Dijeljenje tajni

Milutinović, Vedrana

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Vedrana Milutinović

DIJELJENJE TAJNI

Diplomski rad

Voditelj rada:
doc. dr. sc. Matija Kazalicki

Zagreb, rujan, 2016

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Tebi, vjernom Ocu i Prijatelju, bez kojeg ovaj put ne bi imao značenja! Mojoj baki Nadi i Tanjuški!

Sadržaj

Uvod

Definicija riječi tajna prema hrvatskom jezičnom portalu je ono što se nikome ne smije reći, ono što mora ostati skriveno, ono što se taji, skriva, što se ne priča, ne objavljuje. Stoga tajna je uvijek nešto oko čega nastojimo da ostaje skriveno, nepoznato i nedostupno široj javnosti, onima na kojima nije da o njoj pa bar i nešto znaju. I kao takva često ima i svoju materijaliziranu stranu, postaje opipljiva i vidljiva činjenica lako iskoristiva, kako onima kojima pripada tako i, onima koji bi stjecanjem iste oštetili vlasnika a sami se okoristili.

Današnje doba smatra se ponajviše informatičkim dobom. Dobom u kojem su od sredine prošlog stoljeća pa sve do današnjih dana razvoj tehnologije i interneta uzeo veliki mah i, isto tako, na velika vrata ušao u mnoge živote u mnogim njegovim segmentima od onih osobnih, društvenih, interesnih, poslovnih itd. Ono što čini objekt interneta, ukoliko korisnika smatramo subjektom, je podatak. U pozadini rada mreže i algoritama su ulazni podaci, koji kao takvi su tajne i nastoje biti zaštićeni i sačuvani od svih mogućih prijetnji. Danas nije potrebno napustiti obitavalište kako bismo platili račun u banci, izvršili transfer novca, izišli na izbore i sl. No u svemu tome bitno je zaštiti svaki podatak potreban pri inim radnjama jer to su napose osjetljivi i izrazito bitni. Podaci kao takvi su pohranjeni u bazama podataka, na serverima i izloženi učestaloj upotrebi a time i prijetnji.

Stoga se traže metode kako podatke što bolje zaštiti, kako povećati stupanj sigurnosti. Metode dijeljenja tajni su upravo jedan od načina zaštite podatka njegovim dijeljenjem. Pa ukoliko podatak nazovemo tajnom dolazimo do pojma dijeljenje tajni. U radu koji je pred nama bavit ću se opisom i primjenom metoda dijeljenja tajni, njihovim kvalificiranjem i svojstvima. U kriptografiji, taj pojam odnosi se na bilo koju metodu kojom se tajna (ključ, podatak) može podijeliti među grupom članova tako da svaki član posjeduje jedan dio te tajne odnosno podatka. Tajna se može otkriti samo kombiniranjem dijelova koje posjeduju članovi što zapravo znači da nijedan član ne može otkriti ni tajnu niti bilo kakvu informaciju o tajni koristeći samo svoj dio.

Da bi se tajna podijelila mora postojati netko da ju podijeli. U engleskoj literaturi djelitelja tajne se naziva *dealer* $\mathcal{D}$ čija je zadaća, na siguran način, podijeliti tajnu među n članova. Taj siguran način pretpostavlja u sebi pojam sheme praga, koji ću precizno definirati kasnije u radu. Neformalno, shema praga znači da bilo kojih t (eng. threshold) (ili više) članova mogu zajedno odrediti tajnu dok bilo koji broj članova manji od t ne

mogu odrediti tajnu na osnovu dijelova koje posjeduju. Struktura koja se zasniva na ovom principu naziva se (t, n)-shema praga.

Slijedno kroz poglavlja opisat ću klasifikaciju metoda dijeljenja tajne i uz osnovna svojstva svake metode, privatnost i mogućnost otkrivanja tajne, objasniti još dva svojstva, provjerljivost i proaktivnost. Zatim će slijediti poglavlja o samim metodama (shemama), najprije Shamirovom shemom dijeljenja tajni pa Blakleyevom. U svakom od poglavlja razmotrit ćemo konstrukciju sheme kao i navesti po jedan primjer. Dalje susrest ćemo s pojmom i metodom vizualne kriptografije. Razlika koja će se očitovati između vizualne kriptografije i ostalih metoda će biti u rekonstrukciji tajne ([6]). Naime vizualna kriptografija služi se čovjekovim vidom, što olakšava situacije u kojima nam računala nisu dostupna, dok ostale metode za rekonstrukciju koriste matematički račun, odnosno direktno proporcionalno kompleksnosti tajne algoritme i računala. Kao zadnju metodu objasnit ću onu koja se temelji na kineskom teoremu o ostacima i dvije metode implementirane zakonima brojeva dokazanih u kineskom teoremu o ostacima uz definiranje posebnih nizova brojeva.

Pojam (t, n)-shema praga su 1979. godine uveli američki kriptograf *George Blakley* i izraelski kriptograf *Adi Shamir* neovisno jedan od drugog. Oni se također smatraju i tvorcima ideje dijeljena tajni.

Poglavlje 1

Klasifikacija i svojstva metoda dijeljenja tajni

U ovom poglavlju napravit ćemo kratki pregled klasifikacije metoda i navesti i objasniti dva svojstva, *proaktivnost* ([3]) i *provjerljivost*.

1.1 Klasifikacija metoda dijeljenja tajni

Od vremena kada su Shamir i Blakley predstavili ideju i svoje metode dijeljenja tajni (eng. *secret sharing*) do danas nastalo je puno novih metoda dijeljenja tajni na osnovu nekih drugih matematičkih alata i zakonitosti što je rezultiralo da ih možemo na osnovu toga i kvalificirati. Sve te metode su se u kriptografiji pokazale idealnima za čuvanje informacija visoko osjetljive naravi i koje su izrazito bitne poput enkripcija ključeva, koda za lansirenje projektila ili bankovnih računa.

Shamir i Blakley uvode pojam (t, n)-*sheme praga* što definira metodu u kojoj djelilac podjeli tajnu na n članova. Stoga neki podskup $\mathcal{B}$ skupa svih članova može odrediti tajnu spajanjem svojih dijelova ako vrijedi $|\mathcal{B}| \geq t$ inače ako je $|\mathcal{B}| < t$ tada članovi ne mogu otkriti nikakvu informaciju o tajni. Shamirova metoda dijeljenja tajni, koja će biti obrađena kao zasebna cjelina u radu, zasniva se na Langrengeovom interpolacijskom polinomu dok Blakleyeva na geometriji hiperravnine, tj. da se u ravnini dva neparalelna pravca sijeku u točno jednoj točki ili puno općenitije da se u n dimenzionalnom prostoru bilo kojih n hiperravnina u općem položaju ima sjecište u točno jednoj točki.
Već kod dva osnovna algoritma dijeljenja tajni dolazimo do podjele istih. No prije nego objasnimo podjelu, objasnit ću značenje dostupne familije (eng. *access structure*) i uvesti oznaku za pojmove koji ću upotrebljavati i u daljnjem radu. Neka je $\mathcal{P} = \{P_i : 1 \leq i \leq n\}$ skup n članova te S skup dijelova tajne. Neka je Γ familija podskupova skupa $\mathcal{P}$ i neka elementi iz Γ imaju svojstvo da s njima možemo otkriti tajnu. Tada familiju Γ nazivamo

dostupnom familijom a njene elemente autoriziranim skupovima. Sada možemo napraviti prvu podjelu metoda dijeljenja tajni. Metode dijeljenja tajni se mogu podijeliti na savršene i nesavršene. Za metodu dijeljenja tajni kažemo da je savršena ako bilo koji podskup dostupne familije može otkriti tajnu dok bilo koju drugi neautorizirani podskup ne može otkriti ni jednu informaciju o tajni. Shamirova metoda je savršena dok Blakleyeva nije. Razlog zašto Blakleyeva shema nije savršena je zato što svaki sudionik zna da otkriće tajne leži u hiperravnini koja je jedinstveno određena njegovim dijelom.

Spomenuli smo i pojam $(t, n)-$sheme praga stoga metode dijeljenja tajni možemo kvalificirati i na osnovu toga koriste li $(t, n)-$sheme praga ili ne.

Također ne želimo uvijek podijeliti samo jednu tajnu nego više njih pa onda metode možemo kvalificirati i na osnovu toga dijele li samo jednu tajnu ili više.

U ovom radu ću osim Shamirove metode za koju smo već naveli da koristi Langrangeov interpolacijski polinom i Blekleyeve metode koja koristi zakone geometrije hiperravnine kao još jednu metodu obraditi i dijeljenje tajni koje se zasniva na kineskom teoremu o ostatcima.

Imamo tri metode i tri različite tehnike koje te metode koriste stoga zadnja podjela metoda je upravo na osnovu tehnika koje se koriste.

1.2 Svojstva metoda dijeljenja tajni

Sve metode dijeljenja tajni imaju dva osnovna svojstva:

1. *Privatnost*: otkrivanje tajne se mora zaštiti od neautoriziranog podskupa članova
2. *Mogućnost otkrivanja tajne*: tajna mora biti otkrivena pomoću pojedinačnih dijelova autoriziranog podskupa članova

Tajnu se uvijek nastoji što bolje očuvati od svih potencijalnih neprijatelja. Već u samoj ideji dijeljenja tajne(i) štiti se sigurnost i cjelovitost tajne. Neprijatelj je stoga prisiljen otkriti više dijelova tajni da bi ju otkrio ili uništio. U (t, n) – shemi praga potrebno je domoći se t dijelova da bi tajna bila otkrivena ili uništiti n-t-1 dio kako bi i samo otkriće bilo nemoguće. No vrijeme djelovanja, u smislu otkrivanja dijelova, neprijatelja jednako je vremenu života tajne. Postupno i konstantno otkrivanje svakog autoriziranog podskupa kroz duži vremenski period čini za neprijatelja uspjeh vrlo vjerojatnim.

Prirodno rješenje zaštite tajne bi bilo periodički stvarati novu tajnu ili ponovno stvoriti drugačije dijelove bez mijenjanja tajne. No u slučaju pojedinih tajni nije uvijek moguće stvoriti novu tajnu (npr. oporuke ili recept za Coca Colu). Stoga je puno lakše periodički stvarati nove dijelove u zamjenu za stare. Ono znači da se neprijatelju skraćuje vrijeme djelovanja i da ukoliko i otkrije neke dijelove tajne (s kojim je dalje nemoguće otkriti samu

tajnu) nakon stvaranja novih ovi postaju neupotrebljivi. Ovakvo svojstvo metode naziva se ***proaktivno*** svojstvo.

S druge strane, svaki pojedini član može biti potencijalni neprijatelj i može lagati o dijelu koji posjeduje kako bi se domogao ostalih dijelova. Stoga svojstvo metode kojom se može provjeriti jesu li u procesu dijeljenja tajne djelitelj i članovi bili pošteni naziva se ***provjerljivost***.

Poglavlje 2

Shamirova metoda dijeljenja tajni

U prvom poglavlju već smo spomenuli Shamirovu metodu i naveli da je *(t, n)–shema praga.*

Definicija 2.0.1. *Neka su t i n pozitivni cijeli brojevi td. $t \leq n$.* ***(t, n)–shema praga*** *je metoda dijeljenja (tajne) ključa $\mathcal{K}$ među skupom od n članova tako da svaki podskup od t članova može otkriti ključ $\mathcal{K}$ dok svaki podskup čiji je broj članova manji od t ne može otkriti ključ $\mathcal{K}$.*

Pogledajmo kako možemo konstruirati Shamirovu (t, n)–shemu praga. Objasnit ćemo dva načina konstrukcije. Prvi je korištenjem linearnih jednadžbi za određivanje koeficijenata polinoma a drugi je Langrangeovom interpolacijom polinoma ([5]). Neka je skup ključeva (tajni) $K = \mathbb{Z}_p$, pri čemu je $p \geq n + 1$ prost broj i $\mathbb{Z}_p$ je prsten ostatak modulo p. Neka je i skup dijelova ključa S jednak $\mathbb{Z}_p$. Opisat ćemo konstrukciju dijeljenja ključa $\mathcal{K}$ Shamirovom shemom.

2.1 Shamirova metoda i intepolacijski polinomi

Konstrukcija Shamirove t-n sheme praga:

1. Djelitelj $\mathcal{D}$ izabere n različitih elemenata iz $\mathbb{Z}_p$. Označimo ih s x_i, za $1 \leq i \leq n$ (tu je potreban zahtjev da je $n + 1 \leq p$). Za $i \in \{1, \ldots, n\}$ djelitelj $\mathcal{D}$ vrijednosti x_i pridruži svakom članu P_i.

2. *Dijeljenje dijelova:*

   - Neka je $K \in \mathbb{Z}_p$ (tajna) tajni ključ koji želimo podijeliti. Djelitelj $\mathcal{D}$ tajno odabere (neovisno i slučajno) t-1 element $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$.

- $\forall i \in \{1, \ldots, n\}$ $\mathcal{D}$ izračuna $y_i = a(x_i)$, pri čemu je

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

Za $1 \leq i \leq n$ djelitelj $\mathcal{D}$ članu P_i pridruži i izračunati y_i.

U ovoj konstrukciji djelitelj nad konačnim prstenom $\mathbb{Z}_p$ sastavi slučajni polinom $a(x)$ koji je najviše stupnja $t-1$ i u kojem je konstantni član polinoma zapravo traženi ključ $\mathcal{K}$. Svaki član P_i dobije par (x_i, y_i) pripadnog polinoma, za $1 \leq i \leq n$. Objasnimo kako podskup skupa svih članova, označimo ga s $\mathcal{B}$, kardinaliteta t odredi ključ polinomijalnom interpolacijom.
Bez smanjenja općenitosti neka članovi $P_1, \ldots, P_t$ žele odrediti ključ $\mathcal{K}$.

- Iz konstrukcije znamo da je $y_i = a(x_i)$ za $\forall j \in \{1, \ldots, t\}$, pri čemu je $a(x) \in \mathbb{Z}_p[x]$ tajni polinom kojeg je odredio djelitelj $\mathcal{D}$
- Stupanj polinoma $a(x)$ je najviše $t-1$ pa polinom možemo zapisati u obliku $a(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$. Koeficijenti $a_0, \ldots, a_{t-1} \in \mathbb{Z}_p$ su nepoznati a za $x = 0$ $a(0) = K$,odnosno vrijednost polinoma u točki nula jednaka je ključu koji želimo odrediti
- $\forall j \in \{1, \ldots, t\}$ $y_j = a(x_j)$. Članovi podskupa $\mathcal{B}$ $P_i, i \in \{1, \ldots, t\}$ tvore linearni sustav od t jednadžbi s t nepoznanica $a_0, \ldots, a_{t-1}$
- Linearne jednadžbe su međusobno nezavisne stoga ćemo dobiti jedinstveno rješenje sustava i traženi ključ $\mathcal{K}$ odnosno a_0

Iz ovoga očito slijedi da indekse $1, \ldots, t$ možemo zamijeniti s bilo kojim indeksima $i_1, \ldots, i_t$.
Pogledajmo sada jedan primjer.

Primjer 2.1.1. *Neka je $p = 17$, $t = 3$ i $n = 5$ i neka su koordinate $x_i = i, 1 \leq i \leq 5$ poznate. Pretpostavimo da članovi podskupa $B = \{P_1, P_3, P_5\}$ žele odrediti ključ $\mathcal{K}$ a pripadni y_i su redom 8, 10 i 11 za $i = 1, 3, 5$. Polinom $a(x)$ možemo zapisati $a(x) = a_0 + a_1 x + a_2 x^2$ i izračunamo a(1), a(3) i a(5) u konačnom polju $\mathbb{Z}_{17}$. Dobit ćemo sustav od 3 linearne jednadžbe:*

$$\begin{aligned} a_0 + a_1 + a_2 &= 8 \mod 17 \\ a_0 + 3a_1 + 9a_2 &= 10 \mod 17 \\ a_0 + 5a_1 + 8a_2 &= 11 \mod 17 \end{aligned}$$

Rješavanjem ovog sustava dobije se jedinstveno rješenje u $\mathbb{Z}_{17}$*:* $a_0 = 13$*,* $a_1 = 10$ *i* $a_2 = 2$*. Ključ* $K = a_0 = 13$*.*

Teorem 2.1.2. *Shamireva* $(t, n)-$*shema praga s navedenom konstrukcijom je savršena.*

Dokaz. Želimo dokazati dvije stvari. Prva je da odabir bilo kojih t članova iz skupa svih članova možemo odrediti ključ (tajnu) i da za bilo koji odabir članova manji od t ne možemo odrediti ključ.
Pokažimo najprije da bilo kojih t članova prema konstrukciji (Shamirove sheme) zajedno mogu odrediti ključ $\mathcal{K}$, tj. riješiti pripadni sustav od t linearnih jednadžbi. Za $\forall j \in \{1, \ldots, t\}$ vrijedi $y_j = a(x_j)$, pri čemu je $a(x) = a_0 + \ldots + a_{t-1}x^{t-1}$ i a_0 je ključ . Iz t dijelova dobijemo pripadni sustav linearnih jednadžbi u $\mathbb{Z}_p$:

$$\begin{aligned} a_0 + a_1x_1 + \cdots + a_{t-1}x_1^{t-1} &= y_1 \\ a_0 + a_1x_2 + \cdots + a_{t-1}x_2^{t-1} &= y_2 \\ &\vdots \\ a_0 + a_1x_t + \cdots + a_tx_t^{t-1} &= y_t \end{aligned}$$

Matrični zapis sustava je:

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

Označimo matricu sa A. Matrica A je poznata Vandermondeova matrica čija je determinanta dana jednadžbom:

$$\det(A) = \prod_{1 \le j < i \le t} (x_i - x_j) \mod p \tag{2.1}$$

Matematičkom indukcijom se pokaže da je formula (2.1) dobra. Za dokaz pogledati [2]. Gornji sustav ima rješenje ako je determinanta različita od 0. Sjetimo se da su odabrani x_i, $i = 1, \ldots, n$, međusobno različiti pa stoga su i razlike $x_i - x_j$ različite od nule. Produkt danih razlika računamo u $\mathbb{Z}_p$ (p prost broj a $\mathbb{Z}_p$ je konačni prsten). Produkt elemenata različitih od nule je također različit od nule u prstenu pa je i $\det(A) \neq 0$. Determinanta matrice A je različita od nule pa sustav ima jedinstveno rješenje u $\mathbb{Z}_p$. To znači da bilo koji podskup od t članova može odrediti ključ u danoj metodi.

Ostalo je pokazati da kombiniranjem dijelova članova kojih je manje od t ne možemo odrediti ključ. Neka je odabrano bilo kojih $t - 1$ članova iz skupa svih članova. Zapišemo

li svaku pojedinačnu jednadžbu kao i gore dobit ćemo sustav od $t-1$ jednadžbe s t nepoznanica. Pretpostavimo da je y_0 vrijednost ključa $\mathcal{K}$. kako je $K = a_0 = a(0)$, dodajmo sustavu i tu jednadžbu. Sada imamo t jednadžbi s t nepoznanica. Matrica sustava je opet Vandermondeova i dobit ćemo jedinstveno rješenje. Stoga za svaku vrijednost y_0 dobije se jedinstveni polinom $p(x)$, označimo ga s $a_{y_0}(x)$, tako da vrijedi $y_j = a_{y_0}(x_j)$, $j \in \{1 \dots t-1\}$ i $y_0 = a_{y_0}(0)$. Stoga ne možemo ni jednu vrijednost ključa isključiti kao da ne bi bila zapravo traženi ključ pa bilo koji podskup od $t-1$ članova ne može dobiti ni jednu informaciju o ključu $\mathcal{K}$. □

2.2 Shamirova metoda i Langrangeov interpolacijski polinom

Svaki polinom se može zapisati na sljedeći način:

$$a(x) = \sum_{i=1}^{t} y_i l_i,$$

gdje su funkcije l_i dane formulom

$$l_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x - x_j}{x_i - x_j}$$

Svaka od tih funkcija je polinom stupnja t sa svojstvom da je $l_i(x_j) = \delta_{i,j}$, za $i, j = 1, 2 \dots, t$. Skup $\mathcal{B}$ s t članova može izračunati polinom $a(x)$ korištenjem Langrangeove formule interpolacije. Računanje se još dodatno pojednostavi jer nije potrebno izračunati sve koeficijente polinoma $a(x)$ nego samo slobodni član $a_0 = a(0) = K$. Stoga računa se sljedeći izraz koji se dobije uvrštavanjem točke $x = 0$ u Langrangeovu interpolacijsku formulu:

$$K = \sum_{j=1}^{t} y_j \prod_{\substack{k=1 \\ k \neq j}}^{t} \frac{x_k}{x_j - x_k}$$

Definiramo (za $j = 1, 2, \dots, t$)

$$b_j \equiv \prod_{\substack{k=1 \\ k \neq j}}^{t} \frac{x_k}{x_j - x_k}$$

. Tada je $K = \sum_{j=1}^{t} y_j b_j$. Iz ovoga iščitavamo da se $\mathcal{K}$ dobije linearnom kombinacijom t dijelova pridruženih članovima.
Ova konstrukcija vrijedi za svaki skup ključeva $K = \mathbb{Z}_m$ s pripadnim dijelovima ključa $S = \mathbb{Z}_m$.

Napomena 2.2.1. *Uočimo da u ovom slučaju* $\boldsymbol{m}$ *ne mora biti prost broj.*

Opisat ćemo konstrukciju tzv. $(t, t)-$sheme praga koju ćemo susresti i u sljedećim poglavljima.

Konstrukcija $(t, t)-$***sheme praga:***

1. Djelitelj $\mathcal{D}$ tajno izabere (slučajno i nezavisno) $t-1$ element $y_i \in \mathbb{Z}_m, i = 1, 2, \ldots t-1$
2. Zatim izračuna
$$y_t = K - \sum_{j=1}^{t-1} y_j \mod m$$
3. Svakom članu P_i djelitelj $\mathcal{D}$ dadne njegov $y_i, i = 1, 2, \ldots, t$

Teorem 2.2.2. *Metoda definirana gornjom konstrukcijom je savršena.*

Dokaz. Dokazujemo opet dvije tvrdnje. Prva je da kombiniranjem dijelova od svih t članova može se otkriti ključ $\mathcal{K}$ a druga je da kombiniranjem manje od t dijelova ne može se otkriti.
Prva tvrdnja očito vrijedi prema načinu na koji je definirana podjela dijelova jer je

$$K = \sum_{j=1}^{t} y_j \mod m$$

Neka je $\mathcal{B} = \mathcal{P} \setminus P_i$ za neki $i \in \{1, \ldots, t\}$. Zbrajanjem dijelova iz $\mathcal{B}$ dobije se $K - y_t$. Budući da članovi iz $\mathcal{B}$ ne znaju vrijednost od y_t tada ne mogu saznati ni vrijednost ključa $\mathcal{K}$. Time smo dokazali da je $(t, t)-$shema savršena. □

Za kraj poglavlja pogledajmo rješenje primjera 2.1.1 korištenjem Langrangeove interpolacijske formule.

Primjer 2.2.3. *Članovi* $\{P_1, P_3, P_5\}$ *korištenjem svojih dijelova mogu izračunati* b_i*,* $i = 1, 2, 3$*. Npr. za* $i = 1$

$$b_1 = \frac{b_3 b_5}{(b_1 - b_3)(b_1 - b_5)} \mod 17 = 5 \cdot 3 \cdot 2^{-1} \cdot 4^{-1} \mod 17 = 4.$$

Analogno bi dobili i $b_2 = 3$ *i* $b_3 = 11$*.* $y_i = \{8, 10, 11\}$ *za* $i = 1, 2, 3$ *pa je* $\mathcal{K} = (4 \cdot 8 + 3 \cdot 10 + 11 \cdot 11) \mod 17 = 13$*.*

Poglavlje 3

Blakelyeva metoda dijeljenja tajni

Blakleyeva metoda dijeljenja tajni je geometrijska i također $(t, n)-$shema praga. Radi jednostavnosti metodu ćemo objasniti na trodimenzionalnom prostoru i presjeku ravnina a to je zapravo slučaj sheme za $t = 3$. Ukoliko se želi za dijeljenje tajni koristiti $(t - 1)-$dimenzionalne hiperravnine u $t-$dimenzionalnim prostorima tada možemo primijeniti istu metodu da bi stvorili $(t, n)-$shemu praga neovisno o vrijednostima t i n.
Neka je p prost broj i neka je x_0 ključ (tajna). Djelitelj $\mathcal{D}$ nasumično odabere $y_0, z_0 \mod p$ i s Q označi točku (x_0, y_0, z_0) u $3-$dimenzionalnom prostoru $\mod p$. Djelitelj tada svakom članu P_i dadne različite jednadžbe ravnina koje prolaze kroz točku Q. Dalje (djelitelj $\mathcal{D}$) slučajno odabere brojeve $a, b \mod p$ i definira $c \equiv z_0 - ax_0 - by_0 \mod p$. Tada je jednadžba ravnine jednaka:

$$z = ax + by + c. \tag{3.1}$$

Presjek tri ravnine je točka a presjek dvije ravnine je pravac. Stoga presjekom sve tri ravnine koje su dane članovima $P_i, i = 1, 2, 3.$ dobit će se tražena točka dok presjekom dvije ravnine ne možemo saznati ništa o ključu x_0.
Primijetimo da točka Q ima tri koordinate a samo jednu koristimo da njome predstavimo tajni ključ. To je zato što vrijedi da ako bi cijeli ključ(tajni ključ i ostali dio ključa koji ne čini tajnu koju želimo otkriti) rasporedili među sve tri koordinate tada bi imali jedan i samo jedan ključ koji bi odgovarao točki na pravcu koja je presjek ravnina koje pripadaju članovima.
Tri člana kombiniranjem svojih jednadžbi žele otkriti tajni ključ. Tada se dobije sustav od tri linearne jednadžbe:

$$a_i x + b_i y - z \equiv -c_i \mod p, 1 \leq i \leq 3 \tag{3.2}$$

Matrični zapis sustava je:

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

Kao i kod Shamirove metode vrijedi da će sustav imati rješenje sve dok je determinanta matrice modulo p različita od nule.

Primjer 3.0.1. *Neka je $p = 73$. Neka su članovima $P_i, i \in \{1, 2, 3, 4, 5\}$ dane sljedeće jednadžbe:*

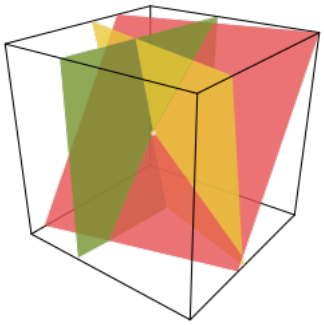
$$\begin{aligned} P_1 &: \quad z = 4x + 19y + 68 \\ P_2 &: \quad z = 52x + 27y + 10 \\ P_3 &: \quad z = 36x + 65y + 18 \\ P_4 &: \quad z = 57x + 12y + 16 \\ P_5 &: \quad z = 34x + 19y + 49 \end{aligned}$$

Ukoliko članovi P_1, P_2, P_3 žele otkriti ključ x_0 tada moraju riješiti pripadni sustav:

$$\begin{bmatrix} 4 & 19 & -1 \\ 52 & 27 & -1 \\ 36 & 65 & -1 \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = \begin{bmatrix} -68 \\ -10 \\ -18 \end{bmatrix} \mod 73$$

Rješenje sustava je $(x_0, y_0, z_0) = (42, 29, 57)$ i stoga traženi tajni ključ je $x_0 = 42$. Analognim postupkom bi tražili x_0 za kombinaciju bilo koja tri člana od P_1, P_2, P_3, P_4, P_5. (Primjer je iz [7].)

Sve dok je p dovoljno velik vrlo je vjerojatno da će matrica imati inverz (determinanta matrice je različita od nule) premda to nije garancija. U slučaju trodimenzionalnog prostora nije teško odabrati takve a, b i c da bi matrica imala inverz. Slično se događa i kod Shamirove metode. Tu zapravo nalazimo sličnost između ove metoda i Shamirove koja se može promatrati kao specijalni slučaj Blakelyeve metode. No kao što smo vidjeli u Shamirovoj metodi matrica sustava je uvijek Vandermondeova pa uvijek postoji rješenje. Još jedna prednost Shamirove metode je da svaki član dobiva manje podataka: (x_i, y_i) u odnosu na $(a_i, b_i, c_i, \dots)$



Slika 3.1: $(3, n)-$shema praga s presjekom ravnina

Na slici 3 prikazan je presjek tri ravnine u jednoj točki u trodimenzionalnom prostoru. Vidimo da točka leži u svakoj od ravnina i to je također informacija koju zna svaki član. Zbog toga Blakelyeva metoda nije savršena što smo naveli i u prvom poglavlju.

Konstrukcija za Blakleyevu metodu:

1. Jednadžbe ravnina $\pi_i, i = 1, 2, 3 \ldots$ su informacije koje djelitelj $\mathcal{D}$ dodjeli članovima
2. S presjekom svojih ravnina članovi mogu otkriti točku čija jedna od koordinata je tajna

Poglavlje 4

Vizualna kriptografija

U vizualnoj kriptografiji podatak koji želimo šifrirati dan je u obliku slike, koja može sadržavati i tekst. Zapravo slika, kako ćemo i nazivati tajni podatak u poglavlju, je format čije se dešifriranje ne provodi računarskim putem nego putem ljudskog vida što je osobito pogodno u situacijama kada računala nisu dostupna.

Godine 1994. vizualnu kriptografiju su uveli Adi Shamir i Moni Naor[1]. Vizualna kriptografija je također $(t, n)-$shema praga.

4.1 Nešto malo o pikselima

Sheme vizualne kriptografije koriste se u šifriranju monokromatskih slika, odnosno binarnih slika. Monokromatska slika,što i po samom imenu možemo naslutiti, sastoji se od tonova jedne boje i najpoznatiji primjer je crno-bijela fotografija. Binarna slika (eng. 1-bit monochrome) uzima vrijednost piksela iz skupa $\{0, 1\}$. Piksel je osnovni element digitalne slike i u računalu je predstavljenim s određenim brojem bitova. No slika ne mora nužno biti monokromatska, moguće je raditi i sa slikama u boji na koje se prije samog postupka šifriranja primjenjuju određene preinake.

Djelitelj $\mathcal{D}$ pri djeljenju slike ne dijeli originalnu sliku na dijelove (u vizualnoj kriptografiji dijelovi se nazivaju ***folije***) i koje distribuira među članovima. Razlog tomu je da bi pojedini dijelovi sadržavali jasno čitljive podatke o slici, odnosno originalni raspored piksela s izvorne slike. Uzmimo za primjer da promatramo neki crni piksel s folije s_i (eng. slide) člana P_i. U bilo kojem trenutku kada bi preklopili folije i ukoliko bi među njima bila i folija s_i rezultat bi bio crni piksel. No to bi značilo i da je taj piksel u originalnoj slici također crn a to dalje povlači da svaka folija sadrži dio originalne slike a time je u pitanje doveden uvjet sigurnosti sheme. Naor i Shamir su bili svjesni toga i uspjeli su tomu

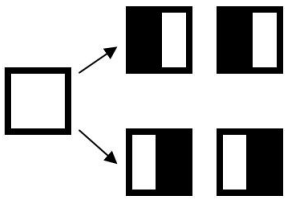
[1] izraelski matematičar

doskočiti. Djelitelj $\mathcal{D}$ će i dalje podijeliti sliku na folije (prozirne folije) i razdijeliti ih među članovima, no svaki piksel iz originalne slike će također biti šifriran za svaku pojedinu foliju. Da bi lakše razumjeli ideju koja stoji u pozadini pogledajmo jedan primjer za $(2, 2)-$vizualnu shemu praga.

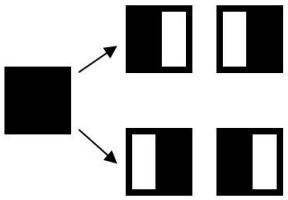
Radi jednostavnosti označimo bijeli piksel s 0, a crni piksel s 1. Naor i Shamir su se dosjetili da svaki piksel (bijeli ili crni) zamijene s manjim brojem piksela, odnosno subpiksela koji će predstavljati dijelove slike. Taj broj subpiksela označimo s m. Broj m će označavati *ekspanziju* orginalnog piksela. (Piksel možemo zamisliti i kao kvadrat kako su i ilustrirani na slikama 4.1 i 4.2, koji se djelovanjem algoritma $(2, 2)-$vizualne sheme praga dijeli na manji broj crnih i bijelih pravokutnika.) Sada se vratimo na primjer $(2, 2)-$sheme praga i pokažimo način na koji djelitelj $\mathcal{D}$ može generirati folije za članove. Neka se djelitelj $\mathcal{D}$ u procesu šifriranja piksela koristi i bacanjem novčića koji je pravilan, tj. vjerojatnost da padne pismo ili glava je jednaka ($p_{pismo} = p_{glava} = \frac{1}{2}$).

Šifriranje bijelog piksela:
Djelitelj $\mathcal{D}$ baci novčić. Ako padne pismo na obje folije zacrni lijevu polovinu kvadratića a ako padne glava obrnuto.

Šifriranje crnog piksela:
Djelitelj $\mathcal{D}$ baci novčić. Ako padne pismo na prvoj foliji zacrni lijevu a na drugoj desnu polovinu kvadratića. Ako padne glava obrnuto.



Slika 4.1: Šifriranje bijelog piksela



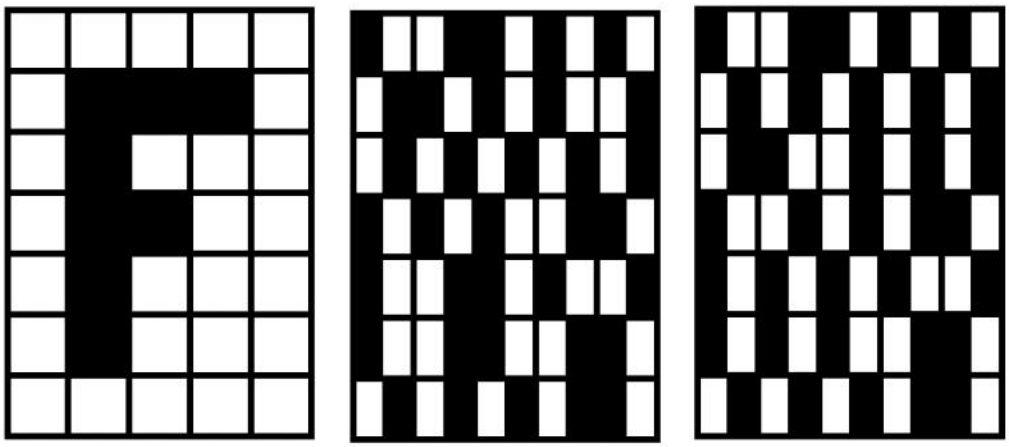
Slika 4.2: Šifriranje crnog piksela

Za ovako definirani algoritam šifriranja piksela iz originalne slike vrijedi uvjet sigurnosti za shemu. BSO, pretpostavimo da promatramo nasumično odabran piksel , nazovimo ga $\boldsymbol{p}$, u foliji s_i, za $i = 1$. Jedan od dva subpiksela od $\boldsymbol{p}$ je crn, a drugi je bijel. Štoviše,

svaka od dvije mogućnosti – prvi subpiksel je crn, a drugi bijel i prvi je bijel, drugi crn – su jednako vjerojatne. Ovo je nezavisno od toga je li piksel iz originalne slike bijel ili crn. Zbog toga, član P_1 na osnovu svoje folije ne može zaključiti ništa o tome je li originalni piksel crn ili bijel.
Potpuno isti argument vrijedi i za foliju s_2, odnosno člana P_2. Budući da se algoritam šifriranja piksela originalne slike koristi bacanjem pravilnog novčića, promatranje bilo koje grupe subpiksela na pojedinačnim folijama ne može se saznati ništa o originalnoj slici. Ovime je pokazano da je shema zadovoljaca uvjet sigurnosti.
Nadalje možemo se pitati što se dogodi preklapanjem dviju folija? Možemo promatrati određeni piksel sa prve slike u nizu slike 4.3. Ukoliko je piksel crn, preklapanjem folija dobiju se dva crna subpiksela jedan do drugog (promotrite šifrate tog piksela za prvu i drugu foliju redom). Ukoliko je bijel, preklapanjem folija dobije se jedan crni i jedan bijeli subpiksel jedan do drugog.

Ovdje je zgodno spomenuti termin "gray level" za piksel dobiven preklapanjem folija. Originalni crni piksel ima "gray level" jedan a ako je bijel „gray level" je jedna polovina. Ovime u rekonstruiranoj slici je prisutan 50%-tni gubitak kontrasta što može otežavati dešifriranje. Otežavanju dešifriranja doprinosi i rastegnutost folija koje pak dolazi od printanje istih i teško ih je pravilno poravnati. Stoga shema ima najbolju primjenu na slikama koje se sastoje od relativno malo relativno velikih piksela ([1])).

Komentar: Dijelovi koje dobivaju članovi se zapravo tiskaju na prozirne folije i pri tom ne dolazi do tiskanja bijelih piksela. Zbog toga je prikladniji naziv za bijele piksele prozirni.



Slika 4.3: Vizualna $(2,2)-$shema praga; originalna slika i pripadne folije ([1])

4.2 Opis (2, n)-vizualne sheme praga

U ovom poglavlju objasnit ću konstrukciju vizualne sheme praga za $t = 2$. Već smo rekli da ukoliko imamo veći broj folija teško ih je poravnati i time je otežana rekonstrukcija originalne slike pa ćemo , stoga, promatrati samo konstrukciju sheme za generiranje dvije folije.

Za opis $(2, n)-$vizualne sheme praga upotrebljavaju se $n \times m$-dimenzionalne matrice M_0 i M_1. Matrica M_0 upotrebljava se za šifriranje bijelog piksela a matrica M_1 crnog. Elementi obje matrice su iz skupa $\{0, 1\}$ pa se nazivaju i binarnim matricama, a njihovi retci su binarni vektori.

Konstrukcija $(2, n)-$***vizualne sheme praga:***
Za svaki piksel P djelitelj $\mathcal{D}$ napravi sljedeće korake:

1. Generira slučajnu permutaciju π skupa $\{1, 2, \ldots, m\}$
2. Ako je P crni piksel onda upotrijebi permutaciju π nad stupcima matrice M_1, inače nad stupcima matrice M_0. Dobijenu matricu označi s T_P.
3. za $1 \leq i \leq n$ $i-$ti redak matrice T_P se sastoji od m 0 i 1 koji predstavljaju P u $i-$toj foliji

Prije nego se pozabavimo osobinama koje moraju imati matrice M_0 i M_1, pogledajmo na primjeru šifriranje nekog piksela za $(2, 3)$-vizualnu shemu praga. Pripadne matrice M_0 i M_1 su redom:

$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Za proizvoljan m i skup $\{1, 2, \ldots, m\}$ ukupan broj permutacija skupa jednak je $m!$. Za $m = 3$ ima ih $3! = 6$.

$$\pi_1 = (123) \qquad \pi_2 = (132) \qquad \pi_3 = (213)$$
$$\pi_4 = (231) \qquad \pi_5 = (312) \qquad \pi_6 = (321)$$

Djelitelj $\mathcal{D}$ slučajnu permutaciju može izabrati npr. bacanjem kocke. Pretpostavimo da želi šifrirati crni piksel, u oznaci P, i neka je pri bacanju kocke pala 3. Tada $\mathcal{D}$ konstruira novu matricu T_P čiju su stupci redom 2., 1. pa 3. stupac matrice M_1.

$$T_P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Sada iz redaka matrice T_P iščitavamo 'boju' (crna ili bijela) pripadnih subpiksela originalnog piksela. Prvi član na svojoj foliji ima prvi i treći subpiksel bijel (proziran) a drugi crn. Analogno iščitamo za ostala dva člana.

Pri konstrukciji matrica M_0 i M_1 važno je da zadovoljavaju sigurnost sheme, tj. da članovi gledanjem u svoje folije ne mogu otkriti nikakvu informaciju o izvornoj slici, ali i da je preklapanjem folija rekonstruirana slika čitljiva. Prije nego navedem svojstva kojima su ova dva uvjeta osigurana, potrebno je uvesti neke oznake i definirati binarnu relaciju nad recima matrica M_0 i M_1.

S $wt(x)$, označit ćemo broj jedinica u binarnom vektoru x, pri čemu je x redak matrice M_i, $i = 0, 1$. Sa $x\ OR\ y$ definira se binarna relacija nad vektorima x i y tako da vrijedi: $0\ OR\ 0 = 0$, $1\ OR\ 0 = 0\ OR\ 1 = 1$ i $1\ OR\ 1 = 1$. Za matrice M_0 i M_1 prvo se odredi broj jedinica u svakom retku (isti je za sve retke u obje matrice) i označi se s w. Ako je ekspanzija piksela m tada će broj nula (0) u recima biti $m - w$. Sada se svaki piksel originalne slike sastoji od w crnih subpiksela i $m - w$ bijelih subpiksela. Nadalje se odredi broj $\gamma \in \mathbb{R}$ td. je $0 \leq \gamma \leq 1$. γ će predstavljat relativni kontrast u slici dobiven preklapanjem folija. Uvjet sigurnosti sheme postignut je svojstvom da je $wt(M_1[i]) = w$, $0 \leq i \leq 1$ a slika je čitljiva iz preklopljenih folija ako vrijedi $wt(M_1[i]\ OR\ M_1[j]) \geq w + \gamma m$, $0 \leq i < j \leq 1$.

Uzmimo za primjer piksel P_i iz folije s_i i njemu odgovarajući piksel P_j iz folije s_j. Preklapanjem navedenih folija tj. odgovarajućih piksela broj crnih subpiksela novonastalog piksela bit će jednak $wt(P_i\ OR\ P_j)$. Pikseli P_i i P_j su dobiveni primjenom iste permutacije nad stupcima matrice M_0 ili M_1 (u ovisnosti o tome je li piksel iz originalne slik koji je kriptiran bio crni ili bijeli). AKo je matrica bila M_0 tada vrijedi da je $wt(P_i\ OR\ P_j) = w$, inače $wt(P_i\ OR\ P_j) \geq w + \gamma m$. Stoga zaključujemo da je rekonstruirani bijeli piksel $\frac{w}{m}$ crn, a crni piksel je najmanje $\frac{w+\gamma m}{m}$ crn. Očito je razlika između bijelih i crnih rekonstruiranih piksela najmanje u γm od m subpiksela s time je omogućena čitljivost.

Pogledajmo još neke primjere matrica M_0 i M_1 za $(2, n)-$vizualnu shemu praga i $(t, n)-$vizualnu shemu praga, za $t \neq 2$.

1. $(2, 2)-\text{VTS}^2$ za $m = 2$ i $\gamma = \frac{1}{2}$

$$M_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

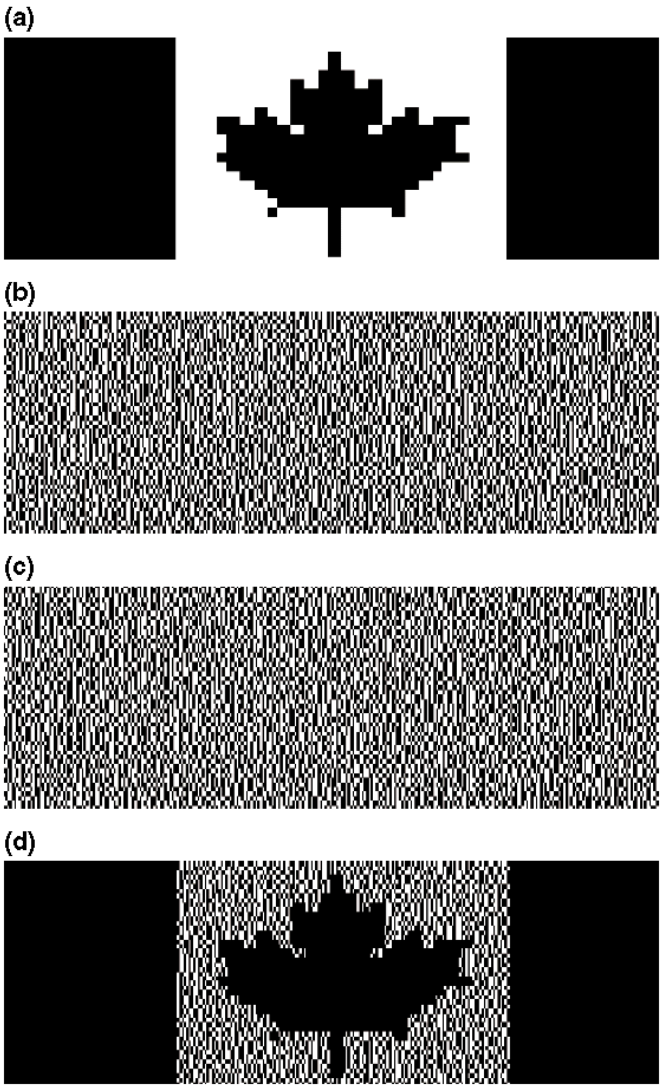
2. $(2, 3)-\text{VTS}$ za $m = 3$ i $\gamma = \frac{1}{3}$

$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

[2] visual threshold scheme

3. $(3,3)-$VTS za $m = 4$ i $\gamma = \frac{1}{4}$

$$M_0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$



Slika 4.4: Kanadska zastava šifrirana na folijama i rekonstruirana slika iz preklopljenih folija

Poglavlje 5

Dijeljenje tajni i Kineski teorem o ostacima

U prvom poglavlju sam napisala da tajnu možemo podijeliti koristeći Kineski teorem o ostacima (eng. Chinese Remainder Theorem). Štoviše, KTO-a sam za sebe već čini jednu shemu za dijeljenje tajni bez dodatne potrebe za njegovom izmjenom. Iskažimo sada teorem.

Teorem 5.0.1. *(Kineski teorem o ostacima) Neka su $m_1, m_2, \ldots, m_t$ u parovima relativno prosti prirodni brojevi*[1]*, te neka su $a_1, a_2, \ldots, a_t$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \mod m_1, x \equiv a_2 \mod m_2, \ldots, x \equiv a_t \mod m_t \tag{5.1}$$

ima rješenje. Ako je x_0 jedno rješenje, onda su sva rješenja od (5.1) dana sa $x \equiv x_0$ (mod $m_1 m_2 \cdots m_t$).

Neka su $m_1, m_2, \ldots, m_t$ u parovima relativno prosti brojevi. Proizvoljan broj S takav da vrijedi $0 \leq S < \prod_{i=1}^{t} m_i$ jednoznačno se može odrediti korištenjem Kineskog teorema o ostacima. Polazeći od ove ideje konstruira se shema za dijeljenje tajni temeljena na KTO.

Konstrukcija (t, n)***–sheme CRT:***

1. Djelitelj $\mathcal{D}$ izabere n u parovima relativno prostih brojeva tako da za odabir bilo kojih t od njih i ključ $\mathcal{K}$ vrijedi $\mathcal{K} < \prod_{k_i=1}^{t} m_{k_i}$ a za odabir bilo kojih $(t-1)$ njih (i manje) $\mathcal{K} > \prod_{k_i=1}^{t-1} m_{k_i}$

2. U sljedećem koraku $\mathcal{D}$ odredi dijelove s_i, za $i = 1, 2, \ldots, n$ za članove $P_1, P_2, \ldots, P_n$ tako da vrijedi $s_i \equiv \mathcal{K} \mod m_i$

[1] $(m_i, m_j) = 1, i \neq j, i, j \in \{1, 2, \ldots, t\}$

3. za rekonstrukciju ključa $\mathcal{K}$ koristi se KTO i kombinacija dijelova bilo kojih t članova

U daljnem nastavku poglavlja pogledat ćemo još dvije metode implementirane Kineskim teoremom o ostacima.

5.1 Mignotteova shema praga

Mignotteova shema praga koristi specijalne, tzv. Mignotteove nizove cijelih brojeve. Osim definicije Mignotteovog niza ovaj odjeljak ne donosi ništa novo u konstrukciju sheme praga u odnosu na prethodni odjeljak.

Definicija 5.1.1. *Neke je n prirodan broj, tako da $n \geq 2$ i neka je $2 \leq t \leq n$. Za niz pozitivnih cijelih brojeva $p_1 < p_2 < \cdots < p_n$ koji su u parovima relativno prosti kažemo da je $(t, n)-$ Mignotteov niz ako vrijedi:*

$$\prod_{i=0}^{t-2} p_{n-i} < \prod_{i=1}^{t} p_i.$$

Gornja nejednakost ekvivalentna je s sljedećom nejednakosti

$$max_{1\leq i_1<\cdots<i_{t-1}\leq n}(p_{i_1} \ldots p_{i_{t-1}}) < min_{1\leq i_1<\cdots<i_t\leq n}(p_{i_1} \ldots p_{i_t})^2.$$

Prije nego opišemo konstrukciju sheme za $(t, n)-$ Mignotteov niz definirajmo oznake koje ćemo koristiti u konstrukciji.
Za neki $p_1, p_2, \ldots, p_n$ $(t, n)-$ Mignotteov niz označimo s $\alpha = \prod_{i=1}^{t} p_i$, $\beta = \prod_{i=0}^{t-2} p_{n-i}$ i $p = p_1 p_2 \cdots p_n$.

Za poznati (t,n)-Mignotteov niz, shema je dana s:

- Djelitelj $\mathcal{D}$ za ključ $\mathcal{K}$, ,odnosno tajnu, slučajno izabere cijeli broj iz intervala (β, α)
- dijelove I_i odabere tako da vrijedi $I_i \equiv \mathcal{K} \bmod p_i$, za $1 \leq i \leq n$
- Ključ $\mathcal{K}$ može se dobiti korištenjem Kineskog teorema o ostacima za t različitih dijelova $I_{i_1}, \ldots, I_{i_t}$ kao jedinstveno rješenje modulo $p_{i_1} p_{i_2} \cdots p_{i_t}$ sustava

$$\begin{cases} x \equiv I_{i_1} \mod p_{i_1} \\ x \equiv I_{i_2} \mod p_{i_2} \\ \vdots \\ x \equiv I_{i_t} \mod p_{i_t} \end{cases} \tag{5.2}$$

[2](a, b, c) je oznaka za najmanji zajednički višekratnik brojeva a, b, c

Ključ $\mathcal{K}$ je očito cjelobrojno rješenje sustava (5.2) (zadovoljava sve uslove Kineskog teorema o ostacima). Za proizvoljni izbor t dijelova iz $\{I_{i_1}, \ldots, I_{i_n}\}$, $\mathcal{K}$ je iz $\mathbb{Z}_{p_{i_1} p_{i_2} \cdots p_{i_t}}$ jer je $\mathcal{K} < \alpha$. S druge strane, ukoliko imamo samo $(t-1)$ dio, odnosno $I_{i_1}, I_{i_2}, \ldots, I_{i_{t-1}}$, za neke $i_1, \ldots, i_{t-1}$ iz $\{1, 2, \ldots, n\}$ znamo da je $\mathcal{K} \equiv x_0 \bmod p_{i_1} p_{i_2} \cdots p_{i_{t-1}}$ pri čemu je x_0 jedinstveno rješenje sustava analognog sustavu (5.2). Zbog ovog očito vrijedi da skup kardinaliteta manjeg od t ipak sadrži neku informaciju o tajni što Mignotteovu shemu čini nesavršenom. Mignotteovu shemu se može generalizirati, tj. mogu se koristiti i nizovi pozitivnih cijelih brojeve čiji elementi nisu nužno u parovima relativno prosti. Takva proširena shema konstruira se isto kao i navedena no za otkrivanje ključa $\mathcal{K}$ koristi se općenitija varijanta Kineskog teorema o ostacima. Detaljnije možete pogledati u [4].
Pogledajmo jedan primjer za Mignotteovu shemu, s unaprijed namještenim malim parametrima radi lakšeg računanja.

Primjer 5.1.2. *Neka je* $n = 5$ *i* $t = 3$. *Članovi Mignotteovog niza su redom jednaki:* $p_1 = 10, p_2 = 14, p_3 = 18, p_4 = 22, p_5 = 26$. *Lako se vidi da članovi* p_i, $1 \leq i \leq 5$, *zadovoljavaju svojstvo Mignotteovog niza. Neka je ključ* $\mathcal{K} = 615$ *i pripadni* I_i *(redom) su:* $I_1 = 5, I_2 = 13, I_3 = 3, I_4 = 21, I_5 = 17$ *(prisjetimo se* $I_i = \mathcal{K} \bmod p_i$ *za* $1 \leq i \leq 5$*).*
U fazi rekonstrukcije ključa $\mathcal{K}$*, možemo upotrijebiti vrijednosti dijelova prva tri člana (ili bilo koja tri člana), i* $\mathcal{K}$ *dobiti kao jedinstveno riješenje modulo* 630 *sustava:*

$$\begin{cases} x \equiv 5 \mod 10 \\ x \equiv 13 \mod 14 \\ x \equiv 3 \mod 18 \end{cases}$$

Uočimo da brojevi 10, 14 *i* 18 *nisu u parovima relativno prosti pa se Kineski teorem o ostacima ne može direktno primijeniti. Jedan od načina da riješimo sustav je da svaki od brojeva predstavimo kao umnožak prostih brojeva i zbog osobina relacije modulo dobiveni moduli će biti potencije prostih brojeva. Time ćemo dobiti sustav ekvivalentan početnom koji se riješi direktnom primjenom Kineskog teorema o ostacima čime dobijemo i vrijednost traženog ključa* $\mathcal{K} = 615$.

Napomena 5.1.3. *Za kraj odjeljka osvrnimo se još jednom na određivanje ključa* $\mathcal{K}$. *Za bilo koji* $t-1$ p_i, $1 \leq i \leq n$, $\mathcal{K}$ *se ne može odrediti jer je njihov umnožak manji ili jednak* β *a* $\mathcal{K} > \beta$. *S druge strane, za bilo kojih* t p_i, $1 \leq i \leq n$, $\mathcal{K}$ *se može odrediti jer je njihov umnožak veći ili jednak* α *(*$\mathcal{K} < \alpha$*).*

5.2 Asmuth-Bloomova shema praga

Ova shema, koju su predložili Asmuth[3] i Bloom[4], također koristi specijalne nizove brojeva. Točnije, koristi nizove $p_0, p_1, \dots p_n$ tako da $p_0 < p_1, < \cdots < p_n$ i imaju svojstvo:

$$p_0 \prod_{i=0}^{t-2} p_{n-i} < \prod_{i=1}^{t} p_i$$

Niz s ovakvim svojstvom se naziva i Asmuth-Bloomov niz.

Za poznati Asmuth-Bloomov niz, shema je dana s:

- Djelitelj $\mathcal{D}$ za ključ $\mathcal{K}$ slučajno izabere element iz $\mathbb{Z}_{p_0}$
- Za izabrani ključ $\mathcal{K}$ $\mathcal{D}$ bira cijeli broj γ tako da vrijedi $\mathcal{K} + \gamma \cdot p_0 < \prod_{i=1}^{t} p_i$ (važno je da samo da γ zadovoljava ovu nejednakost)
- dijelove I_i dobije kao $I_i \equiv (\mathcal{K} + \gamma p_0) \bmod p_i$, za $1 \leq i \leq n$
- Ključ $\mathcal{K}$ možemo otkriti kao $\mathcal{K} \equiv x_0 \bmod p_0$. x_0 se dobije pomoću Kineskog teorema o ostacima za t dijelova $I_1, \dots, I_t$ kao jedinstveno rješenje modulo $p_1 p_2 \cdots p_t$ sustava

$$\begin{cases} x \equiv I_1 \mod p_1 \\ x \equiv I_2 \mod p_2 \\ \vdots \\ x \equiv I_t \mod p_t \end{cases} \tag{5.3}$$

Kao i kod Mignotteove sheme, Asmuth-Bloomova se može generalizirati i konstruirati za nizove brojeva čiji članovi nisu parovima relativno prosti. Za razliku od Mignotteove sheme Asmuth-Bloomova je *savršena* zbog odabira cijelog broja γ koji je neovisan o ključu $\mathcal{K}$ kojeg je izabrao djelitelj $\mathcal{D}$. Dobro je primjetiti da ključ $\mathcal{K}$ može se otkriti za bilo kojih t dijelova pridruženih članovima, tj. za bilo koji podskup veličine t skupa $\{I_1, I_2, \dots, I_n\}$

Pogledajmo primjer i za ovu shemu i u ovom primjeru ćemo također koristiti male vrijednosti za sve parametre iz jednostavno praktičnih razloga.

Primjer 5.2.1. *Neka je* $n = 4$ *i* $t = 3$. *Članovi Asmuth-Bloomovog niza su redom jednaki:* $p_0 = 3, p_1 = 11, p_2 = 13, p_3 = 17, p_4 = 19$. *Niz* p_i, $0 \leq i \leq 4$, *zadovoljava Asmuth-Bloomovo svojstvo jer vrijedi* $3 \cdot 17 \cdot 19 < 11 \cdot 13 \cdot 19$. *Neka je ključ* $\mathcal{K} = 2$. *Uzmimo da je* $\gamma = 51$. *Tada je* $2 + 51 \cdot 3 = 155$ *pa izračunamo dijelove* I_i *redom za* p_i, $1 \leq i \leq 4$,

[3] C. A. Asmuth

[4] J. Bloom

dobijemo: 1, 12, 2 *i* 3. *Kao u primjeru* 5.1.2 *odaberemo bilo koja tri člana pa možemo uzeti prva tri, tj.* $\{1, 12, 2\}$.

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 12 \mod 13 \\ x \equiv 2 \mod 17 \end{cases} \tag{5.4}$$

Direktnom primjenom Kineskog teorema o ostacima dobije se da jedinstveno rješenje modulo $11 \cdot 13 \cdot 17$ *sustava* (5.4) *je* 155. *Još preostaje izračunati ključ* $\mathcal{K}$ *a on se izračuna iz* $\mathcal{K} = 155 \equiv 2 \mod 3$.

Poglavlje 6

Primjena

U prvom poglavlju rada objasnila sam značenje dostupne familije, tj. familije skupova čiji elementi mogu rekonstruirati neki podatak d koji je bio „razbijen“ na dijelove. Svjedoci smo tomu da su sustav za komunikaciju podataka i računalne mreže u posljednjih nekoliko godine doživjeli nevjerojatan evaluacijski stupanj i da se raznovrsni podaci šalju putem mreže. No svakako velika većina tih podataka ima svoju vrijednost i kao takve potrebno ih je zaštiti od bilo koje vrste nelegalne upotrebe ukoliko bi ih se netko domogao u samom putovanju od točke A do točke B unutar mreže. Stoga je pitanje sigurnosti podataka postalo izrazito bitnim pitanjem današnjice. Shema za dijeljenje tajne je jedan od strategija za sigurnost podataka. Godine 1987. su na odjelu električnih komunikacija tokijskog univerziteta trojica profesora Ito, Saito i Nishizeki su pokazali kako konstruirati shemu dijeljenja tajne za bilo koju dostupnu familiju pri čemu je kod kontrola pristupa metoda dobila svoju primjenu.

Pod elektroničkim izborima (eng. e - voting) se smatra izborni sustav u kojem se izborni podaci prikupljaju, spremaju i kasnije upotrebljavaju kao digitalni podaci. Povjerljivost, autentičnost, integritet i povjerljivost su najvažnija sigurnosna svojstva e-izbora a metode dijeljenja tajni uspješno ih zadovoljavaju i jedna od metoda koja se koristi je Shamirova (t, n) – shema praga.

U prvom poglavlju smo govorili o svojstvu provjerljivosti sheme dijeljenja tajne, odnosno da svaki član može provjeriti valjanost svog dijela. Shemu koja ima navedeno svojstvo nazivamo provjerljivom shemom dijeljenja tajne (eng. VSS, verifiable secret sharing) no sad uvodimo i pojam javno provjerljive sheme dijeljenja tajni. Za shemu kažemo da je javno provjerljiva ukoliko svaki član može provjeriti valjanost svih dijelova tajne distribuiranih od djelitelja $\mathcal{D}$.

Elektroničko bankarstvo i elektronički novac su danas sve učestalije u uporabi. E-novac je digitalna zamjena za gotovinu koja se koristi u elektroničkim plaćanjima. Postoje dva tipa e-novca a to su: online e-novac i offline e-novac. Online e-novac pretpostav-

lja direktnu interakciju s bankom, putem pametnog telefona ili modema, u transakciji s trećom stranom. Offline e-novac omogućava korisnicima obavljanje transakcija bez direktnog uplitanja banke. Offline tip e-novca zasigurno predstavlja kompliciraniji oblik istog i kao takav zahtjeva sigurnost i pouzdanost. Javno provjerljive metode dijeljenja tajni u kombinaciji sa još nekim kriptografskim alatima uspješno rješavaju sve manjkavosti sustava offline e-novca povećavajući njegovu sigurnost.

Bibliografija

[1] Franka Miriam Brueckler, *Kako sakriti sliku*, (2011), http://www.mathos.unios.hr/~middlemath/ppt/vizualna-kriptografija.pdf.

[2] N. Elezovic, *Linearna algebra*, Element, 1995.

[3] A. Herzberg, S. Jarecki, H. Krawczyk i M. Jung, *Proactive Secret Sharing Or: How to Cope With Perpetual Leakage*, (1998), http://www.cs.cornell.edu/courses/cs754/2001fa/339.PDF.

[4] S. Iftene, *General Secret Sharing Based on the Chinese Remainder Theorem*, (2007), https://eprint.iacr.org/2006/166.pdf.

[5] V. Seničar, *Sheme za deljenje skrivnosti*, Magistarska radnja, FMF - Fakulteta za matematiko in fiziko, Ljubljana, 2002.

[6] D. R. Stinson, *Visual criptography and threshold schemes*, (1999), http://www.cs.jhu.edu/~fabian/courses/CS600.624/stinson.pdf.

[7] W. Trappe i L. C. Washington, *Introduction to cryptography with coding theory*, Pearson, 2005.

Sažetak

U ovom radu vidjeli smo neke od osnovnih shema (metoda) dijeljenja tajni, ponajprije one Shamira i Blakleya koji su i idejni začetnici metode *dijeljenja tajni*. Metodama se tajni podatak od strane djelitelja $\mathcal{D}$ podijeli na dijelove i distribuira među grupom učesnika tako da svaki od učesnika dobije pojedini dio tajne pri čemu se ni s jednim od dijelova ne može otkriti ni jedna informacija o tajni. Definiranjem $(t, n)-$shemu praga rekonstrukcija tajne moguća je jedino oporabom t ili više dijelova koje posjeduju članovi. Za svaki strogo manji broj dijelova od t dijelova nemoguće je otkriti bilo koju informaciju o tajni. Sheme poput Shamirove i Asmuth-Bloomove su se pokazale i kao savršene, dok ostale nisu. Autoriziranim skupovima dostupne familije skupova definirani su oni skupovi pomoću kojih možemo otkriti tajnu na osnovu dijelova članova istog. Kod vizualne kriptografije osim što je isto $(t, n)-$shema praga i konstrukcija tajne odnosno pripadnih dijelova sadrži u pozadini matematički račun, za njenu rekonstrukciju koriste se prije svega čovjekov vid.

Summary

In this thesis we have seen some of the basic *secret sharing schemes* (methods), primarily Shamir's and Blakely's who are also initiators of the idea of the secret sharing method. By using secret sharing schemes, the *dealer* $\mathcal{D}$ splits the secret into shares and distributes them among the group of participants. Each participant gets a single share of the secret which does not give them any clue about the secret itself. By defining a (t,n)-threshold scheme, the reconstruction of the secret is possible only by combining shares of t or more participants. For any group with less than t participants no information of the secret can be gained. Shamir's and Asmut-Bloom's schemes have shown to be perfect, while others have not. An access structure defines the authorized sets of participants who are qualified to reconstruct the secret using their shares. In visual cryptography, apart from it being a (t, n)-threshold scheme, the construction of the secret and its belonging shares holds a mathematical calculation in the background, while the secret is reconstructed using human sight.

Životopis

31.05.1991. sam rođena u gradu Prijedor koji leži na obalama rijeke Sane u državi Bosni i Hercegovini. Prvih četrnaest godina svog života provodim u rodnom gradu i u njemu pohađam osnovnu školu "Branko Ćopić" te paralelno glazbenu školu u kojoj uz nastavu solfeđa učim svirati i gitaru. Kako poslovica kaže da je talent tek 1% a rad 99%, tako i moj talent za matematiku leži u tom intervalu od $[0, 1]$ i za njegovo otkriće ponajviše je zaslužna moja razrednica Bosiljka Majkić koja me uvodi u prvi mali svijet matematike, ljepote njene zakonitosti i izazova rješavanja zadataka. Predanim radom kroz osnovnu školu postala je skoro neodjeljivi dio mene, ili bolje ja neodjeljivi dio nje. To je, vjerujem, i imalo za posljedicu kasniji upis studija Matematike. Srednju školu pohađam u Banjoj Luki tj. Opću gimnaziju "Bl. Ivan Merz" pri Katoličkom školskom centru. U srpnju 2010 god. upisujem preddiplomski sveučilišni studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilita u Zagrebu, a 2014. diplomski sveučilišni studij Računarstvo i matematika.

Pored matematike, vrijeme volim posvećivati glazbi i književnosti i provoditi ga s ljudima.