Metode podjele tajni

Novaković, Sanja

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:904957

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij - Financijska matematika i statistika

Sanja Novaković

Metode podjele tajni

Diplomski rad

Osijek, 2019.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij - Financijska matematika i statistika

Sanja Novaković

Metode podjele tajni

Diplomski rad

Voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2019.

Sadržaj

1 Uvod **1**

2 Podjela tajni **3**
2.1 Trivijalna podjela tajne 4

3 Shamirova metoda podjele tajni **5**
3.1 Primjena Shamirove sheme 5
3.2 Shamirova metoda i interpolacijski polinomi 6
3.2.1 Svojstva Shamirove (t, w) granične sheme 10
3.2.2 Lagrangeov interpolacijski polinom 10
3.2.3 Pojednostavljena (t, t) shema praga 13
3.3 Primjeri 14

4 Blakleyeva metoda podjele tajni **16**

5 Pristupne strukture i opća podjela tajni **19**
5.1 Monotona konstrukcija sklopa 20

6 Zaključak **26**

7 Literatura **27**

Popis slika **28**

Sažetak **29**

Životopis **30**

1 Uvod

Metoda podjele tajni je jedan od najvažnijih mehanizama u kriptografiji jer omogućava sigurnu komunikaciju između dvije ili više strana. Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija grčkog je podrijetla i mogla bi se doslovno prevesti kao *tajnopis*. Osnovni je zadatak kriptografije omogućiti dvjema osobama komuniciranje preko nesigurnog komunikacijskog kanala na način da treća osoba, koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke.

Prema hrvatskom jezičnom portalu tajna je ono što se nikomu ne smije reći, ono što mora ostati skriveno, što se taji, skriva, ne priča, ne objavljuje. Postoji više vrsta tajni: državna tajna, poslovna tajna, službena tajna, vojna tajna, osobna tajna.... Tajna je činjenica poznata užem krugu osoba, za koju postoji opravdan opći ili individualni interes da se znanje o njoj ne proširi.

Razvojem interneta, bankarstva, elektronske pošte i drugih suvremenih načina komuniciranja svakim danom osobne informacije su sve izloženije napadima. Jedan je od načina čuvanja podataka kopirati podatke na više mjesta, ali je samim time povećana izloženost napadima neželjenih osoba. Možemo smanjiti izloženost tako da podatke podijelimo na više dijelova te svaki dio čuvamo na različitim mjestima. U tom slučaju napadač može otkriti samo dio podataka. Sigurnost informacija vrlo je bitna, pogotovo kada je riječ o bankovnom računu. Cilj je dijeliti informacije, ali na siguran način, a upravo se time bavi ovaj rad.

Poznata američka tvrtka prehrambene industrije i svjetski lanac restorana brze hrane "McDonald's" koristi metodu podjele tajne. Njihov trezor čuvaju dva ključa od kojih se jedan nalazi kod zaštitarske firme pa nije moguće otvoriti trezor bez prisustva iste.

Slika 1.1: Sigurnost poslovnice u Osijeku

Mnoge poznate korporacije na sličan način čuvaju tajni recept. Jedan je od najpoznatijih primjera čuvanja tajne recept za "Coca Colu". Tajnu formulu, odnosno tajni sastojak kodnog imena "Merchandise 7X", poznaje samo par ljudi na svijetu. Tajni recept, star 127 godina, čuva se u sefu jedne banke u Atlanti. Osobe koje znaju tajnu formulu potpisale su ugovor o čuvanju tajnosti podataka, a kako se radi o svega nekoliko osoba, navodno uopće ne smiju putovati zajedno u slučaju, primjerice, nesreće.

Slika 1.2: Trezor u kojem se čuva recept

2 Podjela tajni

Tajno dijeljenje izumili su neovisno Adi Shamir i George Blakley 1979. godine. Tradicionalne metode nisu bile prikladne za postizanje visoke razine povjerljivosti i pouzdanosti. Za pohranu šifrirnog ključa bilo je potrebno izabrati između čuvanja jedne kopije ključa na jednom mjestu za maksimalnu tajnost i čuvanja više kopija ključa na različitim mjestima radi veće pouzdanosti. Povećanje pouzdanosti ključa pohranjivanjem više kopija smanjuje povjerljivost stvaranjem veće mogućnosti da kopija padne u krive ruke.
Sheme podjele tajni rješavaju ovaj problem i omogućavaju postizanje proizvoljno visoke razine povjerljivosti i pouzdanosti.

Shema podjele tajni metoda je distribucije tajne među grupama sudionika, od kojih je svakom dodijeljen dio tajne. Da bi podijelili tajnu, mora postojati osoba koja će ju podijeliti, a ta se osoba naziva djelitelj tajne. U nastavku rada označavat ćemo ga s D. Tajnu S podijelit će na w dijelova, tako da svakom sudioniku dodijeli dio tajne koji nazivamo dionica, pri čemu niti jedan sudionik ne zna koju je dionicu dobio drugi sudionik. Tajna se može rekonstruirati samo kada se dionice spoje u cjelinu, jer niti jedna dionica sama za sebe ne otkriva ništa o tajni.

Sheme podjele tajni idealne su za pohranjivanje vrlo osjetljivih i važnih informacija.

Sigurna tajna shema dijeljenja raspodjeljuje dionice tako da svatko tko ima manje od t dionica ima jednako podataka o tajni kao i onaj koji nema niti jednu dionicu. Pogledajmo primjer koji nam pokazuje nesigurno dijeljenje tajne.

Primjer 2.1. *Naša je tajna "matematika", koju ćemo podijeliti na* 5 *dionica.*

$$"ma - te - ma - ti - ka"$$

Osoba koja nema niti jednu dionicu zna samo da se riječ sastoji od 10 *slova. Trebala bi odabrati riječ iz* 30^{10} *kombinacija, dok osoba koja ima jednu dionicu treba pogoditi još* 8 *slova pa samim time i manje kombinacija, točnije* 30^8.

Iz ovog kratkog primjera vidimo da shema nije sigurna, jer osoba s više dionica ima više saznanja o tajni nego osoba koja nema niti jednu dionicu. Pogledajmo primjer koji prikazuje sigurnu shemu dijeljenja.

Primjer 2.2. *Tajna koju želimo podijeliti je* X. P_i *su javni ključevi, a* Q_i *njihovi odgovarajući privatni ključevi.*
Svakom sudioniku J *na raspolaganju je* $P_1(P_2(\cdots(P_N(X))))), Q_j$.

U ovoj shemi svaki sudionik s privatnim ključem 1 *može ukloniti vanjski sloj šifriranja dok sudionik s ključevima* 1 *i* 2 *može ukloniti prvi i drugi sloj. Svaki sudionik s manje od* N *ključeva nikada ne može u potpunosti doći do tajne bez potrebe da prethodno dešifrira sloj šifriran javnim ključem za koji, pak, nema odgovarajući privatni ključ. Svaki korisnik sa svim* N *privatnim ključevima može dešifrirati sve vanjske slojeve kako bi dobio* X, *tj. tajnu, pa je prema tome to sigurna shema dijeljenja.*

2.1 Trivijalna podjela tajne

U (t, w) shemi praga:

- $t = 1$ U ovom je slučaju podjela tajne trivijalna. Tajna se može podijeliti svim sudionicima, jer je potreban samo jedan sudionik da bi ju rekonstruirao.
- $t = w$ Postoji više shema podjele tajni za $t = w$. To je slučaj kada su sve dionice potrebne da bi se rekonstruirala tajna.
- $1 < t < w$ Neka je dan proizvoljan pravi podskup skupa sudionika. Radi se o iznimno korisnoj shemi, jer ne zahtijeva sve sudionike pri rekonstruiranju tajne. Želimo da šef u nekom poduzeću u svakom trenutku može pristupiti tajnom receptu, ali isto tako, želimo da u slučaju šefove odsutnosti radnici mogu nesmetano raditi. Napravimo shemu praga $(5, 15)$, tj. šefu dodijelimo 5 dionica tajne, a radnicima preostalih 10. U svakom trenutku će 5 radnika zajedno biti u mogućnosti otvoriti recept.

3 Shamirova metoda podjele tajni

Shamirova metoda podjela tajni koristi se za zaštitu tajne na distribuirani način, najčešće za osiguranje drugih ključeva za šifriranje. Tajnu dijelimo na više dijelova koji se nazivaju dionicama. Te se dionice koriste za obnovu izvorne tajne. Da biste otključali tajnu pomoću Shamirove podjele tajni, potreban vam je minimalni broj dionica. To se naziva pragom i koristi se za označavanje minimalnog broja dionica potrebnih za otključavanje tajne.

Definicija 3.1. *Neka su t, w prirodni brojevi, $t \leq w$. Shema praga (threshold scheme) (t, w) metoda je podjele tajne S među w sudionika (označenih s $\mathcal{P}$). Potpuna tajna S može se rekonstruirati iz bilo koje kombinacije t komadića tajne. Poznavanjem manjeg broja komadića tajna se ne može rekonstruirati.*

Ako je $t = w$ tada je za rekonstruiranje tajne potreban svaki dio izvorne tajne.

3.1 Primjena Shamirove sheme

Prema časopisu "Time" kontrola nuklearnog oružja u Rusiji početkom devedesetih godina ovisila je o sličnom mehanizmu pristupa "dva od tri". Prema uputama američkih zračnih snaga koncept "dvije osobe" dizajniran je za postizanje većeg stupnja sigurnosti kako ne bi došlo do zlonamjernog i neovlaštenog lansiranja nuklearnog oružja od strane pojedinca. U slučaju lansiranja rakete "Minuteman", nakon primitka naloga za lansiranje, oba se sudionika moraju složiti da je nalog valjan. Valjanost naloga utvrdit će uspoređujući autorizacijski kod iz naloga sa zapečaćenim autentifikatorom (posebna koverta koja sadrži kod). Autentifikatori se nalaze u posebnom sefu koji ima dvije odvojene brave. Svaki operater ima ključ jedne brave pa niti jedan operater ne može sam otvoriti sef. Nakon provjere autentifikacije, potrebno je ključeve umetnuti u utore na upravljačkoj ploči, kako bi se dodatno povećala sigurnost utori su udaljeni dovoljno daleko jedan od drugoga kako jedna osoba ne bi mogla istovremeno okrenuti oba ključa. Za lansiranje nuklearne rakete potrebna je suradnja najmanje dviju strana od tri. Tri su uključene strane predsjednik, ministar obrane i ministarstvo obrane.
Pravilo "dva čovjeka" primjenjivalo se u raketnim silosima i podmornicama.

Sličan pristup koriste banke kako bi osigurale velike svote novca, tj. za otključavanje trezora. U banci se nalazi trezor koji se svakodnevno otvara. Tamo su zaposleni direktor i tri službenika, koji ne vjeruju jedan drugome. Želimo osmisliti sustav u kojemu bilo koja dva od triju službenika, kada su zajedno, mogu otvoriti trezor ili direktor sam to može učiniti, ali niti jedan od službenika ne može sam. Direktor banke može generirati dionice za šifru trezora u banci i dati po jednu dionicu svakom zaposleniku. Čak i kada direktor nije dostupan, trezor se može otvoriti uz prisustvo dovoljnog broja zaposlenika koji su u mogućnosti otključati ga zajedno. Ovaj problem možemo riješiti pomoću Shamirove metode podjele tajni što je i temom ovog poglavlja.

3.2 Shamirova metoda i interpolacijski polinomi

Proučava se bezuvjetna sigurnost, tj. ne postavljaju se nikakvi uvjeti na količinu izračuna koji neki podskup sudionika može obaviti. Djelitelj tajne označen je s D , pretpostavimo da $D \notin \mathcal{P}$, on bira šifru koju želi podijeliti. Kada D želi podijeliti šifru, on svakom sudioniku dodijeli dionicu (djelomičnu informaciju).

Koristimo sljedeće oznake

$$\mathcal{P} = \{P_i : 1 \leq i \leq w\},$$

gdje je w skup sudionika.

Definicija 3.2. *Neka je $\mathbb{F}$ neprazan skup na kojemu su zadane binarne operacije zbrajanja $+: \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ i množenja $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$. Kažemo da je uređena trojka $(\mathbb{F}, +, \cdot)$* ***polje*** *ako vrijede sljedeća svojstva:*

- $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\forall \alpha, \beta, \gamma \in \mathbb{F}$;
- $\exists 0 \in \mathbb{F}$ *sa svojstvom* $\alpha + 0 = 0 + \alpha = \alpha, \forall \alpha \in \mathbb{F}$;
- $\forall \alpha \in \mathbb{F}$ *postoji* $-\alpha \in \mathbb{F}$ *tako da je* $\alpha + (-\alpha) = -\alpha + \alpha = 0$;
- $\alpha + \beta = \beta + \alpha, \forall \alpha, \beta \in \mathbb{F}$;
- $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma, \forall \alpha, \beta, \gamma \in \mathbb{F}$;
- $\exists 1 \in \mathbb{F} \setminus \{0\}$ *sa svojstvom* $1 \cdot \alpha = \alpha \cdot 1 = \alpha, \forall \alpha \in \mathbb{F}$;
- $\forall \alpha \in \mathbb{F} \setminus \{0\}$ *postoji* $\alpha^{-1} \in \mathbb{F}$ *tako da je* $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$;
- $\alpha \cdot \beta = \beta \cdot \alpha, \forall \alpha, \beta \in \mathbb{F}$;
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma, \forall \alpha, \beta, \gamma \in \mathbb{F}$.

Konačna polja su polja s konačno mnogo elemenata, npr. $\mathbb{Z}_p := \{0, 1, \ldots, p-1\}$, sa zbrajanjem i množenjem po modulu p, gdje je p prost broj. Prvo se računa zbroj ili umnožak na uobičajen način, a onda njegov ostatak pri dijeljenju s p.

Primjer 3.3. *Pogledajmo kako se računa u danim poljima:*

$$\mathbb{Z}_2 : 1 + 1 = 0, 2 + 1 = 1\, tj. - 1 = 1$$

$$\mathbb{Z}_5 : 2 + 4 = 1, 5 \cdot 2 = 0.$$

Konstrukcija Shamirove (t, w) ***sheme praga***

- Djelitelj D izabire w različitih elemenata iz $\mathbb{Z}_p$, označavaju se s x_i za $1 \leq i \leq w$ (ovdje je potreban zahtjev da je $p \geq w+1$).

  Za $i \in 1, \ldots, w$, djelitelj D vrijednosti x_i pridruži svakom P_i.

  Raspodjela udjela

- Djelitelj D želi podijeliti ključ K, $K \in \mathbb{Z}_p$. Tajno odabire $t-1$ element, koji označavamo s $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$.
- $\forall i \in 1, \ldots, w$, D računa $y_i = a(x_i)$, gdje je

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \pmod{p}.$$

- Za $i \in 1, \ldots, w$, djelitelj D članu P_i pridruži izračunati y_i.

Kasnije će podskupina sudionika $B \subseteq \mathcal{P}$ udružiti svoje dionice kako bi došli do traženog ključa.

Ako je $|B| \geq t$ sudionici će moći izračunati ključ, ali ako je $|B| < t$ to neće moći.

U ovoj shemi djelitelj D konstruira slučajni polinom $a(x)$ koji je najvišeg stupnja $t-1$, gdje je konstantni član traženi ključ K.

Svaki član P_i zna par (x_i, y_i) pri čemu polinom u točki x_i poprima vrijednost y_i. Pogledajmo kako podskup B od t sudionika može rekonstruirati ključ polinomijalnom interpolacijom.

Pretpostavimo da sudionici P_i žele odrediti ključ K.

Znamo da je $y_i = a(x_i), \forall j \in 1, \ldots, t$, gdje je $a(x) \in \mathbb{Z}_p$ tajni polinom djelitelja.

Polinom $a(x)$ najvišeg je stupnja $t-1$, a može se zapisati u obliku

$$a(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1},$$

koeficijenti $a_0, a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$ nepoznati su, $a(0) = K$.

Članovi podskupa B tvore sustav t linearnih jednadžbi s t nepoznanica $a_0, \ldots, a_{t-1}$.

Ako su jednadžbe linearno nezavisne postojat će jedinstveno rješenje te će a_0 biti traženi ključ K.

Pogledajmo sustav linearnih jednadžbi:

$$\begin{aligned} a_0 + a_1x_1 + a_2x_1^2 + \cdots + a_{t-1}x_1^{t-1} &= y_1 \\ a_0 + a_1x_2 + a_2x_2^2 + \cdots + a_{t-1}x_2^{t-1} &= y_2 \\ &\vdots \\ a_0 + a_1x_t + a_2x_t^2 + \cdots + a_{t-1}x_t^{t-1} &= y_t. \end{aligned}$$

Matrični zapis sustava jest:

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{t-1} \end{bmatrix}$$

Matrica koeficijenata označava se s $V(x_1, x_2, \ldots, x_t)$ i naziva se Vandermondeova matrica.

Definicija 3.4. *Determinanta matrice*

$$V(x_1, x_2, \ldots, x_t) = \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{vmatrix}$$

zove se Vandermondeova determinanta.

Pokažimo da je determinanta Vandermondeove matrice jednaka

$$\prod_{1 \le j < i \le t} (x_i - x_j).$$

Svaki stupac množi se s $-x_1$ i dodaje se sljedećem stupcu kako bi se poništio prvi redak, tj. dobili na prvom mjestu 1 i sve ostalo 0. Pogledajmo kako izgleda determinanta nakon prve iteracije.

$$\begin{vmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{t-2}(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) & \cdots & x_3^{t-2}(x_3 - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_t - x_1 & x_t(x_t - x_1) & \cdots & x_t^{t-2}(x_t - x_1) \end{vmatrix}$$

Zatim, svaki se stupac množi s $-x_2$ i dodaje sljedećem stupcu kako bi se poništio prvi redak. Pogledajmo još kako izgleda determinanta nakon ovog postupka.

$$(x_2 - x_1)\begin{vmatrix} (x_3 - x_1)(x_3 - x_2) & \cdots & (x_3 - x_1)x_3^{t-4}(x_3 - x_2) \\ (x_4 - x_1)(x_4 - x_2) & \cdots & (x_4 - x_1)x_4^{t-4}(x_4 - x_2) \\ \vdots & \ddots & \vdots \\ (x_{t-1} - x_1)(x_{t-1} - x_2) & \cdots & (x_{t-1} - x_1)x_{t-1}^{t-4}(x_{t-1} - x_2) \\ (x_t - x_1)(x_t - x_2) & \cdots & (x_t - x_1)x_t^{t-4}(x_t - x_2) \end{vmatrix}$$

Nastavi li se isti postupak, doći će se do željenog rezultata.

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

Prisjetimo se da su svi x_i $i \in \{1, \ldots, n\}$ međusobno različiti pa niti jedan izraz $x_i - x_j$ nije 0.

Kako je p prost broj, $\mathbb{Z}_p$ je polje, a produkt ne-nul elemenata u polju opet je ne-nul element, time se dolazi do zaključka $det(A) \neq 0$.

Samim time sustav ima jedinstveno rješenje u $\mathbb{Z}_p$.

Ovaj rezultat pokazuje da bilo koji podskup od t sudionika može doći do traženog ključa K.

Primjer 3.5. *Neka je $p = 17$, $t = 3$, $w = 5$ i neka su koordinate x_i , $1 \leq i \leq 5$ poznate. Pretpostavimo da članovi podskupa $B = \{P_1, P_3, P_5\}$ žele doći do ključa K, gdje su pripadni y_i redom $8, 10$ i 11 za $i = 1, 3, 5$.*
Polinom se zapisuje kao

$$a(x) = a_0 + a_1 x + a_2 x^2$$

i izračunava $a(1)$, $a(3)$, $a(5)$ u konačnom polju $\mathbb{Z}_{17}$. Rezultat jest sustav od tri jednadžbe s tri nepoznanice:

$$a_0 + a_1 + a_2 = 8 \pmod{17}$$
$$a_0 + 3a_1 + 9a_2 = 10 \pmod{17}$$
$$a_0 + 5a_1 + 8a_2 = 11 \pmod{17}.$$

Rješavanjem sustava dobiveno je jedinstveno rješenje u $\mathbb{Z}_{17}$:

$$a_0 = 13, a_1 = 10, a_2 = 2.$$

Dolazi se do ključa $K = a(0) = 13$.

Pogledajmo zatim može li skupina od $t-1$ sudionika doći do ključa K. Iz odgovarajućeg sustava linearnih jednadžbi dobit će se sustav od $t-1$ jednadžbe s t nepoznanica. Pretpostavimo da je ključ $K = a_0 = a(0)$ te se sustavu dodaje i ta jednadžba. Sada imamo sustav od t jednadžbi s t nepoznanica, time dobivamo Vandermondeovu matricu, samim time i jedinstveno rješenje. Za svaku vrijednost y_0 dobije se jedinstveni polinom $a_{y_0}(x)$ takav da je

$$y_i = a_{y_0}(x_i), \forall i \in \{1, \ldots, t-1\}$$

$$y_0 = a_{y_0}(0).$$

Dolazimo do zaključka da tajna ne može biti narušena grupom sudionika $t-1$, ukoliko im ona nije već unaprijed poznata, a istima nisu dostupne nikakve informacije o tajni.

3.2.1 Svojstva Shamirove (t, w) granične sheme

- **Informacijsko-teorijska sigurnost.** Skup kriptografskih algoritama potrebnih za implementaciju određene sigurnosne usluge. Njegova sigurnost proizlazi isključivo iz teorije informacija koja proučava kvantifikaciju, pohranu i komunikaciju informacija. Sustav se ne može slomiti čak i ako protivnik ima neograničenu računalnu moć.
- **Minimalnost.** Veličina svakog pojedinog dijela ne prelazi veličinu izvornih podataka.
- **Proširivost.** Uz fiksan t komadići se P_i mogu dodavati ili brisati bez utjecaja na druge komadiće.
- **Dinamičnost.** Sigurnost se može poboljšavati bez promjene tajne, povremenim mijenjanjem polinoma (uz zadržavanje istog slobodnog člana) i novom podjelom dionica među sudionicima.
- **Fleksibilnost.** U organizacijama gdje je važna hijerarhija, pojedinim sudionicima može se dati različit broj dionica prema njihovoj važnosti u organizaciji. Npr. guverner može sam otvoriti trezor, dok su za otvaranje istog trezora potrebna 4 viceguvernera.

3.2.2 Lagrangeov interpolacijski polinom

Popularna tehnika za provedbu shema pragova koristi Lagrangeovu interpolaciju.

Teorem 3.6 (Lagrangeova interpolacijska formula)**.** *Neka je p prost broj, $x_1, x_2, \ldots, x_{m+1}$ različiti elementi iz $\mathbb{Z}_p$ i $a_1, a_2, \ldots, a_{m+1}$ (ne nužno različiti) elementi iz $\mathbb{Z}_p$.*

Tada postoji jedinstveni polinom $A(x) \in \mathbb{Z}_p[x]$ koji ima stupanj najviše m, za koji vrijedi

$$A(x_i) = a_i, 1 \leq i \leq m+1.$$

Polinom $A(x)$ je dan s:

$$A(x) = \sum_{j=1}^{m+1} a_j \prod_{1 \leq h \leq m+1, h \neq j} \frac{x - x_h}{x_j - x_h}.$$

Prethodni teorem daje rezultat da je polinom $a(x)$ stupnja najviše $t-1$ jedinstven i daje eksplicitnu formulu koja se može koristiti za izračunavanje $a(x)$.

Formula za $a(x)$ je sljedeća:

$$a(x) = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \pmod{p}.$$

Podskupina B od t sudionika može izračunati $a(x)$ koristeći interpolacijsku formulu. Sudionici podskupine B ne trebaju znati cijeli polinom $a(x)$, dovoljno je doći do slobodnog člana $K = a(0)$. Stoga može se izračunati sljedeći izraz, koji se dobiva zamjenom $x = 0$ u Lagrangeovoj interpolacijskoj formuli:

$$K = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \right) \pmod{p}.$$

Definirajmo

$$b_j = \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \pmod{p}, 1 \le j \le t,$$

b_j se može izračunati, a njihove vrijednosti nisu tajne. Tada imamo:

$$K = \sum_{j=1}^{t} b_j y_{i_j} \pmod{p}.$$

Naposljetku, ključ je linearna kombinacija $\pmod{p}$ od t dijeljenja. Sada će se ponovno pokušati izračunati ključ iz primjera 3.5.

Primjer 3.7. *Prisjetimo se par detalja iz primjera 3.5.* $P = 17, t = 3, w = 5$ *i poznate su koordinate* x_i, $1 \le i \le 5$. *Članovi podskupa* $B = \{P_1, P_3, P_5\}$ *žele doći do ključa* K, *gdje su pripadni* y_i *redom* $8, 10$ *i* 11 *za* $i = 1, 3, 5$.

Sudionici $\{P_1, P_3, P_5\}$ *mogu izračunati* b_1, b_2 *i* b_3 *uvrštavajući iste u prethodnu formulu. Na primjer, za j=1 oni dobiju:*

$$\begin{aligned} b_1 &= \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} \pmod{17} \\ &= 3 \cdot 5 \cdot 2^{-1} \cdot 4^{-1} \pmod{17} \\ &= 4. \end{aligned}$$

Slično je za $j = 2, j = 3$, $b_2 = 3$ *i* $b_3 = 11$. *Kada se sve uvrsti u formulu za* K *dobije se sljedeće:*

$$K = 4 \cdot 8 + 3 \cdot 10 + 11 \cdot 11 \pmod{17} = 13,$$

dobiven je isti ključ kao i ranije.

Zanima nas što bi se dogodilo da podskup B od $t-1$-og sudionika pokuša izračunati ključ K?

Pretpostavimo da oni misle da je $y_0 \in \mathbb{Z}_p$ za ključ K. U Shamirovoj shemi praga znamo da je ključ $K = a_0 = a(0)$. Prisjetimo se da $t-1$ dionica dobiva izračunavanjem polinoma $a(x)$ s $t-1$ elemenata iz $\mathbb{Z}_p$. Sada će se primjeniti teorem 3.6 gdje je jedinstveni polinom $a_{y_0}(x)$ prikazan kao

$$y_{i_j} = a_{y_0}(x_{i_j}),\ 1 \leq j \leq t-1,$$

iz toga slijedi

$$y_0 = a_{y_0}(0).$$

Pogledajmo skicu pojednostavljene (t,t) sheme pragova o kojoj ćemo nešto više reći u sljedećem poglavlju.

Skica pojednostavljene (t,t) shema praga

- D tajno izabire $t-1$ elemenata $y_1, \ldots, y_{t-1}$ iz polja $\mathbb{Z}_m$.
- Zatim izračunava
$$y_t = K - \sum_{i=1}^{t-1} y_i \pmod{m}.$$
- Za $1 \leq i \leq t$, D daje udio y_i u P_i.

Postoji polinom $a_{y_0}(x)$ koji je u skladu s poznatim dionicama $t-1$ od B čiji je ključ y_0. Budući da to vrijedi za svaku vrijednost $y_0 \in \mathbb{Z}_p$, slijedi da se niti jedna vrijednost ključa ne može isključiti, a samim time skupina od $t-1$ sudionika ne posjeduje nikakve informacije o ključu.

Vratit ćemo se na naš primjer. Pretpostavimo da sudionici P_1 i P_3 žele izračunati K. Sudionici P_1, P_3 s pripadnim $y_1 = 8$ i $y_3 = 10$, za svaku moguću vrijednost y_0 ključa postoji jedinstven polinom $a_{y_0}(x)$ koja postiže vrijednost 8 za $x = 1$ i vrijednost 10 za $x = 3$. Koristeći interpolacijsku formulu dobivamo:

$$a_{y_0}(x) = 6y_0(x-1)(x-3) + 13x(x-3) + 13x(x-1) \pmod{17}.$$

Sudionici $\{P_1, P_3\}$ ne mogu znati koji je ispravni polinom pa nemaju nikakvu informaciju o ključu.

3.2.3 Pojednostavljena (t, t) shema praga

U ovom odjeljku će se detaljnije proći kroz pojednostavljenu graničnu shemu s posebnim slučajem $w = t$.

Oznake:

$\mathcal{K}$-(skup svih mogućih pozitivnih ključeva) $\mathcal{K} = \mathbb{Z}_m$
$\mathcal{S}$-(skup svih mogućih dionica) $\mathcal{S} = \mathbb{Z}_m$,

m ne mora biti prost broj i ne treba uvjet $m \geq w + 1$.

Kada D želi podijeliti ključ $K \in \mathbb{Z}_m$ on provodi korake iz prethodno navedene skice pojednostavljene sheme. Uočimo da t sudionika može izračunati K prema formuli

$$K = \sum_{i=1}^{t} y_i \pmod{m}.$$

Zanima nas mogu li $t - 1$ sudionika izračunati K? Jasno je da prvih $t - 1$ sudionika ne mogu to učiniti, zato što će kao dionice dobiti $t - 1$ neovisne slučajne brojeve. Promotrimo $t - 1$ sudionika u skupu $P \setminus \{P_i\}$, $1 \leq i \leq t - 1$. Sudionici posjeduju dionice

$$y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_{t-1}$$

i

$$y_t = K - \sum_{i=1}^{t-1} y_i \pmod{m}.$$

Zbrajanjem dijelova iz B dobije se $K - y_i, i \in \{1, \ldots, t - 1$, ali se ne zna vrijednost y_t, stoga nemaju ni podatke o K. Pogledajmo na primjeru kako se koristi shema (t, t).

Primjer 3.8. *Uzmimo da je* $p = 14, t = 6$ *te su njima dodijeljene dionice* $y_1 = 2$, $y_2 = 5$, $y_3 = 3$, $y_4 = 7$, $y_5 = 9$, $y_6 = 6$. *Ključ* K *je*

$$K = 2 + 5 + 3 + 7 + 9 + 6 \pmod{14} = 4.$$

Pretpostavimo da prvih 5 *sudionika želi izračunati* K. *Oni znaju da je*

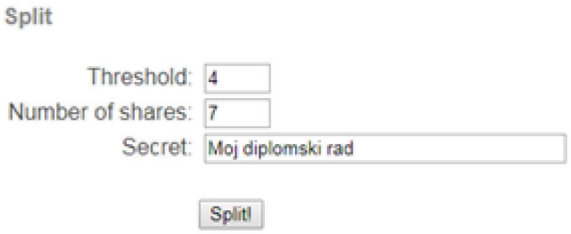
$$y_1 + y_2 + y_3 + y_4 + y_5 \pmod{14} = 12$$

ali ne znaju vrijednost y_6. *Postoji korespodencija jedan na jedan između* 14 *mogućih vrijednosti od* y_6 *i* 14 *mogućih vrijednosti ključa* K*:*

$$y_6 = 0 \Leftrightarrow K = 12, y_6 = 1 \Leftrightarrow K = 13, y_6 = 2 \Leftrightarrow K = 0, \ldots, y_6 = 13 \Leftrightarrow K = 11.$$

3.3 Primjeri

Primjer 3.9. *Neka je tajna "Moj diplomski rad" podijelit ćemo ju pomoću Shamirove sheme* $(4, 7)$*, tj. na* 7 *dijelova od kojih bilo koja* 4 *zajedno daju tajnu. Na sljedećim slikama prikazana je prvo podjela, a zatim otkrivanje tajne pomoću online programa* `http://point-at-infinity.org/ssss/demo.html`*.*



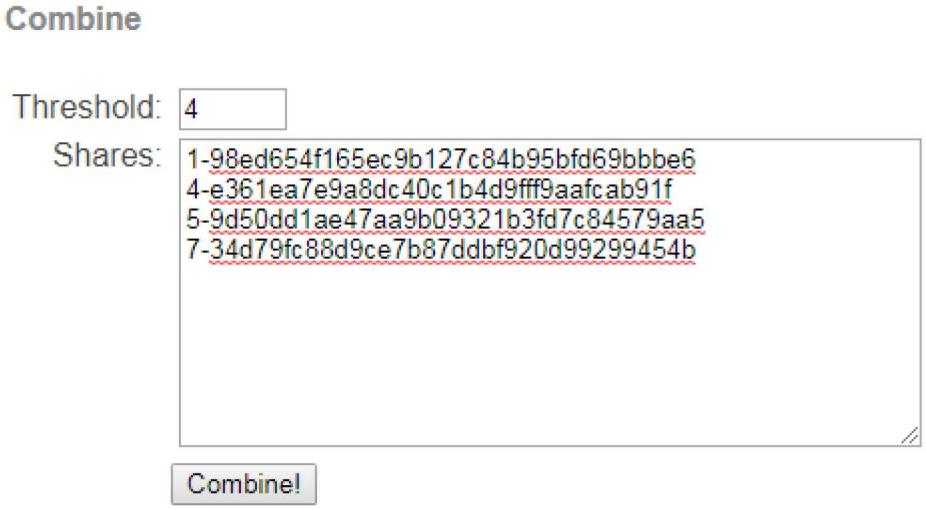
Slika 3.1: Parametri

Na prethodnoj slici prikazana nam je tajna i ulazni parametri prema kojima se radi podjela, zatim ćemo na sljedećoj slici vidjeti rezultate podjele.

```
1-98ed654f165ec9b127c84b95bfd69bbbe6
2-0f81355265d8149b6df1f7bf61c9a94611
3-64838a39e096689ac36fe856a2f001a9a7
4-e361ea7e9a8dc40c1b4d9fff9aafcab91f
5-9d50dd1ae47aa9b09321b3fd7c84579aa5
6-205b9d18608e57e094fc6801e8bf0eff4a
7-34d79fc88d9ce7b87ddbf920d99299454b
```

Slika 3.2: Podjele šifre

Uzima se bilo koja 4 *koda od* 7 *navedenih i kopiraju se u novi prozor koji kombinira, tj. sastavlja šifru od danih kodova.*



Slika 3.3: Odabrani kodovi

Pogledajmo je li dobivena zadana početna tajna.

```
Moj diplomski rad
```

Slika 3.4: Dobivena tajna

Dobivena tajna jednaka je početnoj tajni.

4 Blakleyeva metoda podjele tajni

Blakleyeva shema podjele tajni koristi geometriju hiperravnine za rješavanje problema podjele.

Definicija 4.1. *Kod n-dimenzionalnog prostora "hiperravnina" $n-1$ dimenzionalni je objekt koji se koristi za podjelu tog prostora na dva poluprostora. U jednodimenzionalnom prostoru to je točka i dijeli pravac na dva polupravca, u dvodimenzionalnom prostoru "hiperravnina" je pravac i dijeli ravninu na dvije poluravnine, dok je u trodimenzionalnom prostoru to ravnina i dijeli prostor na dva poluprostora.*

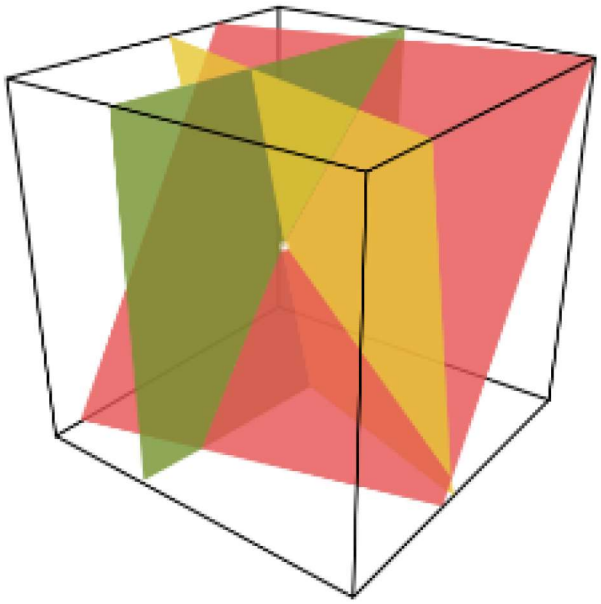
Dva neparalelna pravca u istoj ravnini sijeku se u jednoj točki. Tri neparalelne ravnine u prostoru sijeku se u jednoj točki. Općenito, bilo kojih n neparalelnih $n-1$ dimenzionalnih hiperravnina sijeku se u određenoj točki.

Tajna je dodatno sigurna ako je šifrirana kao pojedinačna koordinata točke sjecišta. Ako se tajna šifrira pomoću svih koordinata, tada sudionik koji posjeduje jednu ili više hiperravnina $n-1$ dobije informacije o tajni, jer zna da mora ležati u njegovoj ravnini. Koristeći samo jednu od n koordinata, sudionik ne posjeduje više informacija od nekoga tko nema niti jednu dionicu, tj. ne zna da tajna mora ležati na osi x za dvodimenzionalni sustav. Tajna se rekonstruira izračunavanjem točke sjecišta ravnine i uzimanjem određene koordinate tog sjecišta.

Tajna se zadaje kao prva koordinata točke sjecišta u t dimenzionalnom prostoru, a dionice su pravci u ravninama koje prolaze kroz tu točku.

Blakleyeva je shema podjele tajni (t, n) shema praga kao i Shamirova, ali Blakleyeva shema je manje prostorno učinkovita od Shamirove. Shamirove dionice velike su samo koliko je velika izvorna tajna, dok su Blakleyeve tri puta veće. Blakleyeva shema može se dodatno osigurati dodavanjem ograničenja na ravnine koje se mogu koristiti kao dionice. Rezultirajuća shema ekvivalentna je Shamirovom polinomnom sustavu.

Pogledajmo grafički Blakleyevu $(3, n)$ shemu praga.



Slika 4.1: (3,n) shema

Skica Blakley-eve sheme

- p prost broj, $\mathbb{Z}_p$ polje na kojem radimo, x_0 tajna
- djelitelj D odabere $y_0, z_0 \pmod{p}$ te dobivenu točku označi s $Q = (x_0, y_0, z_0)$
- i-ti sudionik dobije jednadžbu $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{it}x_t = y_i$
- djelitelj svakom sudioniku dodjeljuje jednadžbu ravnine koja prolazi kroz točku Q na način da nasumično odabere brojeve $a, b \, mod \, p$ i definira $c \equiv z_0 - ax_0 - by_0 \pmod{p}$
- tada dobivamo jednadžbu ravnine

$$z = ax + by + c$$

- članovi kombiniranjem dobivenih jednadžbi žele otkriti tajnu te dobivaju sustav od tri linearne jednadžbe:

$$a_i x + b_i y - z \equiv -c_i \, mod \, p, \; 1 \leq i \leq 3$$

- matrični zapis sustava jest:

$$\begin{bmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = \begin{bmatrix} -c_1 \\ -c_2 \\ -c_3 \end{bmatrix}$$

- sustav ima rješenje dok je determinanta matrice $\pmod{p}$ različita od nula.

Primjer 4.2. *Neka je* $p = 41$. *Članovima* $S_i, i \in \{1, 2, 3, 4, 5\}$ *dane su sljedeće jednadžbe:*

$$\begin{aligned} z &= 14x + 38y + 40 \\ z &= 2x + 19y + 28 \\ z &= 13x + 26y + 8 \\ z &= 29x + 32y + 36 \\ z &= 37x + 25y + 35. \end{aligned}$$

Ukoliko članovi S_1, S_3, S_5 *žele rekonstruirati tajnu* x_0 *moraju riješiti sustav:*

$$\begin{bmatrix} 14 & 38 & -1 \\ 13 & 26 & -1 \\ 37 & 25 & -1 \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = \begin{bmatrix} -40 \\ -8 \\ -35 \end{bmatrix}.$$

Rješenje sustava jest $(x_0, y_0, z_0) = (27, 19, 33)$ *pa je tražena tajna* $x_0 = 27$. *Analogno, bilo koja tri člana od* S_1, S_2, S_3, S_4, S_5 *mogu rekonstruirati tajnu.*

5 Pristupne strukture i opća podjela tajni

U prethodnim poglavljima tražilo se da bilo kojih t od w sudionika mogu otkriti ključ. Općenita situacija točno je odrediti koja podskupina sudionika može odrediti ključ, a koja ne. Neka je Γ skup podskupova od $\mathcal{P}$, podskupovi od Γ su oni podskupovi sudionika koji bi trebali biti u stanju izračunati ključ. Γ se naziva shema podjele pristupnih struktura. Pristupna struktura i svaki podskup u Γ zove se autorizirana tajna podskupa sheme podjele.

Neka je $\mathcal{K}$ skup ključeva i neka je $\mathcal{S}$ skup mogućih dionica. Kao i ranije, kad djelitelj želi podijeliti ključ $K \in \mathcal{K}$, dat će svakom sudioniku dionicu iz skupa $\mathcal{S}$. Zatim će podskup sudionika pokušati odrediti K iz dionica koje zajedno posjeduju.

Definicija 5.1. *Savršena shema podjele tajni koja realizira pristupnu strukturu Γ metoda je dijeljenja ključa K među skupovima od w sudionika na način da su zadovoljena sljedeća dva svojstva:*

1. *Ako ovlašteni podskup sudionika $B \subseteq \mathcal{P}$ objedini svoje dionice, tada mogu odrediti vrijednost K.*
2. *Ako neovlašteni podskup sudionika $B \subseteq \mathcal{P}$ objedini svoje dionice, tada oni ne mogu utvrditi ništa o vrijednosti K.*

Pretpostavimo da je $B \in \Gamma$ i $B \subseteq C \subseteq \mathcal{P}$, te da podskup C želi odrediti K. Budući da je B ovlašteni podskup, on već može odrediti K. Dakle, podskup C može odrediti K zanemarujući udjele sudionika u $C \backslash B$. Nadskup ovlaštenog skupa ponovno je ovlašteni skup. Prethodni rezultat govori da bi pristupna struktura trebala zadovoljiti monotono vlasništvo:

$$\text{ako je } B \in \Gamma \text{ i } B \subseteq C \subseteq \mathcal{P} \text{ tada je } C \in \Gamma.$$

U nastavku ovog poglavlja pretpostavimo da su sve pristupne strukture monotone. Primijetimo se da shema pragova (t, w) realizira pristupnu strukturu

$$\{B \subseteq \mathcal{P} : |B| \geq t\}.$$

Takva pristupna struktura naziva se granična pristupna struktura.

Ako je Γ pristupna struktura i ako za A takav da je $A \subseteq B$, $A \neq B$, vrijedi $A \notin \Gamma$, tada je $B \in \Gamma$ minimalni ovlašteni podskup . Skup minimalno ovlaštenih podskupova od Γ označen je s Γ_0 i naziva se osnovom od Γ. Budući da se Γ sastoji od svih podskupova od $\mathcal{P}$ koji su nadskupovi podskupine s bazom Γ_0, slijedi da je Γ jedinstveno određen kao funkcija od Γ_0.

Pogledajmo matematički zapis:

$$\Gamma = \{C \subseteq \mathcal{P} : B \subseteq C, B \in \Gamma_0\}.$$

Primjer 5.2. *Ukoliko je* $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ *i*

$$\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\},$$

tada je

$$\Gamma = \Gamma_0 \cup \{\{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}.$$

Obzirom na ovu strukturu pristupa Γ *lako je vidjeti da se* Γ_0 *sastoji od minimalnih podskupova u* Γ*.*

U slučaju (t, w) pristupne strukture praga, osnova se sastoji od svih podskupova od t sudionika.

5.1 Monotona konstrukcija sklopa

U ovom se dijelu daje konceptualno jednostavna, no ujedno i elegantna konstrukcija Benaloha i Leichtera koja pokazuje da svaka (monotona) struktura pristupa može biti realizirana savršenom shemom podjele tajne. Ideja je prvo izgraditi monoton sklop koji "prepoznaje" pristupnu strukturu, a zatim izgraditi shemu podjele tajne. To nazivamo *monotona izradnja sklopa.*

Pretpostavimo se da imamo Booleov sklop $\boldsymbol{C}$, s w Booleovih ulaznih podataka, $x_1, \ldots, x_w$ (što odgovara sudionicima $P_1, \ldots, P_w$) i jednim Booleovim izlaznim podatkom y. Sklop se sastoji od dva smjera (prolaza) "*ili*" i "*i*" te se naziva monotoni Booleov sklop. Promjenom bilo kojeg ulaznog podatka x_i iz "0" (laž) u "1" (istina) ne može se promijeniti izlazni podatak y iz "1" u "0". To je posljedica ovakvog označavanja. Prolazi mogu imati proizvoljno mnogo ulaznih podataka, ali samo jedan izlazni.

Ako se odrede Booleove vrijednosti za w ulaznih podataka takvog sklopa, može se definirati

$$B(x_1, \ldots, x_w) = \{P_i : x_i = 1\},$$

podskup od $\mathcal{P}$ odgovara ulaznim podatcima s vrijednosti "1". Može se pretpostaviti da je $\boldsymbol{C}$ monotoni sklop te definirati:

$$\Gamma(\boldsymbol{C}) = \{B(x_1, \ldots, x_w) : \boldsymbol{C}(x_1, \ldots, x_w) = 1\},$$

gdje se s $\boldsymbol{C}(x_1, \ldots, x_w)$ označava vrijednost od $\boldsymbol{C}$ za dane podatke $x_1, \ldots, x_w$.

Iz monotonosti sklopa $\boldsymbol{C}$, slijedi da je $\Gamma(\boldsymbol{C})$ monotoni skup od $\mathcal{P}$. Lako je vidjeti da postoji bijektivna veza između monotonih sklopova te Booleova formula koja sadrži operatore kao $\wedge$ ("i") i $\vee$ ("ili"), ali ne sadrži niti jednu negaciju.

Ako je Γ monotoni skup od $\mathcal{P}$, tada se može jednostavno konstruirati monoton sklop $\boldsymbol{C}$ takav da je $\Gamma(\boldsymbol{C}) = \Gamma$. Može se to učiniti na sljedeći način :

- neka je Γ_0 početna točka od Γ
- zatim se konstruira disjunktni oblik Booleove formule:

$$\bigvee_{B \in \Gamma_0} \left(\bigwedge_{P_i \in B} P_i \right).$$

Prisjetimo se primjera 5.2, gdje je

$$\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\},$$

dobili bismo logičku formulu

$$(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3).$$

Svaka rečenica u logičkoj formuli odgovara smjeru "i" povezanog monotonog sklopa te konačna disjunkcija odgovara smjeru "ili".
Pogledajmo algoritam koji konstruira monotoni sklop.

```
1  f(W_out) ← K;
2  while postoji žica W takva da f(W) nije definirana do
3  |  naći prolaz G iz C takav da je f(W_G) definirana, gdje je W_G izlazna žica od G,
   |   ali f(W) nije definirana za svaku vrijednost ulaznih žica od G;
4  |  if G je "ili" smjer then
5  |  |  f(W) ← f(W_G) za svaku vrijednost ulazne žice W od G;
6  |  else
7  |  |  neka ulazne žice od G budu W_1, ..., W_t;
8  |  |  izaberite (nasumično) t − 1 elemenata iz Z_m, označite ih s y_{G,1}, ..., y_{G,t−1};
9  |  |  y_{G,t} ← f(w_G) − Σ_{I=1}^{t−1} y_{G,i} mod m;
10 |  |  for i ← 1 to t do
11 |  |  |  f(W_i) ← y_{G,i};
12 |  |  end
13 |  end
14 end
```

Ukupan broj prolaza u sklopu jest $|\Gamma_0| + 1$. Ovaj sklop ima dvije "razine", ali to nije uvjet. Pretpostavimo da je $\boldsymbol{C}$ bilo koji monotoni sklop koji prepoznaje Γ (treba imati na umu da $\boldsymbol{C}$ ne mora biti identičan kao u prethodno navedenom algoritmu.) Opisujemo algoritam koji djelitelju omogućava konstruiranje savršene sheme za podjelu tajne koja realizira Γ.

Takva shema se koristi kao osnova za izgradnju (t, t) sheme konstruirane u pojednostavljenoj (t, t) shemi. Stoga se može uzeti da će skup ključeva biti $\mathcal{K} = \mathbb{Z}_m$, za neki prirodan broj m.
Algoritam se nastavlja pridruživanjem vrijednosti $f(W) \in \mathcal{K}$ svakoj žici W u sklopu $\boldsymbol{C}$.
U početku se izlaznoj žici W_{out} sklopa dodjeljuje vrijednost ključa K. Algoritam se ponavlja više puta, radeći od dna sklopa do vrha, sve dok se svakoj žici ne dodijeli vrijednost. Konačno, svakom sudioniku P_i dan je popis vrijednosti $f(W)$ tako da je W ulazna žica sklopa

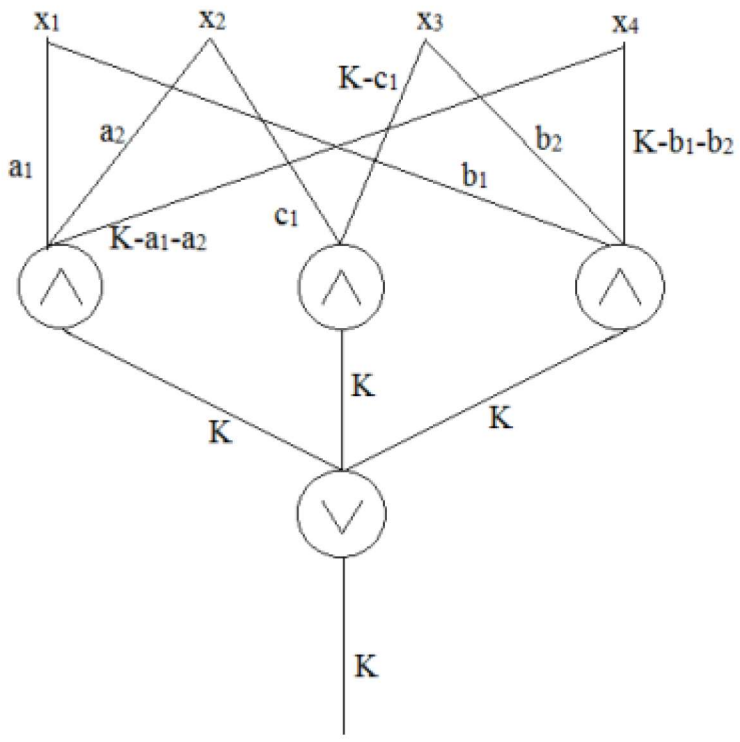
koja prima ulazni podatak x_i. Konstrukcija monotonog sklopa detaljno je opisana u prethodnom algoritmu.

Svaki puta kada su vrata G na vrijednosti izraza "i" prolaz (vrata) ima t ulaznih žica, dijeli se "ključ" $f(W_G)$ za vrata G među njegovim ulaznim žicama, koristeći (t, t) graničnu shemu.
Izvedimo ovaj postupak za pristupne strukture iz primjera 5.2, koristeći sklop koji odgovara logičkoj formuli:

$$(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3)\,.$$

Primjer 5.3. *Neka je K ključ. Vrijednost ključ dodjeljuje se svakoj od ulaznih žica koje se nalaze na kraju smjera "ili". Smatra se da smjer "i" odgovara izrazu $P_1 \wedge P_2 \wedge P_4$. Tri ulazne žice pridružuju vrijednosti $a_1, a_2, K - a_1 - a_2$, gdje se sve računske operacije rade u polju $\mathbb{Z}_m$. Na sličan se način nastavlja dalje. Postoje tri ulazne žice koje odgovaraju izrazu $P_1 \wedge P_3 \wedge P_4$ te dodjeljuju vrijednosti $b_l, b_2, K - b_1 - b_2$. Zatim postoje dvije ulazne žice koje odgovaraju izrazu $P_2 \wedge P_3$ te dodjeljuju vrijednosti $c_l, K - c_1$. Vrijednosti a_1, a_2, b_1, b_2 i c_1 neovisne su slučajne vrijednosti u $\mathbb{Z}_m$.*

Na sljedećoj slici vidi se grafički prikazan dani monotoni sklop.



Slika 5.1: Monotoni sklop

Ako pogledamo dionice koje dobivaju sudionici, imamo sljedeće:

1. P_1 *dobije* $(y_1^1, y_1^2) = (a_1, b_1)$
2. P_2 *dobije* $(y_2^1, y_2^2) = (a_2, c_1)$
3. P_3 *dobije* $(y_3^1, y_3^2) = (b_2, K - c_1)$
4. P_4 *dobije* $(y_4^1, y_4^2) = (K - a_1 - a_2, K - b_1 - b_2)$,

gdje je y^i *i-ta koordinata točke. Svaki sudionik dobiva dva elementa iz* $\mathbb{Z}_m$ *kao svoju dionicu.*

Dokažimo da je ovakva shema savršena. Prvo se provjerava da svaki osnovni podskup može izračunati ključ K*. Ovlašteni podskup* $\{P_1, P_2, P_4\}$ *može izračunati*

$$K = y_1^1 + y_2^1 + y_4^1 \pmod m = a_1 + a_2 + (K - a_1 - a_2) \pmod m.$$

Podskup $\{P_1, P_3, P_4\}$ *može izračunati*

$$K = y_1^2 + y_3^1 + y_4^2 \pmod m = b_1 + b_2 + (K - b_1 - b_2) \pmod m.$$

I na kraju podskup $\{P_2, P_3\}$ *može izračunati*

$$K = y_2^2 + y_3^2 \pmod m = c_1 + (K - c_1) \pmod m.$$

Slijedi da svaki ovlašteni podskup može izračunati K*. Pogledajmo što se događa s neovlaštenim podskupovima, pri čemu ne treba gledati sve neovlaštene podskupove. Ako su* B_1 *i* B_2 *neovlašteni podskupovi,* $B_1 \subseteq B_2$*, i* B_2 *ne može izračunati* K *tada ni* B_1 *ne može izračunati* K*.*

Definiramo podskup $B \subseteq \mathcal{P}$ *kao maksimalni neovlašteni podskup ako je* $B_1 \in \Gamma$*,* $\forall B_1 \supseteq B, B_1 \neq B$*. Pokazat će se da niti jedan od maksimalnih neovlaštenih podskupova ne može odrediti* K*.*

Ovo su maksimalni neovlašteni podskupovi

$$\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}.$$

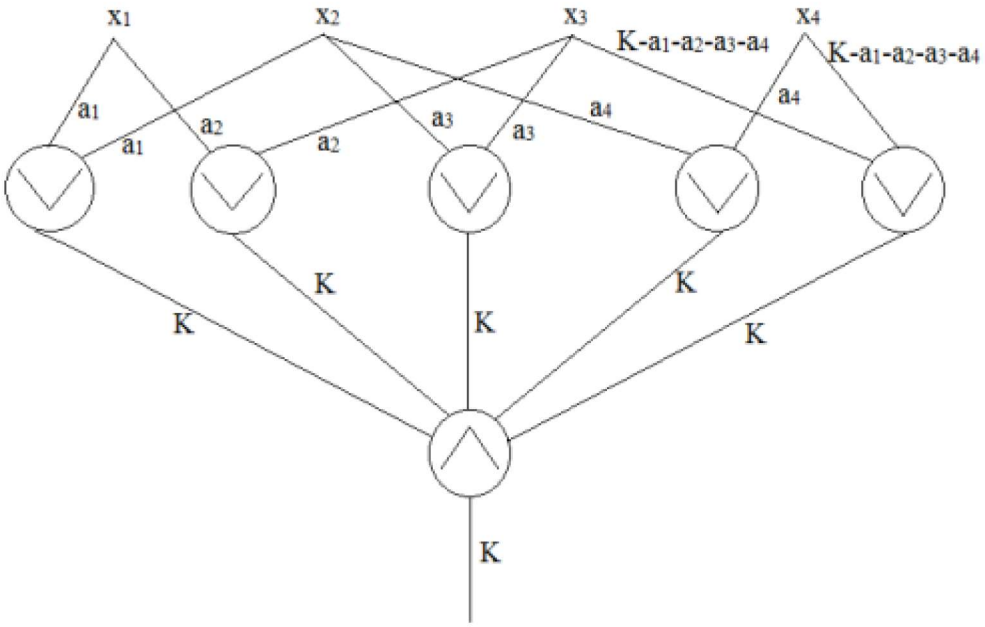
U svakom slučaju lako se vidi da se K *ne može izračunati, bilo zbog nekih nedostajućih dijelova ili zato što su sve dionice koje posjeduje podskupina nasumične. Na primjer, podskup* $\{P_1, P_2\}$ *posjeduje samo nasumične vrijednosti* a_1, b_1, a_2, c_1*. Kao još jedan primjer uzmimo da podskup* $\{P_3, P_4\}$ *posjeduje vrijednosti* $b_2, K - c_l, K - a_1 - a_2, K - b_1 - b_2$*. Budući da su nam vrijednosti* c_1, a_1, a_2 *i* b_1 *nepoznate,* K *se ne može izračunati.*

Realizirajući istu strukturu pristupa može se dobiti različita shema pomoću drugačijeg sklopa. Ilustrirajmo to vraćanjem na pristupnu strukturu sustava iz primjera 5.2.

Primjer 5.4. *Pogledajmo formulu ekvivalentnu onoj s kojom se radilo u navedenom primjeru:*

$$(P_1 \vee P_2) \wedge (P_1 \vee P_3) \wedge (P_2 \vee P_3) \wedge (P_2 \vee P_4) \wedge (P_3 \vee P_4)\,.$$

Zatim implementirajmo shemu koristeći sklop koji odgovara prethodnoj formuli.



Slika 5.2: Monotoni sklop

Ako se pogledaju dionice koje dobivaju sudionici, vidljivo je da:

1. P_1 *dobije* $(y_1^1, y_1^2) = (a_1, a_2)$
2. P_2 *dobije* $(y_2^1, y_2^2, y_2^3) = (a_1, a_3, a_4)$
3. P_3 *dobije* $(y_3^1, y_3^2, y_3^3) = (a_2, a_3, K - a_1 - a_2 - a_3 - a_4)$
4. P_4 *dobije* $(y_4^1, y_4^2) = (a_4, K - a_1 - a_2 - a_3 - a_4)\,.$

Pomoću sljedećeg teorema dokazat će se da monotona konstrukcija sklopa uvijek daje savršenu shemu podjele tajni.

Teorem 5.5. *Neka je* $\boldsymbol{C}$ *bilo koji monotoni Booleov sklop. Tada monotona izgradnja sklopa daje savršenu shemu podjele tajne koja realizira strukturu pristupa* $\Gamma(\boldsymbol{C})$.

Valja primjetiti da kada ovlašteni podskup B želi izračunati ključ, sudionici u B moraju znati sklop koji djelitelj koristi za distribuciju dionica i koje dionice odgovaraju kojoj žici sklopa. Sve ove informacije bit će poznate, samo su stvarne vrijednosti dionica tajne.

Algoritam za rekonstrukciju ključa uključuje kombiniranje dionica prema strukturi sklopa uz određene zahtjeve. Prvi je da smjer "i" odgovara zbrajanju vrijednosti modulo m ulaznih žica (pod uvjetom da su te vrijednosti svima poznate), a smjer "ili" uključuje odabir vrijednosti na bilo kojoj ulaznoj žici (očekuje se da će sve ove vrijednosti biti identične).

Treba se vratiti na primjer 5.3 i ponovno promotriti ovlašteni podskup $\{P_1, P_2, P_4\}$. Pokazano je kako ovaj podskup može izračunati K. Sklop omogućuje rekonstrukciju ključa na sistematski način. Dodijelili bismo vrijednosti šest od osam ulaznih žica i to onima koje proizlaze iz x_1, x_2 i x_4 na slici 5.1. To se vidi krajnje lijevo na slici gdje smjer "i" ima vrijednosti dodijeljene svim njegovim ulaznim žicama. Zbroj vrijednosti na tim žicama daje ključ K. Ovakav način računanja isti je kao što je opisano u primjeru 5.3.

6 Zaključak

Prilikom obrade rada može se, ponajprije, zaključiti kako su metode podjele tajni od presudne važnosti u informatički razvijenom svijetu današnjice. Osim uz razvoj informatičke tehnologije, podjela tajni usko je vezana i uz Internet, mrežu svih mreža, što rezultira mnogobrojnim primjenama iste u suvremenom svijetu. Nadalje, tajna shema podjele tajni višestruko je korisna. Prije svega, može osigurati tajnu na više poslužitelja i pri tome ostati povratna čak i unatoč višestrukim kvarovima poslužitelja. Na taj se način ključ može distribuirati na mnogim poslužiteljima pomoću mehanizma podjele pragova tajne. Ključ se zatim rekonstruira po potrebi.
Također, tajna je podjela iznimno korisna i za senzorske mreže u kojima se veze mogu prisluškivati slanjem podataka u dionicama što otežava zadatak prisluškivača. Sigurnost u takvim okruženjima može se povećati stalnim mijenjanjem načina na koji su dionice izgrađene.

Mogućnost kombiniranja dionica svojevrsna je prednost tajne podjele. Svaka se dionica može pohraniti na različitom poslužitelju, pri čemu je trgovac u mogućnosti oporaviti tajnu, čak i u slučaju kvara nekoliko poslužitelja, ukoliko može povratiti najmanje t dionica. Isto tako, osobe koje provale na jedan poslužitelj ne bi znale tajnu sve dok je na svakom poslužitelju pohranjeno manje od t dionica.

Dobre se lozinke teško pamte. Pametan korisnik mogao bi koristiti tajnu shemu podjele za generiranje skupa dionica za danu lozinku i pohraniti jednu dionicu u svoj adresar, drugu u svoj bankovni depozit, treću dionicu podijeliti s prijateljem i tome slično. Ako jednog dana zaboravi svoju lozinku, korisnik je može lako rekonstruirati. Naravno, pisanje lozinki izravno u adresar predstavljalo bi sigurnosni rizik od potencijalne krađe neprijatelja. No, ukoliko se koristi tajni program podjele, napadač mora ukrasti mnoge dionice iz različitih mjesta čime će njegove namjere automatski biti znatno otežane, odnosno onemogućene.

Djelitelj može poslati sve t dionice potrebne za oporavak izvorne tajne jednom primatelju koristeći t različitih kanala. U tom slučaju, napadač će morati presresti sve dionice kako bi vratio tajnu, a to je zadatak koji je puno teži nego presretanje jedne poruke.

7 Literatura

[1] N. Elezović, Linearna algebra, Element, Zagreb, 1995

[2] V. Pachatz, Implementation and Security Analysis of Secret Sharing Protocols, Magistarski rad, Alpen-Adria-Universität Klagenfurt, 2018

[3] A. Shamir, "How to share a secret", Massachusetts Institute of Technology, 1979

[4] D. R. Stinson: Cryptography Theory and practice (Third Edition), Chapman Hall, Boca Raton, 2006

[5] W. Trappe, L. C. Washington, Introduction to Cryptography with Coding Theory(Second Edition), Pearson Education International, Upper Saddle River, 2006

Popis slika

1.1 Sigurnost poslovnice u Osijeku 1
1.2 Trezor u kojem se čuva recept 2
3.1 Parametri 14
3.2 Podjele šifre 14
3.3 Odabrani kodovi 14
3.4 Dobivena tajna 15
4.1 (3,n) shema 17
5.1 Monotoni sklop 22
5.2 Monotoni sklop 24

Sažetak

U ovom radu vide se korisni rezultati iz područja kriptografije. Cilj je teme podjeliti tajnu među sudionicima na što sigurniji način. Obrađena je trivijalna podjela tajne, Shamirova metoda podjele tajne koja se pokazala savršenom, Blakleyeva metoda te opća podjela tajni. Uz odgovarajuće metode prikazani su primjeri te nekoliko načina na koji se koristi tajna podjela u suvremenom životu. Shema podjela tajnih podataka uključuje djelitelja koji ima tajnu, skup w sudionika te broj potrebnih sudionika za rekonstrukciju tajne (u (t, w) shemi praga to je t). Shema podjele tajne metoda je kojom djelitelj distribuira dionice sudionicima tako da bilo koji podskup od t sudionika može rekonstruirati tajnu iz objedinjenih dionica i bilo koji podskup koji ima manje od t dionica ne može otkriti nikakve djelomične podatke o tajni.

Ključne riječi

Tajna podjela, Shamirova tajna podjela, shema praga, Blakeova metoda, pristupne strukture, djelitelj

Abstract

This paper presents useful results in the field of cryptography. The aim of this topic is to share a secret among participants in the most secure way possible. A trivial division of the secret, the Shamir method of secret division which proved to be perfect, the Blakley method and the general division of secrets were all dealt with. Using appropriate methods examples have been provided along with several ways in which the secret division in modern life is used. The classification scheme includes a divisor that has a secret, a set of w participants, and the number of participants required to reconstruct the secret (in (t, w) the threshold scheme is t). The secret-sharing scheme is a method by which the divisor distributes shares to participants so that any subset of t participants can reconstruct the secret from the pooled shares and any subset of less than t shares cannot reveal any partial information about the secret.

Key words

Secret sharing, Shamir's Secret Sharing, threshold scheme, Blakley method, access structures, dealer

Životopis

Rođena sam 13. studenoga 1992.godine u Našicama. Pohađala sam osnovnu školu Kralja Tomislava te sam nakon toga upisala opću gimnaziju u Srednjoj školi Isidora Kršnjavoga u Našicama. 2011.godine upisujem preddiplomski studij matematike na Odjelu za matematiku Sveučilišta Josipa Jurja Strossmayera u Osijeku. Akademski naziv *prvostupnice matematike* stječem 2016.godine pod mentorstvom izv. prof. dr. sc. Ivana Matića i završni rad *Digitalni potpis*. Iste godine upisujem diplomski studij matematike, smjer Financijska matematika i statistika. Tijekom diplomskog studija, odradila sam stručnu praksu u Erste banci u Osijeku.