje overiť totožnosť účastníkov, potom kombinátor ľahko zabráni zmene identity.

Inou možnosťou obrany proti korupcii účastníkov, je overovanie pravosti podielov. Poslednou, často riskantnou, možnosťou je spoľahnúť sa, že na základe náhodne zvoleného nepravého podielu s'_i sa nepodarí získať žiadnu informáciu o kľúči. Veľmi často je totiž na základe nepravého podielu možné získať nejakú relevantnú informáciu o použitých pravých podieloch.

Pri útoku útočník môže poznať podiely na kľúči od jedného, alebo aj viacerých účastníkov. Zvyčajne predpokladáme, že útočník dokáže rozoznať pravý kľúč od nepravého. Ak množina účastníkov $\mathcal{A} \in \Gamma$, ktorých podiely útočník pozná, je prístupová, potom je jednoduché získať kľúč K pomocou algoritmu kombinátora. Ak $\mathcal{A} \in \Delta$ je neprístupová množina účastníkov, útočník môže rovno začať overovať kľúče z množiny $\mathcal{K}$. Jeho pozícia pri hľadaní kľúča nie je o nič výhodnejšia, ako keby nepoznal žiadny podiel.

Ochrana pred útokom

Ako sme spomenuli, niektoré schémy na zdieľanie tajomstva dokážu odhaliť podvádzajúceho účastníka. V niektorých schémach dokáže kombinátor odhaliť podvodníka[7] len na základe znalosti svojho podielu. Vtedy hovoríme o nepodmienenom odhalení podvádzajúceho účastníka.

Iné schémy umožňujú podmienené odhalenie podvádzajúceho účastníka. Vtedy kombinátor dokáže odhaliť podvodníka na základe znalosti viacerých podielov. Pri schémach umožňujúcich podmienené odhalenie podvodníka je možné odhaliť podvádzajúcich účastníkov len v prípade, ak ich počet nepresiahne istú kritickú hranicu.

[7]Niekedy je možné, že kombinátor síce nedokáže odhaliť podvádzajúceho účastníka, dokáže však aspoň zistiť, že podiely neboli úplne v poriadku.

3 Opis prístupovej štruktúry

3.1 Kumulatívne schémy

Rozdelenie množín účastníkov na prístupové, semiprístupové a neprístupové predstavuje jednu z najdôležitejších charakteristík schémy na zdieľanie tajomstva. Toto rozdelenie množín účastníkov opisuje prístupová štruktúra.

Od počiatku skúmania schém na zdieľanie tajomstva je aktuálna otázka, ako by sa dala zostrojiť schéma, ktorá by mohla mať akúkoľvek monotónnu prístupovú štruktúru. Znamenalo by to, že dokážeme zostrojiť schému, vždy keď nám niekto (napríklad zákazník) oznámi, ktoré množiny účastníkov majú byť prístupové.

Výskum schém na zdieľanie tajomstva ukázal, že podobné schémy je možné zostrojiť. Môžu byť dokonca aj perfektné. Ich slabinou je to, že dĺžka podielov býva oveľa dlhšia ako dĺžka kľúča. To je dôvod, prečo sú stále skúmané aj schémy, ktoré nemajú takú veľkú flexibilitu prístupovej štruktúry, ale zato majú oveľa kratšie podiely (pri rovnako dlhom kľúči).

Úplnú monotónnu schému na zdieľanie tajomstva so všeobecnou[8] prístupovou štruktúrou nazývame **kumulatívna schéma**. Pri výskume sa ukázalo, že kumulatívne schémy konštruujeme tak, že máme množinu častí podielov $\Phi = \{\varphi_1, \ldots, \varphi_m\}$ a každému z účastníkov schémy pridelíme niektoré z jej prvkov ($s_i \subseteq \Phi$, napríklad $s_1 = \{\varphi_1, \varphi_3, \varphi_4\}$) tak, aby množina účastníkov poznala všetky prvky množiny Φ práve vtedy, ak bude prístupová.

Nad časťami podielov následne zostrojíme novú úplnú schému m účastníkov s podielmi $\varphi_1, \ldots, \varphi_m$, v ktorej je prístupová len množina všetkých účastníkov. V pôvodnej schéme boli prvky $\varphi_1, \ldots, \varphi_m$ časťami podielov. V novej schéme sú však priamo podielmi.

V novej schéme je možné zloženie kľúča, len ak poznáme všetky jej podiely $\varphi_1, \ldots, \varphi_m$. Príkladom takej schémy je napríklad Karnin-Green-Hellmanova schéma[9], v ktorej kľúč vypočítame zo vzťahu

$$K = \varphi_1 + \varphi_2 + \cdots + \varphi_m$$

Je jasné, že podmienky, za akých je možné získať kľúč (v pôvodnej schéme), závisia hlavne na spôsobe, akým sme rozdelili časti podielov $\varphi_1, \ldots, \varphi_m$ medzi účastníkov.

[8] Všeobecná znamená, že pre akúkoľvek množinu prístupových množín Γ dokážeme zostrojiť prístupovú štruktúru (Γ, Δ) tak, aby $\Delta = 2^{\mathcal{P}} \setminus \Gamma$.

[9] Niekedy sa používa aj Shamirova (n, n)-prahová schéma.

To čo sme doteraz povedali môžeme zhrnúť do presnejšej definície. Nech (Γ, Δ) je úplná monotónna prístupová štruktúra nad množinou účastníkov $\mathcal{P}$. **Kumulatívna schéma** pre túto prístupovú štruktúru je taká funkcia $\alpha : \mathcal{P} \to 2^{\Phi}$, kde Φ je nejaká množina, že pre každú množinu účastníkov $\mathcal{A} \subseteq \mathcal{P}$ platí

$$\bigcup_{P_i \in \mathcal{A}} \alpha(P_i) = \Phi \qquad \text{práve vtedy ak } \mathcal{A} \in \Gamma$$

Povedané inak, kumulatívna schéma je schéma, ktorá určuje spôsob, ako rozdeliť medzi účastníkov prvky z množiny Φ tak, aby vždy prístupová množina účastníkov po zložení svojich podielov poznala všetky prvky množiny Φ a každá iná množina účastníkov nepoznala aspoň jeden z prvkov z množiny Φ.

3.2 Monotónne obvody a množina prístupových množín

V tejto kapitole sa budeme zaoberať zápisom množiny prístupových množín Γ. Využijeme pri tom množinu minimálnych prístupových množín Γ^- ($\Gamma = \mathrm{cl}(\Gamma^-)$). Vysvetlíme si vzťah medzi množinou prístupových množín Γ a monotónnymi obvodmi.

Možné zápisy množiny prístupových množín ukážeme na praktickom príklade schémy s účastníkmi $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$. Množina minimálnych prístupových množín je

$$\Gamma^- = \{\ \{P_1, P_2\},\ \{P_2, P_3\},\ \{P_3, P_4\}\ \}$$

Potom množina všetkých prístupových množín je

$$\Gamma = \mathrm{cl}(\Gamma^-) = \{\ \begin{array}{l} \{P_1, P_2\},\ \{P_1, P_2, P_3\},\ \{P_1, P_2, P_3, P_4\},\ \{P_1, P_2, P_4\}, \\ \{P_2, P_3\},\ \{P_2, P_3, P_4\},\ \{P_3, P_4\}\ \ \} \end{array}$$

Majme booleovský[10] obvod $C_\Gamma : \mathbb{B}^n \to \mathbb{B}$, ktorého vstupy sú $x_1, \ldots, x_n$ (zodpovedajú účastníkom $P_1, \ldots, P_n$) a výstupom je y. Obvod sa skladá len z hradiel „and" a „or". Obvod neobsahuje žiadne hradlo „not". Takýto obvod sa voláme **monotónny**. Príčinou jeho názvu je to, že ak niektorý z jeho vstupov x_i zmení svoj stav z nuly na jednotku, výstup y sa nikdy nezmení z jednotky na nulu.

Tu je istá podobnosť s monotónnou prístupovou štruktúrou schém. Nech vstup x_i zodpovedá tomu, či kombinátor pozná ($x_i = 1$), alebo nepozná ($x_i = 0$) podiel účastníka P_i a nech výstup y zodpovedá tomu, či je možné jednoznačne zrekonštruovať kľúč ($y = 1$), alebo nie ($y = 0$).

[10] Znakom $\mathbb{B}$ označíme množinu pravdivostných hodnôt $\{0, 1\}$.

Monotónnosť obvodu zaručuje, že ak množina účastníkov $\mathcal{A}$ je prístupová, potom aj každá jej nadmnožina je prístupová. Naopak, ak množina účastníkov $\mathcal{B}$ nie je prístupová, potom prístupovou nie je ani žiadna z jej podmnožín.

Booleovský obvod $C_\Gamma : \mathbb{B}^n \to \mathbb{B}$ zodpovedá úplnej prístupovej štruktúre (Γ, Δ) práve vtedy, ak pre každú množinu účastníkov $\mathcal{A}$ platí

$$C_\Gamma(x_1, x_2, \ldots, x_n) = \begin{cases} 0, & \text{ak } \mathcal{A} \notin \Gamma \\ 1, & \text{ak } \mathcal{A} \in \Gamma \end{cases}$$

kde

$$x_i = \begin{cases} 0, & \text{ak } \mathcal{P}_i \notin \mathcal{A} \\ 1, & \text{ak } \mathcal{P}_i \in \mathcal{A} \end{cases}$$

Booleovský obvod $C_{\Gamma^-} : \mathbb{B}^n \to \mathbb{B}$ zodpovedá úplnej prístupovej štruktúre implikovanej množinou minimálnych prístupových množín Γ^- práve vtedy, ak je obvodom zodpovedajúcim prístupovej prístupovej štruktúre $(\mathrm{cl}(\Gamma), 2^{\mathcal{P}} \setminus \mathrm{cl}(\Gamma))$. Takýto obvod je vždy monotónny.

Je jasné, že medzi monotónnym obvodom C_{Γ^-} a jemu zodpovedajúcou monotónnou množinou minimálnych prístupových množín Γ^- existuje jedno-jednoznačný vzťah.

Jednoduché je aj ukázať, ako previesť množinu prístupových množín Γ^- na monotónny obvod, ktorý jej zodpovedá a naopak. Nech Γ^- je množina minimálnych prístupových množín, potom k nej priradíme booleovský výraz v tvare **disjunktívnej normálnej formy (DNF)**

$$C_{\Gamma^-}(P_1, P_2, \ldots, P_n) = \bigvee_{\mathcal{A} \in \Gamma^-} \left(\bigwedge_{P_i \in \mathcal{A}} P_i \right).$$

Napríklad pre

$$\Gamma^- = \{\ \{P_1, P_2\},\ \{P_2, P_3\},\ \{P_3, P_4\}\ \}$$

môžeme množinu prístupových množín Γ napísať pomocou DNF výrazu

$$\Gamma = (P_1 \wedge P_2) \vee (P_2 \wedge P_3) \vee (P_3 \wedge P_4),$$

prípadne[11]

$$\Gamma = P_1P_2 + P_2P_3 + P_3P_4.$$

V monotónnom obvode by sme mohli každý súčin nahradiť hradlom „and" a súčet by realizovalo hradlo „or". Celkový počet hradiel potrebných na zostrojenie obvodu je $|\Gamma^-| + 1$.

[11] V DNF často zamieňame $\wedge$ za násobenie a $\vee$ za sčítanie(+).

3.3 Konštrukcia schémy so všeobecnou prístupovou štruktúrou

Zostrojiť schému so všeobecnou prístupovou štruktúrou je pomerne náročné. Asi najjednoduchšie riešenie tohto problému predstavuje **Benaloh-Leichterova schéma**.

Schéma 3.
Benaloh-Leichterova schéma
Inicializačná fáza

Nech $(\mathcal{K}, +)$ je aditívna grupa a nech konštruujeme schému s monotónnou prístupovou štruktúrou, ktorá zodpovedá obvodu opísanému pomocou disjuktívnej normálnej formy. Nech

$$C_{\Gamma\text{-}}(P_1, \ldots, P_n) = \sum_{i=1}^{\ell} \mathcal{A}_i \ ,$$

kde $\mathcal{A}_i$ je súčinom n_i vstupov. Konštrukcia využíva ℓ Karnin-Green-Hellmanových schém – jednu pre každý súčin $\mathcal{A}_i$. Všetky schémy zdieľajú ten istý kľúč $K \in \mathcal{K}$. Podiely v schémach sú vyberané nezávisle.

Pri konštrukcii Karnin-Green-Hellmanovej schémy zodpovedajúcej súčinu $\mathcal{A}_i$ dôveryhodná osoba náhodne vyberie $n_i - 1$ častí[12] podielov $\varphi_{i,1}, \ldots, \varphi_{i,n_i-1} \in \mathcal{K}$. Posledná časť podielu (zodpovedajúca súčinu $\mathcal{A}_i$) φ_{i,n_i} sa vyberie tak, aby pre súčin $\mathcal{A}_i$ platilo

$$K = \sum_{j=1}^{n_i} \varphi_{i,j} \ .$$

Každý z účastníkov $P_j \in \mathcal{A}_i$ obdrží jednu časť podielu zo schémy zodpovedajúcej tomuto súčinu (jeden z $\varphi_{i,1}, \ldots, \varphi_{i,n_i}$).

Rekonštrukčná fáza

Ak množina účastníkov je prístupová, potom je (vlastnou) nadmnožinou aspoň jednej množiny $\mathcal{A}_i$ a teda dokáže zostaviť rovnicu zodpovedajúcu súčinu $\mathcal{A}_i$. Ak množina účastníkov nie je prístupová, potom nedokáže zostaviť ani jednu z rovníc.

Popísaná schéma je perfektná.

Opíšme rozdelenie podielov pre prípad, že množina prístupových množín zodpovedá obvodu

$$C_{\Gamma\text{-}} = \underbrace{P_1P_2}_{\mathcal{A}_1} + \underbrace{P_2P_3}_{\mathcal{A}_2} + \underbrace{P_3P_4}_{\mathcal{A}_3}$$

[12] Časti podielov sú to preto, lebo každý účastník dostáva len jediný podiel. V tom prípade sú $\varphi_{i,1}, \ldots, \varphi_{i,n_i}$ podielmi vzhľadom na i-tu Karnin-Green-Hellmanovu schému. Ale vzhľadom na Benaloh-Leichterovu schému sú to len časti podielu.

Výsledná schéma vznikne spojením troch schém (zodpovedajúcim $\mathcal{A}_1$,$\mathcal{A}_2$ a $\mathcal{A}_3$) zdieľajúcim rovnaký kľúč K. Počet účastníkov schém je $n_1 = n_2 = n_3 = 2$.

Predpokladajme, že $(\mathcal{K}, +)$ je aditívna grupa. Najprv dôveryhodná osoba vyberie kľúč $K \in \mathcal{K}$, tak aby výber každého prvku bol rovnako pravdepodobný.

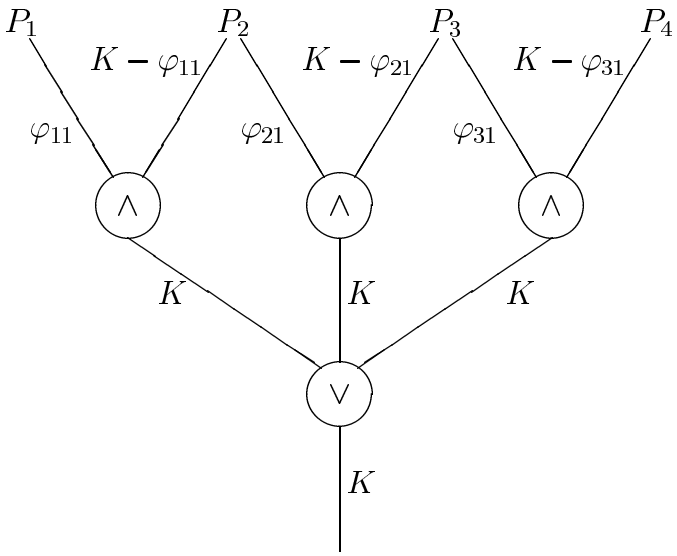
1. Karnin-Green-Hellmanova schéma sa skladá z účastníkov $\mathcal{A}_1 = \{P_1, P_2\}$. Ich časti podielu sú φ_{11}, $\varphi_{12} \in \mathcal{K}$. Časť podielu φ_{11} sa vyberie náhodne. Časť podielu $\varphi_{12} = K - \varphi_{11}$ sa dopočíta.

2. Karnin-Green-Hellmanova schéma sa skladá z účastníkov $\mathcal{A}_2 = \{P_2, P_3\}$. Ich časti podielu sú φ_{21}, $\varphi_{22} \in \mathcal{K}$. Časť podielu φ_{21} sa vyberie náhodne. Časť podielu $\varphi_{22} = K - \varphi_{21}$ sa dopočíta.

3. Karnin-Green-Hellmanova schéma sa skladá z účastníkov $\mathcal{A}_1 = \{P_3, P_4\}$. Ich časti podielu sú φ_{31}, $\varphi_{32} \in \mathcal{K}$. Časť podielu φ_{31} sa vyberie náhodne. Časť podielu $\varphi_{32} = K - \varphi_{31}$ sa dopočíta.

Podiely sa rozdelia medzi účastníkov nasledovne:

- účastník P_1 obdrží podiel $s_1 = (\varphi_{11})$,
- účastník P_2 obdrží podiel $s_2 = (\varphi_{12}, \varphi_{21})$, kde $\varphi_{12} = K - \varphi_{11}$,
- účastník P_3 obdrží podiel $s_3 = (\varphi_{22}, \varphi_{31})$, kde $\varphi_{22} = K - \varphi_{21}$,
- účastník P_4 obdrží podiel $s_4 = (\varphi_{32})$, kde $\varphi_{32} = K - \varphi_{31}$.



Obrázok 1: Rozdelenie častí kľúčov pre C_{Γ}- $= P_1P_2 + P_2P_3 + P_3P_4$.

3.4 Množina neprístupových množín

Ak skúmaná schéma je perfektná, obvykle nepíšeme množinu neprístupových množín, pretože je doplnkom množiny Γ ($\Delta = 2^{\mathcal{P}} \setminus \Gamma$).

Keď prístupová štruktúra je monotónna, potom namiesto množiny všetkých neprístupových množín Δ nám stačí zapísať *množinu maximálnych neprístupových množín* Δ^+. Množinový zápis množiny maximálnych neprístupových množín môže vyzerať napríklad

$$\Delta^+ = \big\{\{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_4\}\big\}$$

Nech $\Delta^+ = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$. Potom kumulatívnou maticou *(cumulative array)* nazveme takú maticu $\mathcal{C}_\Delta = c_{ij}$, kde

$$c_{ij} = \begin{cases} 0, & \text{ak } P_i \in \mathcal{B}_j \\ 1, & \text{ak } P_i \notin \mathcal{B}_j \end{cases}$$

pre $1 \leq i \leq n$ a $1 \leq j \leq m$ (Riadky zodpovedajú účastníkom P_i a stĺpce maximálnym neprístupovým množinám $\mathcal{B}_j$).

Napríklad:
Nech je daná množina maximálnych neprístupový množín[13]

$$\Delta^+ = \big\{ \underbrace{\{P_1, P_3\}}_{\mathcal{B}_1}, \underbrace{\{P_1, P_4\}}_{\mathcal{B}_2}, \underbrace{\{P_2, P_4\}}_{\mathcal{B}_3} \big\}$$

Zápis kumulatívnej matice $\mathcal{C}_\Delta$ je potom:

	$\mathcal{B}_1$	$\mathcal{B}_2$	$\mathcal{B}_3$
P_1	0	0	1
P_2	1	1	0
P_3	0	1	1
P_4	1	0	0

prípadne

$$\mathcal{C}_\Delta = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Aj množinu maximálnych neprístupových množín môžeme ľahko previesť na perfektnú schému.

[13] Ak je schéma perfektná, potom Δ^+, zodpovedá schéme z predchádzajúcej kapitoly $\Gamma = P_1P_2 + P_2P_3 + P_3P_4$.

Schéma 4.

Inicializačná fáza

Nech množina maximálnych neprístupových množín účastníkov pre danú schému je $\Delta^+ = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$. Nech $(\mathcal{S}, +)$ je aditívna grupa a nech časti podielov[14] účastníkov $\varphi_1, \ldots, \varphi_m$ vyberáme z množiny $\mathcal{S}$ a kľúč taktiež z množiny $\mathcal{K} = \mathcal{S}$.

Dôveryhodná osoba náhodne vyberie časti podielov $\varphi_1, \varphi_2, \ldots, \varphi_m$ nezávisle na sebe s rovnomerným rozdelením pravdepodobnosti. Následne vypočíta kľúč[15]

$$K = \varphi_1 + \varphi_2 + \cdots + \varphi_m$$

a rozdá časti podielov účastníkom podľa pravidla, že účastník P_i dostane podiel φ_j ak $P_i \notin \mathcal{B}_j$.

Rekonštrukčná fáza

Kombinátor môže zrekonštruovať kľúč podľa toho istého pravidla, ako ho vypočítala dôveryhodná osoba, čiže dosadí do vzťahu

$$K = \varphi_1 + \varphi_2 + \cdots + \varphi_m.$$

Ešte by sme sa mali presvedčiť, kedy je tejto schéme možné zložiť kľúč – alebo inak, kedy poznáme všetky podiely $\varphi_1, \varphi_2, \ldots, \varphi_m$. Je zrejmé, že ak množina účastníkov nebude prístupová, potom bude (vlastnou) podmnožinou aspoň jednej maximálnej neprístupovej množiny $\mathcal{B}_j$ a teda nebude poznať časť podielu φ_j, nemá žiadnu informáciu o kľúči. Naopak ak by účastníkom chýbala niektorá z častí φ_j, znamenalo by to, že sú (vlastnou) podmnožinou minimálnej neprístupovej množiny $\mathcal{B}_j$ a preto sú množinou neprístupovou.

[14] Každý účastník dostane jednu, alebo viacero častí podielov $\varphi_1, \ldots, \varphi_m$, viacerí účastníci budú zdieľať tú istú časť podielu.

[15] Jedná sa v podstate o Karnin-Green-Hellmanovu schému nad časťami podielov $\varphi_1, \ldots, \varphi_m$. Namiesto nej sme mohli použiť aj inú schému, kde rekonštrukcia kľúča je možná len pri znalosti všetkých podielov. Keď trochu predbehneme, takýmito schémami môže byť aj Shamirova prahová (t, n) schéma $(t = n)$,alebo schéma založená na čínskej zvyškovej vete, alebo nejaká úplne iná schéma. To najdôležitejšie, čo by sme mali z tejto schémy zapamätať, je spôsob, ako sa rozdeľovali časti podielov.

V našom konkrétnom príklade

$$\Delta^+ = \{ \underbrace{\{P_1, P_3\}}_{\mathcal{B}_1}, \underbrace{\{P_1, P_4\}}_{\mathcal{B}_2}, \underbrace{\{P_2, P_4\}}_{\mathcal{B}_3} \}$$

by podiely účastníkov boli nasledovné:

1. účastník P_1 dostane podiel $s_1 = (\varphi_3)$,
2. účastník P_2 dostane podiel $s_2 = (\varphi_1, \varphi_2)$,
3. účastník P_3 dostane podiel $s_3 = (\varphi_2, \varphi_3)$,
4. účastník P_4 dostane podiel $s_4 = (\varphi_1)$.

4 Vybrané schémy na zdieľanie tajomstva

4.1 Schéma založená na čínskej zvyškovej vete

Konštrukciu schémy založenej na čínskej zvyškovej vete uvedieme len ako zaujímavosť. Schéma nie je perfektná, v praxi sa nepoužíva. Je však jednoduchá, patrí k základným schémam pri zdieľaní tajomstva.

Najprv uvedieme čínsku zvyškovú vetu.

Čínska zvyšková veta Nech $m_1, m_2, \ldots, m_t$ sú prirodzené po dvoch nesúdeliteľné čísla. Označme $M = \prod_{i=1}^{t} m_i = m_1 m_2 \ldots m_t$ a $M_i = \frac{M}{m_i}$ (pre všetky $1 \leq i \leq t$). Nech N_i je také prirodzené číslo[16] $0 < N_i < m_i$, že $N_i M_i \equiv 1 \pmod{m_i}$. Potom sústava rovníc

$$K \equiv D_i \pmod{m_i}$$

pre $i = 1, \ldots, t$ má jediné riešenie $K < M$, ktoré môžeme vypočítať

$$K \equiv \sum_{i=1}^{t} D_i N_i M_i \pmod{M}$$

Schéma 5.

Schéma založená na čínskej zvyškovej vete.

Inicializačná fáza

Nech počet všetkých účastníkov schémy je n a nech prístupovou je každá množina s aspoň k účastníkmi. Najprv dôveryhodná osoba vyberie množinu n rôznych, po dvoch nesúdeliteľných čísel $\{m_1, m_2, \ldots, m_n\}$. (Tieto čísla mohli byť vybrané aj dopredu a môžu byť hoci aj verejne známe). Následne dôveryhodná osoba vypočíta hodnoty a, b. Číslo a je súčinom $k-1$ najväčších čísel, b je súčinom k najmenších čísel z množiny $\{m_1, m_2, \ldots, m_n\}$.

Ak $a \geq b$, alebo $b - a$ je príliš malé číslo, potom sme nevhodne zvolili množinu $\{m_1, m_2, \ldots, m_n\}$ a voľbu zopakujeme.

Následne dôveryhodná osoba náhodne vyberie kľúč K z intervalu (a, b) a vypočíta hodnoty $D_1, \ldots, D_n$, podľa predpisu $D_i = K \pmod{M_i}$.

Účastníci $P_1, \ldots, P_n$ obdržia ako podiely dvojice[17] $s_1, \ldots, s_n$ tak, že $s_i = (D_i, m_i)$. Na základe podielu s_i môžme pri rekonštrukcii kľúča zostaviť konguerenciu

$$K \equiv D_i \pmod{m_i}$$

[16] Čísla m_i sú dvoch nesúdeliteľné preto, aby sme ku každému M_i našli N_i

[17] Ak m_i je verejne známe, tak podielom bude samozrejme priamo D_i

Rekonštrukčná fáza

Ak pri rekonštrukcii budeme poznať t podielov, nech sú to bez straty všeobecnosti podiely $s_1, \ldots, s_t$, potom dokážeme zostaviť sústavu kongurencií

$$\begin{aligned} K &\equiv D_1 \pmod{m_1} \\ K &\equiv D_2 \pmod{m_2} \\ &\vdots \\ K &\equiv D_t \pmod{m_t}. \end{aligned}$$

Označme súčin $M = m_1 m_2 \ldots m_t$. Podľa vzťahu $M_i = \frac{M}{m_i}$ vypočítajme hodnoty $M_1, \ldots, M_t$. Hodnotu m podľa čínskej zvyškovej vety vypočítame

$$m \equiv \sum_{i=1}^{t} D_i N_i M_i \pmod{M}.$$

Kde N_i sú (podľa čínskej zvyškovej vety) také prirodzené čísla $0 < N_i < m_i$, že $N_i M_i \equiv 1 \pmod{m_i}$.

Spojením viacerých kongurencií z podielov sme dostali jednu jedinú kongurenciu pre kľúč K. Vieme, že $m \equiv K \pmod{M}$, a teda skutočný kľúč K pri znalosti m môžeme hľadať niekde v postupnosti $m, m+M, m+2M, m+3M \ldots$.

Je jasné, že ak $M \geq b$, potom sme na intervale (a, b) vypočítali kľúč $K = m$. To nastane v prípade, ak pre počet podielov, z ktorých sme zostavili kongurencie, platí $t \geq k$ (b je súčinom k najmenších čísel z množiny $\{m_1, m_2, \ldots, m_n\}$ a M je súčinom $t \geq k$ rôznych čísel z tej istej množiny).

Ak $M < a$, potom nepoznáme kľúč K a budeme ho musieť hľadať v postupnosti $m, m+M, m+2M, m+3M \ldots$ Toto nastane, ak pre počet podielov, z ktorých sme zostavili kongurencie platí $t \leq k-1$ (a je súčinom $k-1$ najväčších čísel z množiny $\{m_1, m_2, \ldots, m_n\}$ a M je súčinom $t \leq k-1$ rôznych čísel z tej istej množiny).

Kým nepoznáme žiaden podiel, kľúčom môže byť ľubovoľná hodnota, z intervalu (a, b). Informáciou, ktorú sme z t podielov dostali je, že kľúč je niekde v postupnosti $m, m+M, m+2M, m+3M \ldots$ a teda sme obmedzili množinu kľúčov. Schéma teda nie je perfektná.

Výhody

- Schéma predstavuje jednoduchú implementáciu neúplnej schémy.
- Je nenáročná na implementáciu.

- Algoritmy dôveryhodnej osoby a kombinátora nie sú časovo, ani pamäťovo náročné.
- Bez obmedzení na počet účastníkov.

Nevýhody

- Schéma spĺňa len málo požiadaviek na bezpečnosť, v praxi sa nepoužíva.
- Veľkosť kľúča sa zväčšuje s počtom účastníkov k potrebných na rekonštrukciu kľúča.
- Popisuje získanie tajomstva iba pre k rovnocenných účastníkov.
- Schéma neumožňuje odhaliť podvádzajúceho účastníka.

4.2 Shamirova prahová schéma

Shamirova prahová (t, n) schéma na zdieľanie kľúča je monotónna schéma pre n účastníkov. Prístupovými množinami sú všetky množiny $\mathcal{A}$ s počtom účastníkov t alebo viac ($|\mathcal{A}| \geq t$). Neprístupovými sú všetky množiny účastníkov $\mathcal{B}$, v ktorých je počet účastníkov menší ako t ($|\mathcal{B}| < \mathrm{t}$). Pretože každá množina účastníkov je alebo prístupová alebo neprístupová, je Shamirova prahová (t, n) schéma je perfektná.

Využijeme **Lagrangeov interpolačný polynóm** a poznatok, že každý polynóm stupňa nanajvýš $t - 1$ nad poľom Z_p je pevne určený pomocou t rôznych bodov v tvare (x_i, y_i) (ak $x_i = x_j \Rightarrow i = j$) pre $1 \leq i \leq t$.

Schéma 6.

Shamirova prahová (t, n) schéma

Inicializačná fáza

Na začiatku dôveryhodná osoba náhodne zvolí kľúč K z množiny $\mathcal{K} = Z_p$ (p > n) a koeficienty $a_1, a_2, \ldots, a_{t-1}$ tiež z množiny Z_p (nech pravdepodobnosť výberu každého z prvkov je rovnaká). Týmto výberom sme určili polynóm

$$f(x) = K + \sum_{i=1}^{t-1} a_i x^i = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}.$$

Dôveryhodná osoba zvolí po dvoch rôzne čísla $x_1, \ldots, x_n \in Z_p \setminus \{0\}$ a zverejní ich. Často používanou voľbou je voľba $x_i = i$. Následne dôveryhodná osoba vypočíta podiely jednotlivých účastníkov[18] $s_i = f(x_i)$ a podiely rozdá účastníkom.

[18] $s_1, \ldots, s_n \in \mathcal{S} = Z_p$

Rekonštrukčná fáza

Uvažujme o množine t účastníkov, ktorí sa pokúšajú o rekonštrukciu kľúča. Predpokladajme, že účastníci, ktorí sa na rekonštrukcii podieľajú, sú $P_{j_1}, P_{j_2}, \ldots, P_{j_t}$. Na základe ich podielov na kľúči a verejných parametrov x_i táto množina účastníkov dokáže zostaviť t bodov[19] (x_i, y_i), ktoré ležia na zvolenom polynóme.

Lagrangeov interpolačný polynóm nám umožňuje spätne na základe znalostí t zostrojiť takýto polynóm. Ak polynóm prechádza bodmi (x_i, y_i), pre $i = 1, \ldots, t$, je definovaný nasledovne.

$$f(x) = \sum_{i=1}^{t} y_i \left(\prod_{1 \leq j \leq t; j \neq i} \frac{x - x_j}{x_i - x_j} \right).$$

Samozrejme nás pri rekonštrukcii kľúča nemusí zaujímať celý polynóm, nám stačí zrekonštruovať kľúč $K = f(0)$.

$$K = f(0) = \sum_{i=1}^{t} y_i \underbrace{\prod_{1 \leq j \leq t; j \neq i} \frac{x_j}{x_j - x_i}}_{b_i}$$

Môžeme si všimnúť, že výraz b_i nie je závislý od y_i, ale len od verejne známych hodnôt $x_1, \ldots, x_t$. Preto môžeme hodnoty b_i dopredu vypočítať. Výpočet kľúča sa potom zjednoduší na

$$K = f(0) = \sum_{i=1}^{t} y_i b_i.$$

Ak sa chceme presvedčiť, či Lagrangeov interpolačný polynóm skutočne prechádza všetkými bodmi (x_i, y_i), stačí dosadiť, či naozaj $y_i = f(x_i)$.

Jedným zo základných predpokladov, na ktorom je bezpečnosť schémy založená, je to, že žiaden z koeficientov $b_1, \ldots, b_t$ nie je nulový. Znamená to totiž, že ak sa o rekonštrukciu pokúsi množina len $t - 1$ účastníkov, potom na základe ich podielov nie je možné získať žiadnu informáciu o kľúči. Nech nám chýba podiel x_k účastníka P_{j_k}.

$$K = f(0) = \sum_{i=1}^{t} y_i b_i = y_k b_k + \underbrace{\sum_{1 \leq i \leq t, i \neq k}^{t} y_i b_i}_{\text{konštanta}}$$

Množina účastníkov vyčísli konštantu aj $b_i \neq 0$. Nepozná však hodnotu y_i. Táto hodnota môže byť akékoľvek číslo zo Z_p, každé s rovnakou pravdepodobnosťou. Ale aj

[19] Presnejšie by sme namiesto x_i a y_i mali značiť x_{j_i} a y_{j_i}. My použijeme toto zjednodušenie, ktorým samozrejme nechceme vyjadriť, že na rekonštrukcii sa musí podieľať práve prvých t účastníkov.

hodnota kľúča môže byť akákoľvek. Keby kľúčom malo byť číslo K' (akékoľvek zo Z_p), potom

$$y_i = (K' - \text{konštanta})b_i^{-1}.$$

Ešte treba dokázať, že $b_i = \prod_{1 \leq j \leq t; j \neq i} \frac{x_j}{x_j - x_i}$ je číslo nenulové. Vieme, že každé x_j je nenulové. Tiež určite vieme, že x_j a x_i sú čísla rôzne a teda aj $(x_j - x_i)^{-1}$ je nenulové. Číslo b_i je súčinom nenulových čísel. Všetky čísla, ktoré násobíme sú z intervalu $\langle 1, p-1 \rangle$ a teda nesúdeliteľné s číslom p a teda ani ich súčin nemôže byť deliteľný p. A teda $b_i \neq 0$.

Dokázali sme, že schéma je perfektná.

Ak poznáme podiely účastníkov $s_1, \ldots, s_n$, potom je možné zostaviť sústavu rovníc, ktorá vyjadrí vzťah medzi koeficientami polynómu $(K, a_1, \ldots, a_{t-1})$ a známymi podielmi $s_1, \ldots, s_t$.

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

Čo je možné v maticovom tvare reprezentovať

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

Všimnime si, že matica systému A nezávisí od zvoleného polynómu, ani od podielov na kľúči, len od verejne známych čísel $x_1, \ldots, x_t$. Matica v tomto tvare sa nazýva **Vandermondova matica**. Pre jej determinant platí

$$\det A = \prod_{1 \leq i < j \leq t} (x_j - x_i) \bmod p.$$

Pretože všetky x_j a x_i sú navzájom rôzne, determinant tejto matice bude nenulový. Systém rovníc má teda v Z_p jediné riešenie.

Shamirova prahová (t, n)-schéma patrí k najjednoduchším. Výborne poslúži, ak postavenie jednotlivých účastníkov v schéme je rovnocenné. Na získanie kľúča je potrebných aspoň t z n podielov.

Prvočíslo p, hodnotu prahu t, ako aj počet účastníkov n volí dôveryhodná osoba podľa bezpečnostných a funkčných požiadaviek kladených na schému.

Shamirova prahová schéma sa vyznačuje ešte jednou zaujímavou vlastnosťou, ktorú dosiaľ nemala ani jedna zo schém. Dôveryhodná osoba (prípadne ktokoľvek ďalší, kto zrekonštruuje polynóm) môže ľahko zvýšiť počet účastníkov schémy n, bez toho, aby musel znovu rozdávať podiely účastníkom.

Výhody

- Schéma je jednoduchá na pochopenie, aj na implementáciu.
- Schéma je základom pre viacero ďalších schém.
- Algoritmy dôveryhodnej osoby aj kombinátora nie sú časovo ani pamäťovo náročné.
- Výborne sa hodí v prípade, ak postavenie osôb v schéme je rovnocenné. Vtedy rozhoduje počet účastníkov, ktorí chcú zložiť kľúč.
- Nekladie obmedzenia na počet účastníkov n (okrem $n < p$).
- Nekladie obmedzenia na prahovú hodnotu počtu podielov t potrebných na rekonštrukciu kľúča.
- Voliteľná dĺžka kľúča (počet možných kľúčov len s drobným obmedzením, že p musí byť prvočíslo, $p > n$).
- Krátke podiely jednotlivých účastníkov.
- Schéma je perfektná.

Nevýhody

- Popisuje získanie tajomstva iba pre t rovnocenných účastníkov.
- Schéma na zdieľanie tajomstva sa nedá priamo použiť na podpis pomocou RSA.
- Schéma neumožňuje odhaliť podvádzajúceho účastníka

4.3 Kumulatívna schéma odhaľujúca podvádzajúceho účastníka

Skoro všetky doteraz uvádzané schémy boli perfektné, ale väčšina z nich neumožňovala príliš flexibilne zvoliť prístupovú štruktúru. Pri väčšine schém sme museli najprv spoznať požadovanú prístupovú štruktúru, až potom sme zistili, či táto schéma ju dokáže realizovať, alebo nie.

Kumulatívne boli len schémy 3 a 4. Tieto schémy však neumožnili kombinátorovi odhaliť podvádzajúceho účastníka schémy. Schéma, ktorú si popíšeme v tejto kapitole, ukáže, ako sa dá tento nedostatok riešiť. Jej nevýhodou je zväčšenie dĺžky podielov účastníkov pri nezmenenej dĺžke kľúča.

Schéma 7.

Inicializačná fáza

Nech množina účastníkov je $\mathcal{P} = \{P_1, \ldots, P_n\}$. Nech schéma je perfektná a jej množina maximálnych neprístupových množín je $\Delta^+ = \{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$. Označme

$$\alpha = 1 + \max\{|\mathcal{B}| \ ; \ \mathcal{B} \in \Delta^+\}.$$

Je jasné, že $\alpha \leq n$.

Nech kľúč je $K \in \mathcal{K} = Z_p$ $(p > \max(\alpha, m))$. Potom dôveryhodná osoba $\mathcal{D}$ pracuje podľa nasledujúceho algoritmu:

1. $\mathcal{D}$ náhodne vyberie čísla $a_{ij} \in Z_p$ (pre $i = 1, \ldots, m$ a $j = 1, \ldots, \alpha$) tak, že kľúč $K = a_{11}$. Dôveryhodná osoba na základe vybraných koeficientov získala polynóm dvoch premenných $F(x, y)$.

$$F(x,y) = \sum_{i=1}^{m} \sum_{j=1}^{\alpha} a_{ij} x^{i-1} y^{j-1}$$

$$\begin{aligned} F(x,y) \ = \ & a_{11} && +a_{12} && y + \ldots + a_{1,\alpha} && y^{\alpha-1} + \\ & +a_{21}\ x && +a_{22}\ x && y + \ldots + a_{2,\alpha}\ x && y^{\alpha-1} + \\ & && \ldots && && \\ & +a_{m,1} x^{m-1} && +a_{m,2} x^{m-1} y && + \ldots + a_{m,\alpha} x^{m-1} y^{\alpha-1} && \end{aligned}$$

2. $\mathcal{D}$ vyberie po dvoch rôzne čísla $x_1, \ldots, x_m \in Z_p \setminus \{0\}$ a zverejní ich[20].

3. $\mathcal{D}$ náhodne vyberie čísla $y_1, \ldots, y_n \in Z_p \setminus \{0\}$. Čísla nemusia byť nutne rôzne, ale musia ostať utajené.

[20] Čísla $x_1, \ldots, x_m$ môžu byť dopredu známe, napríklad $x_1 = 1, x_2 = 2$, atď.

4. $\mathcal{D}$ odovzdá účastníkovi P_j nasledujúce podiely[21]:

   (a) číslo y_j a overovací polynóm[22] (stupňa $m-1$) $c_j(x) = F(x, y_j)$

   (b) rekonštrukčné polynómy[23] (stupňa $\alpha - 1$) účastníka P_j, ktoré sú

$$f_{jt}(y) = F(x_t, y) \text{ ; pre všetky } t \text{ také, že } P_j \notin \mathcal{B}_t$$

Overovacia fáza

Predpokladajme, že množina účastníkov $\mathcal{A} \in \Gamma$ sa pokúša o rekonštrukciu kľúča K a nech účastník $P_i \in \mathcal{A}$ prevzal úlohu kombinátora.

Nech každý účastník $P_j \in \mathcal{A}$ odovzdá kombinátorovi svoje rekonštrukčné polynómy

$$f_{jt}(y) = F(x_t, y) \text{ ; pre všetky } t \text{ také, že } P_j \notin \mathcal{B}_t.$$

Kombinátor P_i pomocou privátneho overovacieho polynómu $c_i(x)$ overí platnosť $c_i(x_t) = f_{jt}(y_i)$ (pretože $c_i(x_t) = F(x_t, y_i) = f_{jt}(y_i)$), pre každý prijatý polynóm. Ak niektorý z polynómov nesplní rovnicu, potom je sfalšovaný a účastník P_j je usvedčený z podvodu.

Niektorý polynóm mohol kombinátor obdržať viackrát od rôznych účastníkov. Vtedy môže overiť, či účastníci P_{j_1} a P_{j_2} prispeli tým istým polynómom zodpovedajúcemu maximálnej neprístupovej množine účastníkov $\mathcal{B}_t$. Malo by platiť $f_{j_1 t}(y) = f_{j_2 t}(y)$.

Rekonštrukčná fáza

Kombinátor verí, že všetky obdržané polynómy sú pravé. Teraz vypočíta postupnosť čísel $\varphi_1, \ldots, \varphi_m$, takých, že $\varphi_t = f_{jt}(0) = F(x_t, 0)$.

Nech množina účastníkov[24] $\mathcal{A}$ je prístupová. Znamená to, že $\mathcal{A} \supset \mathcal{B}_1, \ldots, \mathcal{A} \supset B_m$. Uvažujme nad ľubovoľnou maximálnou neprístupovou množinou $\mathcal{B}_t$. Pre každú množinu $\mathcal{B}_t$ existuje aspoň jeden účastník P_j taký, že $P_j \in \mathcal{A} \setminus \mathcal{B}_t$. Účastník P_j pozná rekonštrukčný polynóm $f_{jt}(y)$ a teda po dosadení, do jeho rekonštrukčného podielu kombinátor môže vypočítať $\varphi_j = f_{jt}(0)$. Prístupová množina účastníkov pozná všetky hodnoty $\varphi_1, \ldots, \varphi_m$.

Nech množina účastníkov $\mathcal{A}$, ktorí sa pokúšajú o rekonštrukciu kľúča je neprístupová. Potom existuje taká maximálna neprístupová množina $\mathcal{B}_t \supseteq A$, ktorá je (vlastnou)

[21] Oba polynómy sú jednej premennej.

[22] Overovací polynóm poslúži kombinátorovi na overenie, či sa niektorí z účastníkov nepokúsili o podvod. Tento polynóm by sa nemal inak využiť pri rekonštrukcii. Pretože kombinátorom môže byť každý z účastníkov, všetci dostanú overovací polynóm.

[23] Za každú maximálnu neprístupovú množinu $\mathcal{B}_t$, v ktorej sa účastník nenachádza, dostane jeden rekonštrukčný polynóm $f_{jt}(y)$.

[24] Rozdelenie častí podielov $\varphi_1, \ldots, \varphi_m$ medzi účastníkov je podobné ako pri schéme 4. Zmenilo sa to, že časti podielov sú polynómy a nie čísla. Ďalšia odlišnosť je v tom, že rekonštrukcia kľúča z týchto častí je založená na Shamirovej prahovej schéme.

nadmnožinou $\mathcal{A}$. Potom ale neexistuje účastník $P_j \in \mathcal{A}$, ktorý by mal poznal polynóm $f_{jt}(y) = F(x_t, y)$ zodpovedajúci neprístupovej množine $\mathcal{B}_t$. Vypočítať hodnotu $\varphi_t = f_{jt}(0)$ sa teda účastníkom nepodarí.

Výpočet kľúča K z hodnôt $\varphi_1, \ldots, \varphi_m$ sa uskutoční pomocou Shamirovej prahovej schémy. Polynóm stupňa $m-1$, ku ktorému sa kombinátor pokúsi dopracovať, je $F(x, 0)$. Kombinátor pozná m dvojíc (x_i, φ_i), ktoré jednoznačne určujú tento polynóm.

Zamyslime sa nad možnosťou, že neprístupová množina účastníkov sa pokúsi o rekonštrukciu kľúča na základe overovacích polynómov $c_j(x)$. Tieto polynómy sa neodovzdávajú kombinátorovi a pri rekonštrukcii by sa nemali použiť. My však predpokladáme, že množina účastníkov $\mathcal{A}$ je skorumpovaná. Skúsi teda využiť akúkoľvek slabinu schémy.

V zadaní sme určili koeficient $\alpha = 1 + \max\{|\mathcal{B}|; \mathcal{B} \in \Delta^+\}$. Najpočetnejšia neprístupová množina sa skladá z $\alpha - 1$ účastníkov. Nech jej účastníci sú $P_{i_1}, \ldots, P_{i_{\alpha-1}}$. Množina účastníkov pozná toľko rôznych overovacích polynómov $c_{i_j}(x)$, koľko rôznych čísel je medzi $y_{i_1}, \ldots, y_{i_{\alpha-1}}$. Predpokladajme, že nastane nastane pre útočníkov najvýhodnejšia možnosť. To je vtedy, ak tieto čísla sú po dvoch rôzne.

Útočníci môžu do všetkých overovacích polynómov dosadiť za $x = 0$. Dostanú tak $\alpha - 1$ dvojíc $(y_{i_j}, c_{i_j}(0))$. My vieme, že $c_{i_j}(x) = F(x, y_{i_j})$ a teda útočníci poznajú rôznych $\alpha - 1$ bodov, ktoré ležia na polynóme $F(0, y)$.

Na ich základe znalosti $\alpha - 1$ bodov by bolo možné jednoznačne zrekonštruovať polynóm stupňa $\alpha - 2$. Polynóm $F(0, y)$ je však stupňa $\alpha - 1$.

Popísaná schéma je perfektná.

Tvrdili sme, že schéma umožňuje odhaliť podvádzajúceho účastníka (prípadne viacerých). Skúsme schému analyzovať z pohľadu podvádzajúceho účastníka.

Cieľom podvádzajúceho účastníka P_j je podvrhnúť namiesto pravého rekonštrukčného polynómu (prípadne viacerých) falošný $f'_{jt}(y) \neq f_{jt}(y)$. Musí to urobiť tak, aby šanca na odhalenie bola čo najmenšia.

Kombinátor P_i overuje rovnosť $c_i(x_t) = f_{jt}(y_i)$. Podvádzajúci účastník P_j nepozná kombinátorov overovací polynóm $c_i(x)$ a ani hodnotu y_i. Jeho jedinou šancou ako sa vyhnúť odhaleniu, je poskytnúť kombinátorovi taký sfalšovaný polynóm $f'_{jt}(y)$, ktorý pre čo najväčšie množstvo hodnôt $y \in Z_p \setminus \{0\}$ zachová požadovanú rovnosť. Ak bude mať podvodník šťastie, bude platiť $f'_{jt}(y_i) = f_{jt}(y_i)$. Vtedy kombinátor podvod neodhalí.

Zaujímalo by nás teda, v koľkých (po dvoch) rôznych hodnotách $y'_1, \ldots, y'_r$, možno zachovať rovnosť $f'_{jt}(y'_i) = f_{jt}(y'_i)$ pre daný polynóm $f_{jt}(y)$, keď oba polynómy sú

stupňa $\alpha - 1$. Oba polynómy sa nesmú rovnať – inak by účastník vlastne nepodvádzal, ale prispel k rekonštrukcii kľúča.

Vieme, že polynóm $f_{jt}(y)$, stupňa $\alpha-1$, je presne určený pomocou ľubovoľných α (po dvoch) rôznych bodov. Keby sa teda podvádzajúci účastník pokúsil napodobniť polynóm $f_{jt}(y)$ v α (alebo viac) hodnotách $y'_1, \ldots, y'_r$, dostal by jedinú možnosť $f'_{jt}(y) = f_{jt}(y)$.

Preto je počet bodov, ktoré má podvádzajúci účastník šancu napodobiť, $r \leq \alpha-1$. Pravdepodobnosť neodhalenia podvádzajúceho účastníka je teda[25] $\frac{\alpha-1}{p-1}$.

Príklad

Nech množina maximálnych prístupových množín je

$$\Gamma^- = \big\{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\big\}.$$

Množina maximálnych neprístupových množín je potom

$$\Delta^+ = \big\{\underbrace{\{P_1, P_3\}}_{\mathcal{B}_1}, \underbrace{\{P_1, P_4\}}_{\mathcal{B}_2}, \underbrace{\{P_2, P_4\}}_{\mathcal{B}_3}\big\}.$$

V našom príklade $\alpha = 3, m = 3$. Zvoľme kľúč $K = 5 \in Z_7$.

1. Nech dôveryhodná osoba $\mathcal{D}$ zvolí polynóm $F(x, y)$.

$$F(x, y) = 5 + x^2 + 2y + y^2 + 4xy + 5xy^2 + 2x^2y^2$$

2. Následne zvolí čísla $x_1, \ldots, x_m \in Z_7 \setminus \{0\}$, napríklad $x_1 = 1, x_2 = 2, x_3 = 3$ a zverejní ich.

3. $\mathcal{D}$ náhodne zvolí $y_1, \ldots, y_n \in Z_7 \setminus \{0\}$, ktoré ostanú utajené. Zvoľme napríklad $y_1 = 2, y_2 = 1, y_3 = 6$ a $y_4 = 4$.

[25] V [3] uvádza pravdepodobnosť $1/p$. Toto číslo je správne, ak sa o podvod nepokúsil účastník schémy, ale niekto, kto nepozná podiel, ktorý falšuje.

4. $\mathcal{D}$ odovzdá podiely účastníkom

P_1 : (a) $y_1 = 2$,overovací polynóm $c_1(x) = F(x,2) = 6 + 2x^2$
(b) $P_1 \notin \mathcal{B}_3$,rekonštrukčný polynóm $F(3,y) = f_{13}(y) = 6y^2$

P_2 : (a) $y_2 = 1$,overovací polynóm $c_2(x) = F(x,1) = 1 + 2x + 3x^2$
(b) $P_2 \notin \mathcal{B}_1$,rekonštrukčný polynóm $F(1,y) = f_{21}(y) = 6 + 6y + y^2$
$P_2 \notin \mathcal{B}_2$,rekonštrukčný polynóm $F(2,y) = f_{22}(y) = 2 + 3y + 5y^2$

P_3 : (a) $y_3 = 6$,overovací polynóm $c_3(x) = F(x,6) = 4 + x + 3x^2$
(b) $P_3 \notin \mathcal{B}_2$,rekonštrukčný polynóm $F(2,y) = f_{32}(y) = 2 + 3y + 5y^2$
$P_3 \notin \mathcal{B}_3$,rekonštrukčný polynóm $F(3,y) = f_{33}(y) = 6y^2$

P_4 (a) $y_4 = 4$,overovací polynóm $c_4(x) = F(x,4) = 5x^2$
(b) $P_4 \notin \mathcal{B}_1$,rekonštrukčný polynóm $F(1,y) = f_{41}(y) = 6 + 6y + y^2$

Ak sa o získanie kľúča pokúsi ľubovoľná prístupová množina, jej účastníci poznajú rekonštrukčné polynómy $F(x_1,y), F(x_2,y), F(x_3,y)$ a teda ľahko vypočítajú čísla φ_1, φ_2 a φ_3. Nech sa o rekonštrukciu tajomstva pokúšajú spolu napríklad účastníci P_2 a P_3.

$$\varphi_1 = F(x_1,0) = f_{21}(0) = 6$$

$$\varphi_2 = F(x_2,0) = f_{22}(0) = f_{32}(0) = 2$$

$$\varphi_3 = F(x_3,0) = f_{33}(0) = 0$$

Výpočet kľúča je potom už len výpočtom polynómu $F(x,0)$ stupňa $m-1 = 2$, prechádzajúceho bodmi $(x_1,\varphi_1), (x_2,\varphi_2), (x_3,\varphi_3)$. Vráťme sa teda k Shamirovej prahovej schéme.

$$\begin{aligned} K &= \varphi_1 \tfrac{x_2x_3}{(x_2-x_1)(x_3-x_1)} + \varphi_2 \tfrac{x_1x_3}{(x_1-x_2)(x_3-x_2)} + \varphi_3 \tfrac{x_1x_2}{(x_1-x_3)(x_2-x_3)} \\ &= \varphi_1 \tfrac{6}{2} + \varphi_2 \tfrac{3}{6} + \varphi_3 \tfrac{2}{2} \\ &= 3\,\varphi_1 + 4\,\varphi_2 + 1\,\varphi_3 \\ &= 5 \end{aligned}$$

Keby sme chceli odvodiť celý Lagrangeov interpolačný polynóm prechádzajúci prechádzajúci bodmi $(x_1,\varphi_1), (x_2,\varphi_2)$ a (x_3,φ_3), vyšlo by nám $F(x,0) = 5 + x^2$.

Ak by sa o rekonštrukciu pokúsila neprístupová množina účastníkov, nezíska aspoň jednu z hodnôt $\varphi_1, \varphi_2, \varphi_3$ a teda nezloží kľúč (Shamirova prahová schéma neumožní zložiť polynóm $m-1 = 2$ stupňa, kým nebudeme poznať všetkým m hodnôt φ_i). A teda vidíme, že daná schéma je perfektná.

Popíšme si aj možné správanie sa podvádzajúceho účastníka. Predpokladajme, že o zloženie kľúča sa pokúsia účastníci P_2 a P_3. Kombinátorom bude P_2 a účastník P_3 sa bude snažiť podvádzať. Kombinátor pozná rekonštrukčné polynómy $F(1, y) = 6 + 6y + y^2$ a $F(2, y) = 2 + 3y + 5y^2$.

Účastník P_3 pozná $F(2, y) = 2 + 3y + 5y^2$ a $F(3, y) = 6y^2$. Polynóm $F(2, y)$ poznajú obaja účastníci a teda je riskantné sfalšovať ho. P_3 sa ale môže pokúsiť sfalšovať polynóm $f_{33}(y) = F(3, y)$ polynómom $f'_{33}(y)$.

Ak by platilo $f_{33}(0) = f'_{33}(0)$, aj keby sa podvod nepodarilo odhaliť, podvodník by si nepomohol. Kľúč by sa aj podarilo takisto zrekonštruovať. Jeho snahou je zmeniť hodnotu $f_{33}(0)$ a nenechať sa odhaliť, čiže zachovať $f_{33}(y_2)$. Hodnotu $y_2 \in Z_p \setminus \{0\}$ nepozná a teda sa môže pokúsiť zachovať čím viac funkčných hodnôt. Vyberie $\alpha - 1$ hodnôt, medzi ktorými sa jeho podvod nepodarí odhaliť a všade inde sa podvod odhalí.

$f_{33}(y) = 6y^2$ a P_3 chce svoj podvod ukryť, ak y_2 je 1, alebo 2. Preto zvolí falošný polynóm tak, aby spĺňal rovnice

$$f'_{33}(1) = f_{33}(1) = 6$$

$$f'_{33}(2) = f_{33}(2) = 3$$

Ak by útočník pridal ešte jednu takúto rovnicu pre ďalšiu potenciálnu hodnotu y_2, vyšlo by mu $f'_{33}(y) = f_{33}(y)$. A teda podvodník by vlastne nepodvádzal. Poslednou rovnicou, ktorú si účastník P_3 zvolí bude hodnota $f'_{33}(0) \neq f_{33}(0) = 0$. Dajme tomu

$$f'_{33}(0) = 1$$

Zo sústavy rovníc potom dostane polynóm $f'_{33}(y) = 1 + 2y + 3y^2$.

y	0	1	2	3	4	5	6
$f_{33}(y) = 6y^2$	0	6	3	5	5	3	6
$f'_{33}(y) = 1 + 2y + 3y^2$	1	6^*	3^*	6	1	2	2

Vidíme $f_{33}(y)$ a $f'_{33}(y)$ sa zhodujú skutočne len v $\alpha - 1 = 2$ hodnotách (označených *). Podvod účastníka P_3 sa nepodarí odhaliť, v prípade ak dôveryhodná osoba zvolila y_2 rovné 1, alebo 2. Pravdepodobnosť, že P_3 sa podarí podvod utajiť je teda $\frac{\alpha-1}{p-1} = \frac{2}{6} = \frac{1}{3}$.

5 Zdieľanie tajomstva v multiúrovňových schémach

5.1 Označenie v multiúrovňových schémach

V tejto kapitole si popíšeme schému na zdieľanie tajomstva uvádzanú v literatúre [5] a [4]. Popísaná schéma tvorí jadro tejto práce. Našou úlohou bude doplniť schému o popis algoritmus kombinátora, opraviť a doplniť predpoklady, za akých bude schéma spoľahlivo pracovať a nakoniec urobiť funkčnú implementáciu spomínanej schémy na overenie našich predpokladov.

Základom multiúrovňových schém na zdieľanie tajomstva je rozdelenie účastníkov medzi jednotlivé úrovne tak, aby každý z účastníkov patril do práve jednej úrovne. Jednotlivé úrovne budeme označovať $\mathcal{P}_1, \ldots, \mathcal{P}_\ell \subseteq \mathcal{P}$. Predpokladáme, že každý z účastníkov patrí práve do jednej úrovne ($\mathcal{P}_i \cap \mathcal{P}_j \neq \emptyset \Leftrightarrow i = j$ a $\mathcal{P}_1 \cup \mathcal{P}_2 \cup \ldots \cup \mathcal{P}_\ell = \mathcal{P}$).

Úroveň $\mathcal{P}_1$ bude najvyššou úrovňou hierarchie účastníkov (najmenší počet účastníkov dokáže zložiť kľúč), úroveň $\mathcal{P}_2$ bude nižšia a tak ďalej, až po najnižšiu úroveň $\mathcal{P}_\ell$. Označme počet účastníkov na i-tej úrovni $n_i = |\mathcal{P}_i|$.

Počet všetkých účastníkov schémy je $n = |\mathcal{P}| = \sum_{i=1}^{\ell} |P_i| = \sum_{i=1}^{\ell} n_i$. Označme počet účastníkov i-tej, alebo vyššej úrovne $N_i = \sum_{j=1}^{i} n_j$, pre $1 \leq i \leq \ell$. Je jasné, že $N_1 = n_1$ a $N_\ell = n$.

Aby sme si úlohu zjednodušili predpokladajme (bez straty všeobecnosti), že účastníci sú číslovaní tak, že $\mathcal{P}_1 = \{P_1, \ldots, P_{N_1}\}$, $\mathcal{P}_2 = \{P_{1+N_1}, \ldots, P_{N_2}\}$ atď. Úroveň $\mathcal{P}_i$ ($i > 1$) sa skladá z účastníkov $\mathcal{P}_i = \{P_{1+N_{i-1}}, \ldots, P_{N_i}\}$.

Aby sme určili, či množina účastníkov $\mathcal{A} \subseteq \mathcal{P}$ je prístupová, zavádzame pojem prah i-tej úrovne. Nech **prah *i*-tej úrovne** je t_i účastníkov. Potom platí:

- ak $|\mathcal{A}| \geq t_i$, potom množina účastníkov $\mathcal{A}$ je prístupová,
- ak $|\mathcal{A}| < t_i$, potom množina účastníkov $\mathcal{A}$ je neprístupová.

Samozrejme medzi prahmi jednotlivých úrovní predpokladáme, že platí $t_1 < t_2 < \ldots < t_\ell$. Pre každú úroveň predpokladáme $1 \leq t_i \leq N_i$ a $t_{i+1} < t_i + n_i$.

Prístupovou množinou na i-tej úrovni je každá taká množina účastníkov $\mathcal{A} \subseteq \mathcal{P}$, ktorá obsahuje t_i (alebo viac) účastníkov úrovne P_i alebo vyššej.

$$\Gamma_i = \{\mathcal{A} \subseteq \mathcal{P} \,; \sum_{j=1}^{i} |\mathcal{A} \cap \mathcal{P}_j| \geq t_i\}$$

Množina všetkých prístupových množín je potom $\Gamma = \bigcup_{i=1}^{\ell} \Gamma_i$.

Uveďme príklad z banky, kedy nejakú finančnú transakciu je možné vykonať, ak jej korektnosť overia traja výkonní námestníci, alebo obaja viceprezidenti, pričom hociktorého námestníka môže nahradiť jeden z viceprezidentov.

Najvyššiu úroveň tvoria dvaja viceprezidenti $\mathcal{P}_1 = \{P_1, P_2\}$, $n_1 = 2$. Nižšia úroveň obsahuje námestníkov $\mathcal{P}_2 = \{P_3, P_4, P_5\}$, $n_2 = 3$. Na rekonštrukciu kľúča je potrebné poznať podiely dvoch účastníkov z prvej úrovne, alebo podiely troch účastníkov z prvej a druhej úrovne dohromady. Prahy potom sú $t_1 = 2$, $t_2 = 3$ a počet účastníkov schémy je $n = 5$.

Pri práci s multiúrovňovými schémami je výhodné dokázať zapísať množinu účastníkov úrovne nanajvýš P_i. Označme ju

$$\mathcal{P}^i = \bigcup_{j=1}^{i} \mathcal{P}_j.$$

5.2 Rozšírenie schémy

Nech schéma Γ_1, ktorej množina účastníkov je $\mathcal{P}^1$, je úplná. Potom o úplnej schéme Γ_2 s množinou účastníkov $\mathcal{P}^2 \supseteq \mathcal{P}^1$ budeme hovoriť hovoriť, že je **rozšírenie schémy** Γ_1, ak platia nasledujúce vety:

1. Množina účastníkov schémy 1 je podmnožinou množiny účastníkov schémy 2 ($\mathcal{P}^1 \subseteq \mathcal{P}^2$).
2. V oboch schémach účastníci zdieľajú ten istý kľúč K.
3. Podiely účastníkov z množiny $\mathcal{P}^1$ ostanú uchované (prípadne sa k nim informácia pridá) aj v schéme $\mathcal{P}^2$.
4. Každá prístupová množina účastníkov $\mathcal{A} \in \Gamma_1$ prístupovou aj v schéme Γ_2 ($\Gamma_1 \subseteq \Gamma_2$).

Ak schéma Γ_2 je rozšírením schémy Γ_1 a schéma Γ_3 je rozšírením schémy 2, potom aj schéma Γ_3 je rozšírením schémy Γ_1. Rozšírenie je tranzitívna relácia.

My sa budeme zaoberať konštrukciou rozšírenia pre prahové schémy. Spôsob ich rozšírenia sme popísali v predchádzajúcej kapitole. Pripomeňme si napríklad príklad z banky. Pre účastníkov množiny $\mathcal{P}^1$ sa schéma javila ako (Shamirova) $(2, 2)$-prahová. Pre účastníkov množiny $\mathcal{P}^2$ sa zas schéma javila ako $(3, 5)$-prahová. Existuje aj pomerne jednoduchý spôsob, ako možno rozšíriť prahovú schému.

Schéma 8. Najprv zostrojíme Shamirovu (t_1, N_1)-prahovú schému Γ_1 s účastníkmi $\mathcal{P}^1$. Následne schému Γ_2, ktorá bude zdieľať ten istý kľúč a bude Shamirova (t_2, N_2)-prahová s množinou účastníkov $\mathcal{P}^2$. Následne by sme zostrojili (t_3, N_3)-prahovú schému Γ_3. Takto by sme pokračovali až po (t_ℓ, N_ℓ)-prahovú schému Γ_ℓ. Samozrejme účastník by dostal podiely zo všetkých schém, v ktorých by vystupoval. Účastník i-tej úrovne by tak dostal $\ell - i + 1$ podielov zo schém Γ_i,...,Γ_ℓ.

Uvedená schéma je perfektná. Jej nevýhodou je, že podiel účastníka z i-tej úrovne sa skladá z viacerých častí a teda je dosť dlhý.

5.3 Prístupová štruktúra multiúrovňovej schémy

Našim cieľom bude zostrojiť schému, ktorej prístupová štruktúra by bola rovnaká ako pri predchádzajúcej schéme. Dĺžka podielov v novej schéme by však mala byť výrazne kratšia – dĺžka podielu už nebude závislá na tom, koľkokrát sme schému rozširovali. Ukážeme si, že účastníkom schémy A_1 nie je potrebné znovu generovať podiely na kľúči do schémy A_2.

Dosiahneme to tak, že zväčšíme stupeň polynómu schémy A_2 tak, aby podiely rozdané v schéme A_1 mohli ostať zachované. Ukážeme si ako potom schému rozširovať ďalej.

Naša schéma mení prístupové štruktúry jednotlivých úrovní $\Gamma_1, \ldots, \Gamma_\ell$. Urobí to však tak, aby prístupová štruktúra $\Gamma = \bigcup_{i=1}^{\ell} \Gamma_i$ ostala zachovaná[26].

Prístupová štruktúra prvej úrovne sa nezmenila. Majme množinu účastníkov $\mathcal{A} \subseteq \mathcal{P}$, ktorá sa skladá z $u_1 = |\mathcal{A} \cap \mathcal{P}_1|$ účastníkov prvej úrovne, $u_2 = |\mathcal{A} \cap \mathcal{P}_2|$ účastníkov druhej úrovne, atď[27].

- $\mathcal{A} \in \Gamma_1 \Leftrightarrow t_1 \leq u_1$
- $\mathcal{A} \in \Gamma_2 \Leftrightarrow t_2 \leq u_2 + \min(t_1, u_1)$
- $\mathcal{A} \in \Gamma_3 \Leftrightarrow t_3 \leq u_3 + \min(t_2, u_2 + \min(t_1, u_1))$
- $\mathcal{A} \in \Gamma_4 \Leftrightarrow t_4 \leq u_4 + \min(t_3, u_3 + \min(t_2, \min(t_1, u_1))$

[26]Predchádzajúca definícia prístupových štruktúr i-tej úrovne je jednoduchá, jasná a prehľadná. Nová definícia je omnoho komplikovanejšia, ale nová schéma má inú prístupovú štruktúru niektorých úrovní. Celková prístupová štruktúra sa však nezmenila!

[27]Znamená, že pri skladaní sme ochotní započítať najviac t_1 účastníkov z množiny P^1, najviac t_2 účastníkov z P^2, atď.

5.4 Konštrukcia schémy

Najprv sa zamyslime nad konštrukciou jednoduchého prípadu multiúrovňovej schémy – nad dvojúrovňovou schémou. Uveďme algoritmus, podľa ktorého by mala postupovať dôveryhodná osoba pri konštrukcii schémy.

Schéma 9. Nech $\mathcal{S} = \mathcal{K}$ (napríklad $\mathbb{R}$, Z_p, alebo $GF(q)$) je pole z ktorého budeme vyberať kľúč K.

1. Dôveryhodná osoba $\mathcal{D}$ v poli náhodne zvolí koeficienty $a_{1,1}, \ldots, a_{1,T_1} \in \mathcal{S}$ polynómu
$$f_1(x) = K + a_{1,1}x + a_{1,2}x^2 + \ldots + a_{1,T_1}x^{T_1}.$$
Polynóm $f_1(x)$ stupňa $T_1 = t_1 - 1$ je zvolený tak, aby $f(0) = K$.

2. $\mathcal{D}$ vyberie[28] po dvoch rôzne hodnoty $x_1, \ldots, x_{N_1} \in \mathcal{S} \setminus \{0\}$ a zverejní ich.

3. $\mathcal{D}$ vypočíta podiely účastníkov, čo budú hodnoty polynómu $f_1(x)$ v prislúchajúcich bodoch.
$$\begin{array}{ccccc} s_1 & = & f_1(x_1) & = & K + a_{1,1}x_1 + a_{1,2}x_1^2 + \ldots + a_{1,T_1}x_1^{T_1} \\ s_2 & = & f_1(x_2) & = & K + a_{1,1}x_2 + a_{1,2}x_2^2 + \ldots + a_{1,T_1}x_2^{T_1} \\ \vdots & & \vdots & & \vdots \\ s_{N_1} & = & f_1(x_{N_1}) & = & K + a_{1,1}x_{N_1} + a_{1,2}x_{N_1}^2 + \ldots + a_{1,T_1}x_{N_1}^{T_1} \end{array}$$
Dôveryhodná osoba odovzdá podiely $s_1, \ldots, s_{N_1}$ účastníkom cez bezpečný kanál. (Všimnime si, že pri prvej úrovni schémy $\mathcal{D}$ konštruuje schému presne tak isto, ako pri Shamirovej prahovej schéme.)

4. Dôveryhodná osoba $\mathcal{D}$ zvolí náhodne koeficienty $a_{2,1}, \ldots, a_{2,T_2}$ polynómu $f_2(x)$ stupňa[29] T_2 tak, aby pre $1 \leq i \leq N_1$ platilo $f_1(x_i) = f_2(x_i)$.
$$f_2(x) = K + a_{2,1}x + a_{2,2}x^2 + \ldots + a_{2,T_2}x^{T_2}$$

5. $\mathcal{D}$ vyberie po dvoch rôzne hodnoty $x_{N_1+1}, \ldots, x_{N_2} \in \mathcal{S} \setminus \{0\}$. Okrem podmienky $x_i \neq x_j$, pre $1 \leq i < j \leq N_2$, je potrebné splniť aj ďalšie podmienky[30], ktoré sú popísané v kapitole 5.6 Matica Systému.

[28] Výber nemusí byť náhodný, vhodná voľba môže byť napríklad $x_1 = 1$, $x_2 = 2$, ...

[29] Voľbu stupňa polynómu T_2 ponecháme zatiaľ bokom, vrátime sa k nej v kapitole 5.5 Voľba polynómu.

[30] Autori schémy (Ghodosi, Pieprzyk, Safavi-Naini) sa domnievajú, že je možná akákoľvek voľba po dvoch rôznych nenulových $x_1, \ldots, x_{N_\ell}$. Naša práca však ukazuje, že to je síce nutná, nie však postačujúca podmienka bezchybnej funkcie schémy.

6. $\mathcal{D}$ vypočíta podiely účastníkov, čo budú hodnoty polynómu $f_2(x_i)$ v prislúchajúcich bodoch (pre $i = N_1 + 1, \ldots, N_2$).

$$s_i = f_2(x_i) = K + a_{2,1}x_i + a_{2,2}x_i^2 + \ldots + a_{2,T_2}x_i^{T_2}.$$

Dôveryhodná osoba $\mathcal{D}$ odovzdá podiely účastníkom úrovne P_2, prostredníctvom bezpečného kanála. Podiely účastníkov úrovne P_1 ostávajú nezmenené.

Podobne, by sme mohli rozšíriť schému na trojúrovňovú. Zvolili by sme polynóm $f_3(x)$ stupňa T_3, vybrali $x_{N_2+1}, \ldots, x_{N_3}$, vypočítali podiely a mohli pokračovať až po úroveň $\mathcal{P}_\ell$.

Takto zostrojenú rozšírenú Shamirovu schému s prahom t_i a počtom účastníkov N_i, ktorej podiely budú generované pomocou voľby polynómu stupňa nanajvýš T_i, budeme označovať za schému $(t_i, N_i)_{T_i}$ prahovú.

Zatiaľ popísaný algoritmus vysvetľuje činnosť schémy len približne. Na to, aby bol plne funkčný, musíme vysvetliť, ako sa dá zvoliť polynóm $f_2(x)$, tak aby pre $i = 1, \ldots, N_1$ platilo $f_1(x_i) = f_2(x_i)$ a objasniť voľbu stupňa T_2 tohto polynómu. Ďalej bude potrebné objasniť bezpečnosť popísaného algoritmu.

5.5 Voľba polynómu

Je jasné, že voľba polynómu $f_2(x)$, $f_3(x)$ atď. nemôže byť úplne náhodná. Vyplýva to z toho, že pre polynóm $f_2(x)$ požadujeme, aby v bodoch, ktoré poznajú účastníci $\mathcal{P}_1$ (vo dvojiciach $(x_1, s_1), \ldots, (x_{N_1}, s_{N_1})$), ostali zachované hodnoty. Veľmi dôležitá je aj voľba stupňa polynómu T_2. Pretože na polynóm kladieme viac obmedzujúcich podmienok ako Shamirova (t_2, N_2)-prahová schéma, môžeme predpokladať, že jeho stupeň bude vyšší, $T_2 > t_2 - 1$.

Zapíšme teda sústavu rovníc, ktorá opíše požiadavku $s_i = f_1(x_i) = f_2(x_i)$ (pre $i = 1, \ldots, N_1$).

$$\begin{aligned} K + a_{1,1}x_1 + \ldots + a_{1,T_1}x_1^{T_1} &= K + a_{2,1}x_1 + \ldots + a_{2,T_2}x_1^{T_2} \\ &\vdots \\ K + a_{1,1}x_{N_1} + \ldots + a_{1,T_1}x_{N_1}^{T_1} &= K + a_{2,1}x_{N_1} + \ldots + a_{2,T_2}x_{N_1}^{T_2} \end{aligned}$$

Tento vzťah by sme mohli opísať pomocou sústavy lineárnych rovníc[31].

$$\begin{aligned} (a_{2,1} - a_{1,1})\, x_1 + (a_{2,2} - a_{1,2})\, x_1^2 + \ldots + (a_{2,T_1} - a_{1,T_1})x_1^{T_1} + a_{2,T_1+1}x_1^{T_1+1} + \ldots + x_1^{T_2} &= 0 \\ &\vdots \\ (a_{2,1} - a_{1,1})x_{N_1} + (a_{2,2} - a_{1,2})x_{N_1}^2 + \ldots + (a_{2,T_1} - a_{1,T_1})x_{N_1}^{T_1} + a_{2,T_1+1}x_{N_1}^{T_1+1} + \ldots + x_{N_1}^{T_2} &= 0 \end{aligned}$$

[31] Všimnime si, že po dosadení verejných parametrov schémy $x_1, \ldots, x_{N_1}$ sa jedná o sústavu lineárnych rovníc.

Túto sústava N_1 rovníc môže zostaviť ktokoľvek, kto pozná verejné parametre schémy. Sústava rovníc sa dá prepísať na vzťah

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{T_2-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{T_2-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{N_1} & x_{N_1}^2 & \dots & x_{N_1}^{T_2-1} \end{pmatrix} \begin{pmatrix} a_{2,1} - a_{1,1} \\ \vdots \\ a_{2,T_1} - a_{1,T_1} \\ a_{2,T_1+1} \\ \vdots \\ a_{2,T_2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Predpokladajme, že máme prístupovú množinu účastníkov $\mathcal{A}$. Ak $\mathcal{A} \in \Gamma_1$ patrí medzi prístupové množiny prvej úrovne, je jasné, že schéma funguje ako Shamirova prahová schéma. Zamyslime sa však hlavne nad prípadom, ak $\mathcal{A} \in \Gamma_2$.

Od schémy požadujeme, aby bolo možné vypočítať kľúč K ako aj celý polynóm $f_2(x)$, ak poznáme aspoň t_2 podielov účastníkov $\mathcal{P}^2$. Na základe týchto podielov $s_{i_1}, s_{i_2}, s_{i_{t_2}}$ je kombinátor schopný zostaviť sústavu t_2 rovníc v tvare $s_{i_j} = f_2(x_{i_j})$ (pre $1 \leq j \leq t_2$).

$$\begin{aligned} s_{i_1} &= K + a_{2,1}x_{i_1} + \dots + a_{2,T_2}x_{i_1}^{T_2} \\ &\vdots \\ s_{i_{t_2}} &= K + a_{2,1}x_{i_{t_2}} + \dots + a_{2,T_2}x_{i_{t_2}}^{T_2} \end{aligned}$$

Prvých N_1 lineárne nezávislých rovníc môže vytvoriť ktokoľvek, kto pozná verejné parametre schémy. Ďalších t_2 lineárne nezávislých rovníc dokáže napísať kombinátor. Predpokladajme, že všetkých N_1+t_2 rovníc je lineárne nezávislých[32]. Potom sústava bude mať jednoznačné riešenie práve vtedy, ak počet neznámych bude taký istý, ako je počet rovníc. Označme počet rovníc $r = N_1 + t_2$.

Neznáme, ktoré sú v danej sústave sú:

- kľúč K,
- koeficienty $a_{1,1}, \dots, a_{1,T_1}$ polynómu T_1,
- koeficienty $a_{2,1}, \dots, a_{2,T_2}$ polynómu T_2.

Pretože počet rovníc a neznámych by mal byť rovnaký, môžeme vypočítať stupeň

[32]To, že prvá sústava je lineárne nezávislá a druhá tiež, nedokazuje, že ak sústavy spojíme aj výsledná sústava bude lineárne nezávislá. Predpoklad, kedy sa to stane budeme skúmať neskôr.

T_2 polynómu f_2.

$$\begin{aligned} \overbrace{1+T_1}^{t_1}+T_2 &= N_1+t_2 \\ T_2 &= N_1+(t_2-t_1) \end{aligned}$$

Skúsme našu úvahu zovšeobecniť pre ľubovoľných množinu $\mathcal{A}$ prístupovej na m úrovni. Zatiaľ predpokladajme, že rovnice budú nezávislé. Neskôr si objasníme podmienky, kedy bude náš predpoklad pravdivý.

Z rovnosti $f_1(x_i) = f_2(x_i)$ pre $i = 1,\ldots,x_{N_1}$ môže každý, kto pozná verejné parametre schémy zostaviť N_1 rovníc v tvare

$$(a_{2,1}-a_{1,1})x_i+(a_{2,2}-a_{1,2})x_i^2+\ldots+(a_{2,T_1}-a_{1,T_1})x_i^{T_1}+a_{2,T_1+1}x^{T_1+1}+\ldots+x_i^{T_2}=0.$$

Ďalších N_2 rovníc sa dá zostaviť z rovnosti $f_2(x_i) = f_3(x_i)$ pre $i = 1,\ldots,x_{N_2}$. Rovnice $f_1(x_i) = f_3(x_i)$ pre prvých N_1 hodnôt nebudeme zostavovať, pretože už vyplývajú z ostatných rovníc.

$$(a_{3,1}-a_{2,1})x_i+(a_{3,2}-a_{2,2})x_i^2+\ldots+(a_{3,T_2}-a_{2,T_2})x_i^{T_2}+a_{3,T_2+1}x^{T_2+1}+\ldots+x_i^{T_3}=0$$

Takto sa dá takto zostaviť $\sum_{i=1}^{m-1} N_i$ rovníc. Ďalších t_m rovníc sa môže kombinátor zostaviť v tvare $s_{i_j} = f_m(x_{i_j})$. Systém, ktorý takto dokázal kombinátor zostaviť, má $r_m = t_m + \sum_{i=1}^{m-1} N_i$ rovníc.

V rovniciach sú neznámymi kľúč K a koeficienty všetkých zvolených polynómov $a_{1,1},\ldots,a_{1,T_1},a_{2,1},\ldots,a_{2,T_2},\ldots,a_{m,1},\ldots a_{m,T_m}$. Ak predpokladáme, že rovnice sú lineárne nezávislé, počet rovníc musí byť rovnaký, ako počet neznámych, aby mal systém jednoznačné riešenie.

$$\begin{aligned} 1+\sum_{i=1}^{m} T_i &= t_m+\sum_{i=1}^{m-1} N_i \\ 1+T_m+\sum_{i=1}^{m-1} T_i &= t_m+\sum_{i=1}^{m-1} N_i \\ T_m &= t_m-1+\sum_{i=1}^{m-1}(N_i-T_i) \end{aligned}$$

Tento rekurentný výraz je pomerne neprehľadný. Trik, ako by sa dal zjednodušiť, je počítať hodnotu výrazu $T_m - T_{m-1}$ a z výsledku sa pokúsime vyjadriť T_m. Takto

však obmedzíme platnosť úpravy výrazu, len pre $m > 1$. Pre $m = 1$ zo Shamirovej prahovej schémy vieme, že $T_1 = t_1 - 1$.

$$\begin{aligned} T_m - T_{m-1} &= t_m - t_{m-1} + N_{m-1} - T_{m-1} \\ T_m &= N_{m-1} + (t_m - t_{m-1}) \end{aligned}$$

5.6 Matica systému

Doteraz sme znalosti kombinátora zapisovali pomocou systému lineárnych rovníc. Jeden systém rovníc, sme zostavili na základe rovnosti polynómov vo vybraných bodoch ($f_1(x_i) = f_2(x_i)$) a ďalší systém rovníc na základe podielov ($s_{i_j} = f_m(x_{i_j})$). Oba systémy rovníc sme spojili a na ich základe počítali kľúč K a prípadne aj koeficienty polynómov.

Teraz sa pokúsime systém rovníc prepísať do maticového tvaru. Budeme vyšetrovať podmienky, za akých je možné zrekonštruovať kľúč a dokazovať bezpečnosť schémy.

Kombinátor sa môže pokúsiť o rekonštrukciu kľúča na ľubovoľnej z ℓ úrovní schémy. Jeho úlohou pri rekonštrukcii kľúča pomocou podielov účastníkov množiny $\mathcal{A}$ bude overiť, na ktorej úrovni je množina prístupová. Ak na žiadnej, ukážeme, že o rekonštrukciu sa nemá význam pokúšať.

Predpokladajme však, že množina účastníkov je prístupová úrovni m. Kombinátor vyberie takú vlastnú podmnožinu $\mathcal{A}_m \subseteq A$, ktorá má t_m účastníkov, ktorá je minimálna prístupová[33] na úrovni m. Pri rekonštrukcii použije len podiely účastníkov množiny $\mathcal{A}_m$. Zvyšné podiely nevyužije, alebo použije len na overenie, či niektorý z účastníkov nepodvádzal.

[33] Z množiny $\mathcal{P}^1$ kombinátor vyberie najviac t_1 účastníkov, z $\mathcal{P}^2$ najviac t_2 účastníkov, atď.

Vektorom neznámych[34] **stupňa** m budeme nazývať stĺpcový vektor $\bar{u}$, zložený z r_m riadkov (v uvedenom poradí):

- kľúč K,
- koeficienty $a_{1,1}, \ldots, a_{1,T_1}$,
- rozdiely koeficientov $a_{2,1} - a_{1,1}, \ldots, a_{2,T_1} - a_{1,T_1}$a koeficienty $a_{2,T_1+1}, \ldots, a_{2,T_2}$,
- rozdiely koeficientov $a_{3,1} - a_{2,1}, \ldots, a_{3,T_2} - a_{2,T_2}$a koeficienty $a_{3,T_2+1}, \ldots, a_{3,T_3}$ atď.

Ak by sme mali popísať, čo obsahuje vektor neznámych, okrem kľúča a koeficientov $a_{1,1}, \ldots, a_{1,T_1}$ polynómu $f_1(x)$, ktoré sú snáď jasné, obsahuje vždy koeficienty polynómu $f_{i+1}(x) - f_i(x)$ (pre $i = 1, \ldots, m-1$). Čiže $a_{i+1,1} - a_{i,1}, \ldots, a_{i+1,T_i} - a_{i,T_i}$ a $a_{i+1,T_i+1}, \ldots, a_{i+1,T_{i+1}}$.

Maticou rovnosti polynómov vo vybraných bodoch stupňa m budeme nazývať stupňovitú maticu M_r skladajúcu sa z $(m-1) \times (m+1)$ blokov v tvare[35] (Blok i, j má veľkosť $N_i \times 1$, ak $j = 1$, inak $N_i \times T_{j+1}$.) .

$$\left(\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c|c} 0 & 0 & \ldots & 0 & x_1 & x_1^2 & \ldots & x_1^{T_2} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & x_{N_1} & x_1^2 & \ldots & x_{N_1}^{T_2} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \hline 0 & 0 & \ldots & 0 & 0 & 0 & \cdots & 0 & x_1 & \cdots & x_1^{T_3} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \cdots & 0 & x_{N_2} & \cdots & x_{N_2}^{T_3} & \cdots & 0 & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & x_1 & \cdots & x_1^{T_m} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & x_{N_{m-1}} & \cdots & x_{N_{m-1}}^{T_m} \end{array}\right)$$

Matica rovnosti polynómov vo vybraných bodoch je navrhnutá tak, aby vzťah $f_i(x_j) = f_{i+1}(x_j)$, pre $i = 1, \ldots, m-1$ a $j = 1, \ldots, N_i$, sa dal vyjadriť pomocou maticového počtu (Kde $\bar{0}$ znamená nulový vektor príslušnej veľkosti.) .

$$M_r \bar{u} = \bar{0}$$

[34] Vektor neznámych obsahuje všetky neznáme – kľúč K a koeficienty $a_{1,1}, \ldots, a_{m,T_m}$. Sú však zapísané pomocou rozdielov. Tie sa dajú ľahko previesť na koeficienty, alebo naopak. Nami zvolený tvar je vhodný na zostavenie prehľadnej matice systému.

[35] Na označenie začiatku a konca blokov budeme používať čiary | a —

Túto maticu môže napísať prakticky ktokoľvek, kto pozná prístupovú štruktúru a verejne známe parametre schémy. Hodnosť matice rovnosti polynómov vo vybraných bodoch je $N_1 + N_2 + \ldots + N_{m-1} = r_m - t_m$.

Rozpíšme maticu na jednotlivé riadky a uvedomme si, aká požiadavka je vlastne zapísaná v predchádzajúcom vzťahu. V prvom riadku je zapísané (ak nezapisujeme členy, kde sa násobí nulou)

$$(a_{2,1}-a_{1,1})x_1+(a_{2,2}-a_{1,2})x_1^2+\ldots+(a_{2,T_1}-a_{1,T_1})x_1^{T_1}+a_{2,T_1+1}x_1^{T_1+1}+\ldots+a_{2,T_2}x_1^{T_2}=0.$$

Toto je prepisom $f_1(x_1) = f_2(x_1)$. V nasledujúcom riadku je požiadavka na rovnosť polynómov $f_1(x)$ a $f_2(x)$ v bode x_2. Požiadavka rovnosti $f_1(x)$ a $f_2(x)$ je zapísaná v prvých N_1 riadkoch. V nasledujúcich N_2 riadkoch je zapísaná požiadavka $f_2(x_i) = f_3(x_i)$, pred $x_1, \ldots, x_{N_2}$ atď.

Vektorom podielov zostaveným pre (minimálnu prístupovú) množinu účastníkov $\mathcal{A}_m \in \Gamma_m$, kde[36] $\mathcal{A}_m = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{t_m}}\}$, nazývame stĺpcový vektor $\bar{s} = (s_{i_1}, s_{i_2}, \ldots, s_{i_{t_m}})^T$.

Maticou kombinátora zostaveným pre (minimálnu prístupovú) množinu účastníkov $\mathcal{A}_m \in \Gamma_m$, kde $\mathcal{A}_m = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{t_m}}\}$, nazývame maticu M_k zloženú z $1 \times m+1$ blokov v tvare

$$\left(\begin{array}{c|ccc|ccc|ccc|c|ccc}
1 & x_{i_1} & \cdots & x_{i_1}^{T_1} & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{T_2} & x_{i_1} & \cdots & x_{i_1}^{T_3} & \cdots & x_{i_1} & \cdots & x_{i_1}^{T_m} \\
1 & x_{i_2} & \cdots & x_{i_2}^{T_1} & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{T_2} & x_{i_2} & \cdots & x_{i_2}^{T_3} & \cdots & x_{i_2} & \cdots & x_{i_2}^{T_m} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
1 & x_{i_{t_m}} & \cdots & x_{i_{t_m}}^{T_1} & x_{i_{t_m}} & x_{i_{t_m}}^2 & \cdots & x_{i_{t_m}}^{T_2} & x_{i_{t_m}} & \cdots & x_{i_{t_m}}^{T_3} & \cdots & x_{i_{t_m}} & \cdots & x_{i_{t_m}}^{T_m}
\end{array}\right)$$

Hodnosť matice kombinátora je t_m.

Matica kombinátora je navrhnutá tak, aby sa vzťah $f_m(x_{i_j}) = s_{i_j}$ pre množinu $\mathcal{A}_m \in \Gamma_m$, sa dal prepísať do tvaru

$$M_k \bar{u} = \bar{s}$$

Aby sme sa o tom presvedčili, uvedomme si, že

$$\begin{aligned}
(1\ x \ldots x^{T_1}\ 0 \ldots 0)\bar{u} &= f_1(x) \\
(1\ x \ldots x^{T_1}\ x \ldots x^{T_2}\ 0 \ldots 0)\bar{u} &= \underbrace{f_1(x) + (f_2(x) - f_1(x))}_{f_2(x)} \\
(1\ x \ldots x^{T_1}\ x\ x^2 \ldots x^{T_2}\ x \ldots x^{T_3}\ 0 \ldots 0)\bar{u} &= \underbrace{f_3(x) + (f_3(x) - f_2(x))}_{f_3(x)}
\end{aligned}$$

[36] $i_1, \ldots, i_{t_m}$ je prečíslovanie účastníkov.

Všetky doterajšie znalosti môžeme zhrnúť do vzťahu jediného vzťahu

$$\left(\frac{M_k}{M_r}\right)\bar{u} \;=\; \left(\frac{\bar{s}}{\bar{0}}\right) \tag{2}$$

Maticu $M_s = \left(\frac{M_k}{M_r}\right)$ budeme nazývať **matica systému prislúchajúca (minimálnej prístupovej) množine účastníkov** $\mathcal{A}_m$. Maticu systému prislúchajúcu k ľubovoľnej prístupovej množine $\mathcal{A}_m$ dokáže zostrojiť ktokoľvek, kto pozná prístupovú štruktúru a verejné parametre schémy $x_1, \ldots, x_n$.

Matica M_s má $r_m = t_m + \sum_{i=1}^{m-1} N_i$ riadkov a $r_m = 1 + \sum_{i=1}^{m-1} T_i$ stĺpcov a teda je štvorcová.

Na to, aby výpočet kľúča pre množinu účastníkov $\mathcal{A}_m$ bol jednoznačný, je postačujúcou podmienkou to, že matica systému M_s prislúchajúca $\mathcal{A}_m$ je regulárna a my poznáme vektor podielov $\bar{s}$ prislúchajúci tejto množine.

Algoritmus kombinátora spočíva vo výpočte M_s^{-1}. Vektor neznámych $\bar{u}$ vypočítame zo vzťahu (pozri vzťah (2))

$$\bar{u} = M_s^{-1}\left(\frac{\bar{s}}{\bar{0}}\right)$$

Predpokladajme, že matica $M_s^{-1} = (b_{i,j})$, pre $i = 1, \ldots, r_m$ a $j = 1, \ldots, r_m$. Je jasné, že na výpočet kľúča K nám stačí vypočítať $b_{1,1}, \ldots, b_{1,t_m}$, pretože

$$K = b_{1,1}s_{i_1} + b_{1,2}s_{i_2} + \ldots + b_{1,t_m}s_{i_{t_m}}. \tag{3}$$

Ak množina účastníkov $\mathcal{A}_m$ je prístupová, jej matica systému M_s pre úroveň m je regulárna a pre inverznú maticu k matici systému $M_s^{-1} = (b_{i,j})$ platí $b_{1,1}b_{1,2}\ldots b_{1,t_m} \neq 0$, potom množina účastníkov minimálna prístupová pre úroveň m.

Dôkaz: Nech poznáme všetky podiely množiny $\mathcal{A}_m$ okrem podielu s_{i_j}. Potom po dosadení do vzťahu (3) dostaneme rovnicu $K = \text{konštanta} + b_j s_{i_j}$. Pretože s_{i_j} môže byť z nášho pohľadu ľubovoľné číslo z $\mathcal{K}$, aj súčin $b_j s_{i_j}$ a teda aj kľúč môžu byť kdekoľvek v $\mathcal{K}$.

Schéma je perfektná a jej prístupová štruktúra zodpovedá popísanej, ak matica systému M_s zodpovedajúca každej minimálnej prístupovej množiny úrovne 1 až ℓ je regulárna a pre jej inverznú maticu $M_s^{-1} = (b_{i,j})$ platí $b_{1,1}b_{1,2}\ldots b_{1,t_m} \neq 0$.

5.7 Algoritmus dôveryhodnej osoby

Ako sme si ukázali multiúrovňovú schému na zdieľanie tajomstva je teda možné zostrojiť pomocou nasledujúceho algoritmu:

1. Dôveryhodná osoba vyberie[37] n po dvoch rôznych čísel $x_1, \ldots, x_n \in Z_p \setminus \{0\}$, ktoré zverejní. Následne náhodne zvolí polynóm $f_1(x) = K + a_{1,1}x + \ldots + a_{1,T_1}x^{T_1}$ stupňa $T_1 = t_1 - 1$ a vypočíta podiely účastníkov $s_1, \ldots, s_{n_1}$ ($s_i = f_1(x_i)$) pre účastníkov úrovne $\mathcal{P}_1$.
   Výsledkom je $(t_1, N_1)_{T_1}$ schéma.

2. Pre $i = 2, \ldots, \ell$ urob:

   - pre $(t_{i-1}, N_{i-1})_{T_{i-1}}$ schému zostroj rozšírenú $(t_i, N_i)_{T_i}$.
   - vypočítaj n_i podielov $s_{1+N_{i-1}}, \ldots, s_{N_i}$ pre účastníkov úrovne $\mathcal{P}_i$ ($s_j = f_i(x_j)$).

3. Dôveryhodná osoba doručí podiely účastníkom cez bezpečný kanál.

5.8 Príklady

Uveďme príklad jednoduchý dvojúrovňovej schémy. O zloženie kľúča sa budú pokúšať rôzne množiny účastníkov. Verejné parametre schémy $x_1, \ldots, x_n$ sú zvolené tak, aby sme mohli demonštrovať, že kombinátor môže, ale nemusí byť úspešný.

Majme dvojúrovňovú schému. Nech prvá úroveň má troch účastníkov $\mathcal{P}_1 = \{P_1, P_2, P_3\}$, pričom na rekonštrukciu kľúča by mali stačiť ľubovoľní dvaja z nich. Na druhej úrovni sú traja účastníci $\mathcal{P}_2 = \{P_4, P_5, P_6\}$. Na úspešnú rekonštrukciu kľúča sú potrební aspoň traja účastníci z úrovní $\mathcal{P}_1$ alebo $\mathcal{P}_2$.

Schéma, ktorú sme navrhli je na prvej úrovni $(2,3)_1$-prahová[38], na druhej úrovni $(3,6)_4$-prahová[39].

$$t_1 = 2 \qquad N_1 = 3$$
$$t_2 = 3 \qquad N_2 = 6$$

[37] Nemusí náhodne, možná voľba je napríklad $x_i = i$

[38] $(2,3)_1$-prahová schéma nám hovorí, že na zloženie kľúča by mali byť potrebné podiely aspoň dvoch účastníkov. Na prvej úrovni sú traja účastníci. Polynóm $f_1(x)$ je prvého stupňa.

[39] $(3,6)_4$-prahová schéma nám hovorí, že na druhej úrovni by na rekonštrukciu kľúča mali byť potrebné tri podiely. V schéme je 6 účastníkov úrovne nanajvýš 2. Podiely sme vypočítali pomocou polynómu $f_2(x)$ stupňa 4.

Dôveryhodná osoba náhodne zvolila koeficienty $x_1, \ldots, x_6$ nasledovne:

$$\begin{aligned} x_1 &= 1 \\ x_2 &= 3 \\ x_3 &= 4 \\ \hline x_4 &= 2 \\ x_5 &= 5 \\ x_6 &= 6 \end{aligned}$$

Všetky výpočty budeme robiť nad poľom $Z_7 = \mathcal{K} = \mathcal{S}$.

5.8.1 Príklad úspešnej rekonštrukcie

Nech sa o rekonštrukciu kľúča pokúsi kombinátor, ktorý pozná podiely s_3, s_5, s_6 účastníkov P_3, P_5, P_6. Podľa popísanej prístupovej štruktúry by títo účastníci mali tvoriť minimálnu prístupovú množinu.

O rekonštrukciu sa pokúsime na základe zostavenia matice systému pre túto množinu účastníkov. Matica kombinátora pre známe podiely s_3, s_5, s_6 je

$$M_k = \begin{pmatrix} 1 & 4 & 4 & 2 & 1 & 4 \\ 1 & 5 & 5 & 4 & 6 & 2 \\ 1 & 6 & 6 & 1 & 6 & 1 \end{pmatrix}$$

Matica rovnosti polynómov pre $x_1 = 1, x_2 = 3$ a $x_3 = 4$ je

$$M_r = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 3 & 2 & 6 & 4 \\ 0 & 0 & 4 & 2 & 1 & 4 \end{pmatrix}$$

Kombinátor zostaví maticu systém $M_s = \left(\frac{M_k}{M_s}\right)$. Následne vypočíta inverznú maticu M_s^{-1} k matici systému. Na základe rovnice $\bar{u} = M_s^{-1} \left(\frac{\bar{s}}{\bar{0}}\right)$ vyjadrí kľúč a koeficienty $a_{1,1}, a_{2,1}, a_{2,2}, a_{2,3}$ a $a_{2,4}$ ako lineárnu kombináciu jemu známych podielov.

$$\begin{pmatrix} K \\ a_{1,1} \\ a_{2,1} - a_{1,1} \\ a_{2,2} \\ a_{2,3} \\ a_{2,4} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 4 & 3 & 1 & 6 & 4 \\ 0 & 6 & 1 & 5 & 2 & 4 \\ 1 & 5 & 1 & 4 & 5 & 6 \\ 6 & 2 & 6 & 5 & 1 & 5 \\ 3 & 1 & 3 & 5 & 4 & 1 \\ 4 & 6 & 4 & 1 & 4 & 1 \end{pmatrix}}_{M_s^{-1}} \begin{pmatrix} s_3 \\ s_5 \\ s_6 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Na základe tejto rovnice vieme, že kľúč možno vyjadriť pomocou podielov ako

$$K = s_3 + 4s_5 + 3s_6$$

Táto množina účastníkov je minimálna prístupová. Predpokladajme, že sa o rekonštrukciu kľúča pokúsi útočník, ktorý pozná len dvojicu z podielov s_3, s_5 a s_6. Po dosadení podielov, ktoré pozná dostane rovnosť (nech posledný podiel je s)

$$K = k_0 + k_1 s$$

V tejto rovnosti útočník pozná koeficienty k_0, k_1 a nepozná kľúč K a podiel s. Podiel s sa môže rovnať ľubovoľnému číslu zo Z_p. Každému z rovnakou pravdepodobnosťou. Pretože konštanta k_1 je nenulová, šanca na rekonštrukciu kľúča nie je o nič vyššia, ako keby sme nepoznali žiaden z podielov.

5.8.2 Príklad neúspešnej rekonštrukcie

V tej istej schéme ako v predošlom príklade predpokladajme, že o rekonštrukciu sa pokúsi kombinátor, ktorý pozná podiely účastníkov s_3, s_4, s_5.

Kombinátor zostaví maticu systému a na je základe rovnosť

$$\underbrace{\begin{pmatrix} 1 & 3 & 3 & 2 & 6 & 4 \\ 1 & 4 & 4 & 2 & 1 & 4 \\ 1 & 5 & 5 & 4 & 6 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 3 & 2 & 6 & 4 \\ 0 & 0 & 4 & 2 & 1 & 4 \end{pmatrix}}_{M_s} \underbrace{\begin{pmatrix} K \\ a_{1,1} \\ a_{2,1} - a_{1,1} \\ a_{2,2} \\ a_{2,3} \\ a_{2,4} \end{pmatrix}}_{\bar{u}} = \underbrace{\begin{pmatrix} s_3 \\ s_4 \\ s_5 \\ 0 \\ 0 \\ 0 \end{pmatrix}}_{\frac{\bar{s}}{0}}$$

Pokus vyjadriť kľúč K a ostatné premenné z vektoru neznámych ako lineárnu kombináciu podielov však zlyhá. Matica systému M_s je singulárna. Znamená to, že premenné z vektoru neznámych sa pre nevhodne zvolené hodnoty $x_1, \ldots, x_n$ nemusia dať vyjadriť ako lineárna kombinácia. Pri ručnom počítaní tejto sústavy narazíme na rovnosť, kde podiel s_3 môžeme vyjadriť ako lineárnu kombináciu zostávajúcich podielov s_4 a s_5. Kľúč však pomocou týchto podielov nevyjadríme.

5.8.3 Výpočet kľúča z podielov neprístupovej množiny

Softvérový produkt, ktorý je súčasťou diplomovej práce, nás upozornil, že množina účastníkov $\{P_4, P_6\}$, ktorá by mala mala byť neprístupová dokáže zrekonštruovať kľúč.

Softvérový produkt to zistil tak, že vypočítal inverznú maticu M_s^{-1} k matici systému pre účastníkov P_3, P_4 a P_6 a vyšlo mu:

$$\begin{pmatrix} K \\ a_{1,1} \\ a_{2,1} - a_{1,1} \\ a_{2,2} \\ a_{2,3} \\ a_{2,4} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 5 & 3 & 2 & 1 & 4 \\ 2 & 4 & 1 & 3 & 5 & 4 \\ 5 & 1 & 1 & 0 & 4 & 6 \\ 2 & 6 & 6 & 2 & 2 & 5 \\ 1 & 3 & 3 & 0 & 1 & 1 \\ 6 & 4 & 4 & 6 & 0 & 2 \end{pmatrix}}_{M_s^{-1}} \begin{pmatrix} s_3 \\ s_4 \\ s_6 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Na základe tejto matice môžeme kľúč napísať ako lineárnu kombináciu podielov nasledovne:

$$K = 5s_4 + 3s_6$$

Znamená to, že o úspešnú rekonštrukciu sa môžu pokúsiť účastníci P_4 a P_6 len na základe svojich podielov. Samozrejme podobný problém s nulovým koeficientom, ktorým by sme mali násobiť podiel účastníka sa stretneme aj pri ďalších množinách účastníkov ($\{P_1, P_4, P_6\}, \{P_2, P_4, P_6\}, \{P_3, P_4, P_6\}, \{P_4, P_5, P_6\}$), ktoré sú nadmnožinou množiny $\{P_4, P_6\}$.

Časť III

Opis postupu riešenia

6 Súvis s diplomovým projektom

Cieľom diplomového projektu bolo zoznámenie sa s problematikou schém na zdieľanie tajomstva. Už samotný názov diplomového projektu „Neúplné a kumulatívne schémy na zdieľanie tajomstva" naznačil, aké schémy boli objektom nášho záujmu.

Existuje niekoľko charakteristík, ktoré často používame ako kritérium vhodnosti použitia schémy v danom prostredí. Týmito charakteristikami obvykle bývajú bezpečnosť, pružnosť prístupovej štruktúry (v zmysle prispôsobiteľnosť, flexibilita) a pomer medzi dĺžkou podielu a kľúča. Ďalším kritériom, ktoré pri výbere schémy na zdieľanie tajomstva môže, ale nemusí hrať úlohu, je schopnosť odhaliť podvádzajúceho účastníka.

Pre kumulatívne schémy na zdieľanie tajomstva je charakteristická veľká pružnosť prístupovej štruktúry. Kumulatívne schémy umožňujú implementovať akúkoľvek úplnú monotónnu prístupovú štruktúru. Kumulatívne schémy dokonca umožňujú urobiť návrh schémy skôr, ako poznáme prístupovú štruktúru. Táto je potom len jedným zo vstupných parametrov schémy.

V kumulatívnych schémach sú všetky množiny účastníkov buď prístupové, alebo neprístupové. Keďže semiprístupové množiny účastníkov neexistujú, nepredstavujú ani bezpečnostné riziko.

Cenou, ktorú kumulatívne schémy platia za svoje inak neobyčajne dobré vlastnosti, je veľmi nepriaznivý pomer medzi dĺžkou podielu a kľúča. Tento pomer sa stáva ešte horším v prípade, ak schéma na zdieľanie tajomstva umožňuje odhaliť podvádzajúceho účastníka.

Neúplné schémy na zdieľanie tajomstva sú založené na zohľadnení iných charakteristík ako pri kumulatívnych schémach. Ich najväčšou výhodou je priaznivý pomer[40] medzi dĺžkou podielu a dĺžkou kľúča. Neúplné schémy často dokážu odhaliť podvádzajúceho účastníka bez výrazného zhoršenia tohto pomeru.

Pružnosť prístupovej štruktúry neúplných schém býva podstatne nižšia ako pri kumulatívnych schémach. V neúplných schémach existujú aj semiprístupové množiny

[40] Pre úplné schémy často aj teoreticky nedosiahnuteľný.

účastníkov. Semiprístupové množiny účastníkov dokážu získať aspoň neúplnú informáciu o kľúči, preto ich môžeme považovať za bezpečnostné riziko.

V diplomovom projekte sme sa zamerali prevažne na tieto dve kategórie schém. Multiúrovňové schémy, ktoré skúmame v tej diplomovej práci čiastočne zohľadňujú podstatné charakteristiky oboch skupín. Pri troche nadsádzky sa dá povedať, že multiúrovňové schémy predstavujú určitý kompromis medzi neúplnými a kumulatívnymi schémami.

Pružnosť ich prístupovej štruktúry je stále pomerne vysoká, aj keď už nie je až taká ako pri kumulatívnych schémach. Prispôsobenie prístupovej štruktúry konkrétnym požiadavkám je možné urobiť pomocou voľby prahov $t_1, \ldots, t_\ell$ a počtu účastníkov $n_1, \ldots, n_\ell$ na jednotlivých úrovniach schémy.

V schéme nie sú žiadne semiprístupové množiny účastníkov. Bezpečnosť multiúrovňových schém je porovnateľná s kumulatívnymi schémami.

Multiúrovňové schémy naviac majú veľmi dobrý pomer medzi dĺžkou podielu a kľúča. Toto je vlastnosť typická pre neúplné schémy.

Multiúrovňová schéma založená na Shamirovej prahovej schéme (pozri zadanie diplomovej práce) sa dá nájsť v literatúre, konkrétne v článkoch [4] a [5]. Oba články pomerne dobre vystihujú problematiku. Ich autori sa dopustili niekoľkých menších nepresností.

Články neuvádzajú algoritmus kombinátora. Popis prístupovej štruktúry uvádzaný v týchto článkoch je nepresný. Autori článkov sa domnievajú, že voľba verejných parametrov $x_1, \ldots, x_{N_\ell}$ neovplyvní prácu algoritmu, resp. že nech zvolíme tieto parametre akékoľvek nenulové po dvoch rôzne, prístupová štruktúra sa nenaruší.

Táto práca popíše algoritmus kombinátora aj prístupovú štruktúru. Ukážeme si, že nevhodná voľba parametrov $x_1, \ldots, x_{N_\ell}$ môže narušiť prístupovú štruktúru.

Nevhodnou voľbou verejných parametrov môžu nastať aj nasledujúce situácie:

1. Niektoré množiny účastníkov, ktoré by podľa opisu prístupovej štruktúry mali byť prístupové, nedokážu získať žiadnu informáciu o kľúči.

2. Niektoré množiny účastníkov, ktoré by podľa opísanej prístupovej štruktúry mali byť neprístupové, dokážu vypočítať kľúč na základe známych podielov.

7 Špecifikácia požiadaviek

7.1 Analýza problému

V doterajšej práci sme sa venovali schémam na zdieľanie tajomstva, ktoré predstavujú novú a zaujímavú časť matematického poznania. Schémy sme analyzovali ako matematický model, spoznávali sme matematické vlastnosti tohto modelu a porovnávali sme rozličné schémy.

Cieľom diplomovej práce je podrobne popísať multiúrovňové schémy na zdieľanie tajomstva založené na Shamirovej prahovej schéme. Výsledky, ktoré sme zistili teoretickým štúdiom, sa pokúsime prakticky overiť.

Na overenie nám poslúži softvérový produkt, ktorý vytvoríme. Pre tento produkt musíme analyzovať požiadavky a na ich základe navrhnúť a implementovať produkt, ktorý by umožnil potvrdiť teoretické výsledky, ktoré sme dosiahli.

Dôležité je najmä prakticky overiť navrhnuté riešenie pri väčšom počte účastníkov schémy. Významnú úlohu bude hrať výpočtová náročnosť problému. Táto závisí od rozdelenia účastníkov medzi úrovne $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$ ako aj od počtu úrovní ℓ.

Výsledný softvérový produkt nám musí umožniť vložiť parametre $T_1, \ldots, T_\ell$ ako aj $N_1, \ldots, N_\ell$, ktoré určujú prístupovú štruktúru. Ďalej by nám mal umožniť vložiť a overiť parametre $x_1, \ldots, x_\ell$, od ktorých záleží, či prístupová štruktúra bude naozaj taká, ako zadal používateľ. Spomenuté parametre určujú prístupovú štruktúru a sú verejne známe. Neurčujú však kľúč, ani podiely účastníkov.

Zadanie diplomovej práce explicitne nepožaduje konkrétne platformy, na ktorých by mal byť daný softvérový produkt dostupný. Požiadavky, ktoré kladieme na výsledný produkt, nie sú príliš špecifické. Softvérový produkt, ktorý vytvoríme, bude napísaný tak, aby po prekompilovaní mohol byť dostupný na väčšine platforiem.

Súčasťou priloženého elektronického média (CD) budú zdrojové súbory. Takto umožníme používateľovi prekompilovať produkt pod tou platformou, ktorú bude chcieť používať. Spôsob ako nainštalovať potrebné knižnice a následne vytvoriť cieľový program popíšeme v tejto práci. Súčasťou média bude program spustiteľný na platforme Linux (doplneným o grafické prostredie X-Window).

7.2 Výber použitých nástrojov

Pri vypracovaní diplomovej práce bude potrebné vyriešiť viacero problémov. Výber vhodných nástrojov využívaných pri tvorbe softvérového produktu môže prácu

výrazne zrýchliť, zjednodušiť a zlepšiť kvalitu výsledného produktu. Pri voľbe nástrojov by sme mali zobrať musíme zohľadniť viaceré skutočnosti. Najvýznamnejšími kritériami budú:

- jednoduchosť tvorby grafického používateľského prostredia,
- jednoduchosť a použiteľnosť vytvoreného grafického prostredia,
- prenositeľnosť grafických prostredí medzi rôznymi platformami,
- obmedzenia vyplývajúce z licenčných podmienok používaných nástrojov,
- jednoduchosť verifikácie a validácie produktu,
- podpora práce s veľkými číslami[41] a podpora aritmetiky v poli Z_p.
- efektivita implementácie,
- čas potrebný tvorbu vytváraného produktu,
- skúsenosti s používaním vybraných nástrojov.

Voľbu použitých nástrojov by sme mohli rozdeliť na voľbu programovacieho jazyka, voľbu knižníc (orientovaných na grafiku a prácu s veľkými číslami.

Zadanie diplomovej práce explicitne nevyžaduje použitie programovacieho jazyka. Väčšina používaných programovacích jazykov obsahuje podporu práce s veľkými číslami, či už priamo v jazyku, alebo prostredníctvom voľne dostupných knižníc. Vhodná by bola podpora práce priamo v poli Z_p, prípadne podpora zložitejších dátových štruktúr (napríklad vektor, matica, polynóm). Náročnosť vytvárania vhodného grafického prostredia, ako aj jeho prenositeľnosť býva pri rôznych programovacích jazykoch rozdielna.

Po zvážení vlastností programovacích jazykov sme sa s vedúcim diplomovej práce zhodli na tom, že najvýhodnejšie bude softvérový produktu implementovať v jazyku C++. Softvérový produkt bude vznikať pod Linuxom, distribúcia *Mandrake 7.2*. Využijeme kompilátor, ktorý je súčasťou tejto distribúcie *gcc 2.95.3*.

Pri tvorbe grafického prostredia pod operačný systém Linux sa využívajú rôzne podporné knižnice. Spomeňme len *Xt*, *OpenLook*, *OSF/Motif*, *Qt*, *KDE*, *GTK+* a *SDL*. Väčšina z vymenovaných knižníc neponúka veľkú prenositeľnosť a ich použitím by ostal dostupný pre málo platforiem.

[41] Kľúč a podiely účastníkov by mali byť aspoň 128-bitové, ale vhodnejšia by bola neobmedzená dĺžka. Potrebný je napríklad výpočet inverznej matice, násobenie vektora maticou, dosadenie funkčnej hodnoty do polynómu, ... Všetky výpočty sa vykonávajú nad poľom Z_p.

Knižnica *Qt* od firmy *Trolltech* (http://www.trolltech.com) ponúka prenositeľnosť, jednoduchý a čitateľný kód. Je založená na dobre prepracovanom objektovom návrhu. Jej jednoduchosť a efektívnosť som ocenil pri tvorbe tímového projektu, na ktorom sa táto knižnica výborne osvedčila. Knižnica je dostupná pre takmer všetky systémy Unix, Microsoft Windows a MacOS. Jediným nedostatkom tejto inak výbornej knižnice sú licenčné podmienky pod Microsoft Windows a MacOS (pod Linuxom bez problémov). Používanie na tieto platformy je viazané na nekomerčné požitie (čo diplomová práca spĺňa). Posledná dostupná verzia, ktorá je uvoľnená pod platformu Microsoft Windows je *Qt 2.3.0 Non-Commercial Edition* (pod Linuxom je dostupná *Qt/X11 3.1.2 Free Edition*).

Knižnicou, pre prácu s veľkými číslami, ktorá sa osvedčila vďaka svojej rýchlosti, prenositeľnosti (Unix, MS Windows, MacOS) a vhodných licenčných podmienok, je *The GNU Multiple Precision Arithmetic Library* (http://swox.com/gmp). Posledná dostupná verzia je *GMP Edition 4.1.2*.

Táto knižnica sa už viackrát osvedčila v úspešných projektoch. Podporuje prácu s veľkými číslami[42]. Je napísaná v jazyku C. Knižnica nepodporuje zložitejšie údajové štruktúry, ako napríklad vektor, matica, alebo polynóm.

Na GMP je založených viacero knižníc. Medzi tie, ktoré poskytujú a vyššie spomenuté údajové štruktúry, patria *LiDIA* a *NTL*. Obe sú dostupné pre najpoužívanejšie platformy. Po prezretí dokumentácie oboch projektov ako aj projektov využívajúcich tieto knižnice sme ako pre náš projekt vhodnejšiu vybrali knižnicu *LiDIA*.

Knižnicou som sa podrobne zaoberal a po detailnom preskúmaní jej možností, sme sa nakoniec rozhodli nevyužiť ani jej možnosti, ktoré sa iba čiastočne zhodujú s požiadavkami, ktoré kladie náš projekt. Knižnica síce poskytuje dátové štruktúry, ktoré nám chýbajú, ale funkcie sa nie vždy zhodujú. Výhodnejšie bude napísať vlastné funkcie, ktoré budú vykonávať presne to, čo potrebujeme.

Pri modernom programovaní v jazyku C++ sa veľmi často využívajú knižnice šablón *(templates)*. Štandardná knižnica *Standard Template Library* (*STL*), ktorá je súčasťou normy C++, je určite súčasťou každého kompilátora. Knižnica je dostupná pod licenciou *GPL*.

Ďalšiu knižnicu šablón ponúka *Qt*. Pri programovaní rozhrania s touto knižnicou zrejme budeme nútení použiť jej šablóny. Ak budeme potrebovať šablóny, väčšinou použije štandardnú knižnicu *STL*, ktorá inšpirovala autorov knižnice šablón aj v knižnici *Qt* (aj *LiDIA*). *STL* sa vyznačuje väčšou flexibilitou. Príčinou, prečo *STL*

[42]Navyše aj s číslami s pevnou desatinnou čiarkou a zlomkami, ktorých čitateľ a menovateľ sú veľké čísla. Toto sú však funkcie, ktoré zrejme pri tvorbe nášho produktu nevyužijeme.

úplne nenahrádza *Qt Template Library* spomínané knižnice šablón, je to, že *Qt* si občas „vynucuje" používanie vlastnej knižnice šablón.

8 Návrh

8.1 Návrh dialógu

Softvérový produkt umožní používateľovi zadať všetky potrebné parametre pomocou dialógu. Tento umožní používateľovi zadať počet úrovní ℓ, do ktorých budú používatelia rozdelení. Pre jednotlivé úrovne schémy môže používateľ zvoliť počty účastníkov $N_1, \ldots, N_\ell$, ako aj prahy $t_1, \ldots, t_\ell$.

Počty účastníkov sa zadávajú nie priamo pre úroveň i (nie n_i), ale počet účastníkov N_i úrovne nanajvýš i. Je to jednoduchšie a prehľadnejšie.

Napríklad ak používateľ zvolí $\ell = 2$, $t_1 = 3$, $N_1 = 5$, znamená to že na prvej úrovni je schéma $(3, 5)$-prahová. Ak používateľ ďalej zvolí $t_2 = 4, N_2 = 7$, znamená to, že ak množina účastníkov nebola prístupová na prvej úrovni môže byť prístupová na druhej, ak má aspoň 4 účastníkov z celkového počtu 7.

Podmienky, ktoré by mali jednotlivé počty účastníkov a prahy spĺňať sú

- $0 < t_i < t_{i+1}$,
- $t_i \leq N_i < N_{i+1}$,
- $t_{i+1} - t_i < N_{i+1} - N_i$.

Tieto podmienky sa overujú priebežne už počas zadávania. Ak softvérový produkt zistí, že parametre nespĺňajú niektorú z podmienok upozorní na to používateľa prostredníctvom chyby zobrazenej v stavovom riadku.

V dialógu sa ďalej zvolí prvočíslo p. Prvočíslo p je charakteristikou poľa Z_p, v ktorom budeme robiť všetky výpočty. Prvočíslo p musí byť vždy väčšie, ako je počet účastníkov schémy. Pri zmene čísla prebehne test, ktorý overí, či nami zadané číslo je naozaj prvočíslo. Ak nie je, upozorní na to používateľa pomocou hlášky v stavovom riadku.

Ďalšími parametrami, ktoré môžu ovplyvniť prístupovú štruktúru, sú $x_1, \ldots, x_{N_\ell}$. Tieto čísla majú byť nenulové a po dvoch rôzne. Ako sme v tejto práci dokázali, je to síce nutná, nie však postačujúca podmienka na to, aby funkčnosť schémy nezlyhala.

Počas overovania sa používateľovi zobrazí progressbar, na ktorom bude zobrazené koľko percent overovania sa už vykonalo. Počas overovania nie je možné meniť parametre schémy. Je však možné stlačiť tlačidlo, ktorý sa overovanie ukončí.

Ak sa počas overovania program zistí, že pre dané koeficienty by konštruovaná schéma nepracovala správne, oznámi to používateľovi pomocou dialógu. Používateľ

sa bude môcť rozhodnúť, či nechá overovanie ďalej bežať a zistí všetky množiny účastníkov, kde by schéma nepracovala správne, alebo overovanie ukončí.

Dialóg obsahuje tlačidlo, pomocou ktorého je možné prácu ukončiť.

9 Implementácia

9.1 Inštalácia knižníc

Pri vývoji softvérového produktu využívame knižnice *STL*, *Qt* a *GMP*. Knižnica *STL* zvyčajne býva súčasťou knižníc dodávaných ku kompilátoru jazyka C++, preto ju nie je potrebné inštalovať. Ak by predsa len nebola, môžeme ju stiahnuť z Internetu (www.sgi.com/stl).

Knižnica *Qt* zväčša býva súčasťou rôznych distribúcii Linuxu. Preto sa pri inštalácii môžeme rozhodnúť, že využijeme verziu knižnice, ktorá je súčasťou distribúcie. Ďalšou možnosťou je, že si stiahneme nejakú verziu knižnice z Internetu a potom ju prekompilujeme.

Výhodou stiahnutia z Internetu je to, že sa môžeme rozhodnúť, akú verziu knižnice použijeme. Najnovšia verzia zrejme nebude dostupná na platformy *Microsoft Windows* a *MacOS*.

Kompilácia knižnice pomerne dlho trvá, preto na nevýkonnom počítači radšej nepoužívajme poslednú dostupnú verziu pre náš operačný systém. Naša verzia by však nemala byť staršia ako 2.2.1, s ktorou som program odskúšal. Neručím za bezproblémové používanie nejakej staršej verzie.

Ak sa rozhodneme nainštalovať knižnicu z Internetu, môžme ju stiahnuť z adresy www.trolltech.com/qt, na ktorej nájdeme odkaz na súbor nazvaný napríklad qt-x11-free-3.1.2.tar.bz2. V názve súboru 3.1.2 znamená verziu.

9.1.1 Inštalácia knižnice Qt zo súboru *.tar.bz2

Súbor s príponou `.tar.bz2` je skomprimovaný. Uložíme ho do adresára, kam chceme knižnicu rozbaliť (napríklad /usr/local). Potom ho rozbalíme príkazom

```
tar xvfy qt-x11-free-3.1.2.tar.bz2
```

Ak sme stiahli súbor s príponou `.tar.gz`, rozbalíme ho príkazom

```
tar xvfz qt-x11-free-3.1.2.tar.gz
```

Rozbalením vznikne adresár `/usr/local/qt-x11-free-3.1.2` a my naň vytvoríme symbolickú linku príkazom

```
ln -s qt-3.1.2 qt
```

Potom knižnicu nakonfigurujeme tak, že domovskom adresári knižnice spustíme skript

```
./configure
```

Vhodnými parametrami môžeme určiť adresáre, kam sa má uložiť skompilovaná knižnica (parameter `-libdir /usr/local/lib`). Adresár, v ktorom sú uložené spustiteľné súbory, môžeme špecifikovať parametrom `-bindir /usr/local/bin`. Adresár, v ktorom sú uložené hlavičkové súbory, môžeme určiť pomocou parametra `-headerdir /usr/local/include/qt`.

Inštaláciu spustíme príkazom

```
make install
```

Počas inštalácie sa kompilujú zdrojové súbory a vznikajú súbory s príponami `.o` a `.lo`. Tieto sa nakoniec spoja do súboru, v ktorom bude uložená celá skompilovaná knižnica. Pre staticky linkované programy vznikne knižnica `libqt.a` a pre dynamicky linkované `libqt.so`.

Kompilácia je pomerne zdĺhavá. Na staršom počítači, aký používam, by trvala niekoľko dní. Preto som sa rozhodol pre inštaláciu zo súboru *.rpm.

9.1.2 Inštalácia knižnice Qt zo súboru *.rpm

Tento spôsob nemusí fungovať v každej distribúcii Linuxu. Pre distribúciu *Mandrake* a *Red-Hat* je však typický. Ak ste pri inštalácii Linuxu zvolili plnú inštaláciu, knižnica *Qt* je už určite súčasťou vášho systému. Môžeme ju prípadne aj inštalovať aj dodatočne pomocou nasledovného postupu:

1. Na inštalačnom médiu nájdime adresár `RMPS`, v ktorom bude súbor, ktorého meno začína na `qt`. Na inštalačnom CD, ktoré používam, je adresár `Mandrake\RPMS`. V ňom sa nachádzajú súbory `qt-1.44-28mdk.i586.rpm` a `qt2-2.2.1-3mdk.i586.rpm`. Ide o verziu knižnice 1.44 a 2.2.1.
2. Nainštalujeme si verziu 2.1.1 príkazom `rpm -i qt2-2.2.1-3mdk.i586.rpm`

Nevýhodou tohto spôsobu inštalácie je, že distribúcie zvyčajne neobsahujú statickú knižnicu `libqt.a`.

9.1.3 Inštalácia knižnice GMP

Knižnica *GMP* na rozdiel od knižnice *Qt* nebýva súčasťou distribúcie Linuxu. Ak ju chceme nainštalovať, najprv musíme z Internetu (www.swox.com/gmp) stiahnuť súbor, v ktorom sa knižnica nachádza. Na mojom počítači používam verziu knižnice 4.1.2. Táto je uložená v súbore `gmp-4.1.2.tar.gz`.

Knižnicu rozbalíme príkazom

```
tar xvfz gmp-4.1.2.tar.gz
```

Potom sa rozhodneme, pre aký druh počítača knižnicu zostavujeme. Ak chceme knižnicu používať len na svojom počítači, spustíme príkaz `./configure` bez parametrov. Vtedy knižnica sama zistí, na akom počítači beží a bude plne využívať možnosti, ktoré tento počítač poskytuje. Vtedy knižnica bude využívať všetky rozšírenia procesora o inštrukcie MMX, SSE a podobne, ktoré náš procesor umožňuje.

Ak náš program v binárnom tvare chceme prenášať na iné počítače, konfigurujeme knižnicu príkazom

```
./configure --build=i386-linux
```

Výhodou druhého postupu je možnosť vytvárať binárne programy, ktoré sa budú dať spustiť na akomkoľvek počítači typu „x86", na ktorom je Linux.

Po konfigurácii knižnicu nainštalujeme príkazom

```
make install
```

9.2 Nastavenie ciest

Pri práci s oboma knižnicami budeme potrebovať nasledujúce vhodne nastavené cesty v premenných prostredia. Nastavíme ich postupnosťou príkazov, ktoré uložíme do súboru `~/.bash_profile`. Ak používame iný shell, tak príkazy uložíme do súboru, ktorý tento shell spustí pri svojom štarte.

```
QTDIR=/usr/local/qt
PATH=$QTDIR/bin:$PATH
MANPATH=$QTDIR/doc/man:$MANPATH
LD_LIBRARY_PATH=$QTDIR/lib:$LD_LIBRARY_PATH
GMPDIR=/usr/local/gmp-4.1.2
```

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$GMPDIR/.libs
export QTDIR PATH MANPATH LD_LIBRARY_PATH GMPDIR
```

V prípade, ak používame `csh`, alebo `tcsh`, tak do súboru `.login` zapíšeme nasledujúcu postupnosť príkazov:

```
setenv QTDIR /usr/local/qt
setenv PATH $QTDIR/bin:$PATH
setenv MANPATH $QTDIR/doc/man:$MANPATH
setenv LD_LIBRARY_PATH $QTDIR/lib:$LD_LIBRARY_PATH
setenv GMPDIR /usr/local/gmp-4.1.2
setenv LD_LIBRARY_PATH $LD_LIBRARY_PATH:$GMPDIR/.libs
```

Nezabudnime, že nové nastavenie ciest sa prejaví až pri ďalšom spustení shellu.

9.3 Vytvorenie programu multilevel-scheme

Súbory, pomocou ktorých program vytvoríme, sú rozdelené do niekoľkých adresárov. Program sa nám podarí vytvoriť len v prípade, ak máme nainštalované knižnice *Qt* a *GMP* a nastavené premenné prostredia QTDIR, GMPDIR a LD_LIBRARY_PATH.

Program vytvoríme spustením príkazu

```
make
```

Ak chceme statické linkovanie knižníc, spustíme príkaz

```
make STATIC=true
```

Použitím statického linkovania sa program nevýznamne zrýchli, ale podstatne predĺži. Staticky linkovaný program je prenositeľný na iné počítače aj v binárnej podobe (samozrejme, ak knižnica *GMP* bola nakonfigurovaná tak, aby to tento počítač zvládol).

Vytvorený program spustíme pomocou príkazu

```
./multilevel-scheme
```

Časť IV

Výsledky a ich zhodnotenie

Diplomová práca dáva prehľad viacerých schém na zdieľanie tajomstva popísaných v literatúre. Väčší priestor venuje kumulatívnej schéme umožňujúcej odhalenie podvádzajúceho účastníka (popísaná v článku [3]) a najmä multiúrovňovej schéme na zdieľanie tajomstva (popísaná v článkoch [4] a [5]).

Spomínané články popisujú prácu schém, ale je v nich niekoľko nepresností. V článku [3], ktorý sa zaoberá kumulatívnymi schémami, nebol vysvetlený algoritmus, pomocou ktorého podvádzajúci útočník vytvorí falošný podiel tak, aby pravdepodobnosť odhalenia bola minimálna. Ukázali sme, že ak útočníkom bude jeden z účastníkov, môže tento útočník nepodstatne zmenšiť pravdepodobnosť svojho odhalenia. V tomto článku nebola vysvetlená voľba parametra α. V práci sme voľbu objasnili.

Články [4] a [5], ktoré sa zaoberajú multiúrovňovými schémami, obsahujú tiež niekoľko nepresností. Prístupová štruktúra schémy nie je opísaná úplne jasne. V článku nie je uvedený ani algoritmus práce kombinátora.

Články predpokladajú, že pri voľbe stačí, aby verejné parametre $x_1, \ldots, x_n$ boli nenulové a po dvoch rôzne. Naša práca ukázala, že pre nevhodne zvolené parametre schéma nemusí pracovať správne.

Môže sa nastať situácie, kedy podľa opísanej prístupovej štruktúry by mala množina účastníkov byť prístupová, ale v skutočnosti nedokáže získať žiadnu informáciu o kľúči.

Neprístupovej množine účastníkov sa zas môže stať, že množina dokáže vyjadriť kľúč len na základe svojich podielov.

Ukázali sme že to, či schéma správne pracuje záleží len od verejne známych parametrov $x_1, \ldots, x_n$ a od počtu účastníkov $n_1, \ldots, n_\ell$ a prahov $t_1, \ldots, t_\ell$ na jednotlivých úrovniach (a samozrejme poľa, v ktorom počítame). Voľba utajených parametrov $a_{1,1}, \ldots, a_{\ell,T_\ell}$ prístupovú štruktúru neovplyvní.

Znamená to, že ak raz overíme koeficienty $x_1, \ldots, x_n$ môžeme na nich ľahko založiť ďalšie schémy, ktoré majú rovnakú prístupovú štruktúru (rovnaké počty účastníkov na jednotlivých úrovniach a rovnaké prahy).

Ukázali sme, akým spôsobom je možné pre koeficienty $x_1, \ldots, x_n$ overiť, či prístupová štruktúra bude požadovaná, alebo nie. Nevýhodu tohto algoritmu je, že musí

prechádzať cez všetky (potenciálne) minimálne prístupové množiny účastníkov a pre každú z nich zvlášť posúdiť, či táto množina dokáže zrekonštruovať kľúč.

Overenie bezpečnosti je teda mimoriadne časovo náročné a prakticky sa dá realizovať len pre menšie množiny účastníkov.

Súčasťou diplomovej práce je softvérový produkt, pomocou ktorého je možné overiť, či koeficienty $x_1, \ldots, x_n$ sú zvolené vhodne, alebo nie.

Použitá literatúra

[1] van Dijk, M., Jackson, W.A., Martin, K.M.: A General Decomposition Construction for Incomplete Secret Sharing. In:*Design, Codes and Cryptography*, 1998. Vol. 15, pp. 301–321.

[2] Desment, Y., King, B., Kishimoto, W., Kurosawa, K.: A Comment on the Efficiency of Secret Sharing Schemes over Any Finite Abelian Group. In: *Lecture Notes in Computer Sience*, 1998. Vol. 1438, pp. 391.

[3] Ghodosi, H., Pieprzyk, J., Safavi-Naini, R., Wang., H.: On Construction of Cumulative Secret Sharing Schemes. *Lecture Notes in Computer Science*, 1998, Vol. 1438, pp. 379–390.

[4] Ghodosi, H., Pieprzyk, J., Safavi-Naini, R.: Secret Sharing in Multilevel and Compartmeted Groups. *Proceedings of ACISP '98 (Australasian Conference on Information Security and Privacy)*, pp. 367-378. Springer Verlang, 1998.

[5] Ghodosi, H., Pieprzyk, J., Safavi-Naini, R.: Remarks on the Multiple Assignment Secret Sharing Scheme. *Proc. 1st International Information and Communications Security Conference, 1997. Pages 72–80.*

[6] Grošek, O., Porubský, Š.: *Šifrovanie – Algoritmy, metódy, prax.* Grada, 1992.

[7] Pieprzyk, Josef: *Cryptology*, 2001, preprint.

[8] Riečanová, Z. a kolektív: *Numerické metódy a matematická štatistika.* Alfa, vydavateľstvo technickej a ekonomickej literatúry spolu s SNTL – Nakladatelství technické literatury, 1987.

[9] Bieliková, Mária: *Ako úspešne vyriešiť projekt.* Vydavateľstvo STU, Bratislava, 2000. 158 strán. ISBN 80-227-1329-5.

[10] Bieliková, Mária: *Softvérové inžinierstvo*: Princípy a manažment. Vydavateľstvo STU, Bratislava, 2000. 220 strán. ISBN 80-227-1322-8.

[11] Ding, C., Pei, D., Salomaa.,A.: *Chinese Remainder Theorem – Applications in Computing, Coding, Cryptography.* Singapore: World Scientific Publishing, 1996. 213 pages. ISBN 981-02-2827-9.

[12] Matejdes, Milan: *Lineárna algebra.* Zvolen: MATCENTRUM, 1998. 276 strán. ISBN 08–968057-0-3.

[13] Gralund, Torbjörn: *GNU MP – The GNU Multiple Precision Arithmetic Library.* Edition 4.1.2, 20.12.2002. (17.1.2003). ftp://ftp.gnu.org/gnu/gmp.