ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.6 (2023) 1–14
https://doi.org/10.32817/amssd.6.1

Zaprimljen: 7. ožujka 2021.
Prihvaćen: 20. listopada 2023.

Metode za podjelu tajne temeljene na Kineskom teoremu o ostacima

Josipa Despotović, Borka Jadrijević

Sažetak

Adi Shamir i George Blakley su 1979. godine, neovisno jedan o drugome, osmislili prvu metodu za podjelu tajne, tzv. shemu praga. U ovom radu su opisane dvije sheme praga koje koriste Kineski teorem o ostacima, Mignotteova i Asmuth-Bloomova shema praga. Pokazano je Asmuth-Bloomova shema savršena, dok Mignotteova to nije. Obje metode ilustrirane su primjerima.

Ključni pojmovi: metode za podjelu tajne, Kineski teorem o ostacima, Mignotteova shema praga, Asmuth-Bloomova shema praga, savršena metoda

1. Uvod

Sva računala priključena na internet, od našeg pametnog telefona ili prijenosnog računala do poslužitelja koji poslužuju sadržaje za masovno posjećene internetske stranice za web-prodaju, pronalaze se i komuniciraju pomoću brojeva, tzv. *IP adresa*. Kada otvorimo web preglednik ne moramo pamtiti i unositi taj dugi broj, umjesto toga dovoljno je unijeti ime internetske domene kao što je npr. *pmfst.hr* i svejedno ćemo doći na pravo mjesto. DNS sustav (eng. *Domain Name System*) je globalno distribuirana usluga koja prevodi čovjeku pamtljiva imena poput *www.amazon.com,* u računalu čitljive numeričke IP adrese poput 80.237.232.142, koje računala koriste za međusobno povezivanje. No, ako netko uspije „oponašati" rad DNS-a i „uvjeriti" naše računalo da se primjerice *www.amazon.com* nalazi na nekoj drugoj IP adresi, nije teško

zamisliti s kakvim se sve problemima možemo suočiti. Kao zaštitu od ovakve vrste napada, uveden je DNSSEC - skup dodataka koji proširuju sigurnost DNS-a. DNSSEC koristi kriptografske algoritme i alate kako bi spriječio mogućnost zlonamjernog povezivanja IP adresa i domenskih imena. Kriptografske metode koje se koriste za provjeru autentičnosti DNS povezivanja svakako su vrlo zanimljive, ali je ključno pitanje kome se može povjeriti glavni kriptografski ključ sustava? Neprofitna organizacija ICANN odgovorna za takve situacije je odabrala sljedeći način: glavni ključ je podijeljen na sedam dijelova koji su na pametnim karticama dani sedmorici različitih ljudi koji se nalaze na geografski različitim mjestima i koji svoje kartice čuvaju u sefovima. Najmanje pet članova ove grupe, svaki sa svojim dijelom ključa, bi se moralo naći u centru za podatkovnu sigurnost u Sjedinjenim Američkim Državama da bi restartalo DNSSEC u slučaju da sustav padne.

"If you round up five of these guys, they can decrypt (the root key) should the West Coast fall in the water and the East Coast get hit by a nuclear bomb." Richard Lamb, voditelj DNSSEC programa u ICANN-u

Kako je moguće da *bilo kojih* 5 od 7 članova ove grupe mogu rekonstruirati glavni ključ, ali primjerice 4 člana od njih 7 to ne mogu? Rješenje leži u kriptografskim alatima koji se nazivaju *metode (sheme) za podjelu tajne*, a navedeni primjer, na jednostavan način, opisuje koncept *dijeljenja tajne*.

2. Podjela tajne

U mnogim situacijama potrebno je pohraniti i zaštiti neku visoko osjetljivu i vrlo važnu informaciju npr. lozinku za otvaranje trezora banke, ključ za šifriranje, kod za kontrolu pristupa nuklearnom oružju, tajni recept i sl. Svaka od ovih informacija mora se držati strogo povjerljivo, ali je također jako važno da se ne izgubi. Tradicionalne metode nisu prikladne za istodobno postizanje visoke razine povjerljivosti i pouzdanosti. To je zato što prilikom spremanja, recimo tajnog ključa za šifriranje, treba birati između čuvanja jedne kopije ključa na jednom mjestu radi maksimalne tajnosti i čuvanja više kopija ključa na različitim mjestima radi veće pouzdanosti. Povećavanjem pouzdanosti ključa pohranjivanjem više njegovih kopija očito se smanjuje se njegova povjerljivost jer ima više mogućnosti da kopija ključa padne u pogrešne ruke.

Metode ili sheme za podjelu tajne (eng. *secret sharing schemes*) rješavaju ovaj problem jer omogućuju proizvoljno visoku razinu povjerljivosti i pouzdanosti. One su zasnovane na sasvim drugačijoj ideji. Umjesto da se čuva više kopija tajne, tajna se dijeli s više osoba i to na način da

svatko dobije jedan dio te tajne, ali tako da nitko od sudionika podjele ne može pronaći tajnu koristeći samo svoj dio tajne. Ali ako dovoljan broj tih osoba udruži svoje djelove tajne, tajna se može potpuno rekonstruirati. U protivnom, nije moguće pronaći tajnu ili, još bolje, bilo kakvu informaciju o toj tajni.

Sheme za podjelu tajne su dakle metode koje se koriste za pohranu i skrivanje nekog važnog podatka, kojeg ćemo nazivati *tajna*, dijeljenjem te tajne na dijelove, koje ćemo nazivati *dionicama tajne* i njihovom raspodjelom određenim osobama, koje ćemo nazivati *sudionici podjele tajne*. Tajna se može rekonstruirati iz određenih podskupova dionica. Onoga tko bira tajnu, dijeli tajnu i dionice tajno distribuira sudionicima nazvamo *djelitelj tajne*. Dakle, bilo koja shema za podjelu tajne sastoji od sljedeća dva dijela:

- *Postupak raspodjele dionica*: Odabrana tajna S se dijeli, ovisno o metodi, na n dionica tajne: s_1, s_2, ..., s_n koje se onda tajno podijele sudionicima.
- *Postupak rekonstrukcije tajne:* Tajna se može rekonstruirati iz odgovarajućeg skupa dionica pomoću određenog algoritma (ovisno o metodi).

3. Sheme praga

Začetnici ideje podjele tajne su izraelski kriptograf *Adi Shamir* i američki kriptograf i matematičar *George Blakley*. Oni su 1979. godine, neovisno jedan o drugome, osmislili prvu metodu za podjelu tajne tzv. *shemu praga* (eng. *threshold scheme*) kao rješenje problema zaštite i sigurnosti kriptografskih ključeva. Tijekom godina razvile su se mnoge metode za podjelu tajne zasnovane na novim idejama i potrebama.

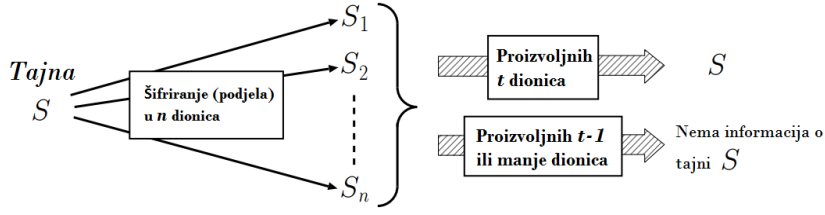
U svom radu *How to Share a Secret* [16] iz 1979. godine, Adi Shamir je objasnio koncept svoje ideje o $(t, n)-$shemi praga koju koristi kako bi efikasno podijelio tajnu na n dijelova. Označimo sa S tajnu koji djelitelj tajne $\mathcal{D}$ mora podijeliti unutar grupe $\mathcal{P}$ koja ima n članova tzv. sudionika podjele tajne. Pretpostavljamo da $\mathcal{D} \notin \mathcal{P}$. Djelitelj $\mathcal{D}$ dijeli tajnu S tako da svaki sudionik $P_i \in \mathcal{P}$, $i = 1, .., n$, dobije svoju dionicu tajne. Raspodjela dionica je tajna, odnosno niti jedan sudionik ne zna nikakvu informaciju o dionicama ostalih sudionika. Za rekonstrukciju izvorne tajne S nisu potrebne sve dionice tajne, nego Shamirova shema zahtijeva *minimalan* broj dionica i taj se minimum t naziva *pragom*. Imamo sljedeći neformalnu definiciju.

Definicija 1. *Neka su t i n prirodni brojevi, tako da je $t \leq n$. $(t, n)-$shema praga je metoda za podjelu tajne S između n sudionika podjele, tako*

da bilo kojih t sudionika može rekonstruirati tajnu S, ali bilo koji skup od $t-1$ (ili manje) sudionika ne može otkriti tajnu S.

Shema podjele tajne je *savršena* ako samo određeni podskupovi skupa sudionika mogu rekonstruirati tajnu, a preostali podskupovi ne mogu dobiti nikakvu informaciju o tajni. Dakle, u savršenom dijeljenju tajne je vrlo jasno naznačeno „tko zna što". Posebno, savršenu shemu praga definiramo na sljedeći način.

Definicija 2. *Za $(t,n)-$shemu praga kažemo da je savršena ako bilo koji skup od t sudionika podjele tajne može rekonstruirati tajnu S, dok bilo koji skup od $t-1$ (ili manje) sudionika ne može otkriti niti jednu informaciju o tajni S.*



Slika 1. Savršena $(t,n)-$shema praga

U bilo kojoj savršenoj shemi za podjelu tajne je veličina svake dionice tajne veća ili jednaka od veličine tajne. Primjerice, ako bi u $(t,n)-$shemi praga neki sudionik podjele tajne P_i imao dionicu tajne čija je veličina manja od veličine tajne, tada bi bilo kojih $t-1$ drugih sudionika imalo neke informacije o tajni jer bi se problem rekonstrukcije tajne s njihovih $t-1$ dionica, sveo na problem rekonstukcije dionice koju posjeduje sudionik P_i, a njena veličina je manja od veličine tajne. No, tada ta shema po defniciji ne bi bila savršena.

Kod implementacije shema za podjelu tajne u praksi, pohrana dionica može predstavljati značajan problem. Stoga je važno da veličina dionica bude što je moguće manja, tj. ako se radi o savršenoj shemi, da veličina dionica bude upravo jednaka veličini tajne.

Definicija 3. *Za metodu podjele tajne kažemo da je idealna ako je savršena i ako veličina svake dionice jednaka veličini tajne.*

Tvorci ideje $(t,n)-$sheme praga Shamir i Blakley su različito realizirali ideju praga. Shamirova shema koristi polinome i polinomnu interpolaciju, točnije Lagrangeovu interpolaciju za podjelu i rekonstrukciju tajne. U ovoj shemi dionice tajne su vijednosti slučajno generiranog polinoma stupnja $t-1$ nad konačnim poljem $\mathbb{Z}_p$ (p je prost broj) u n

slučajno odabranih različitih točaka iz $\mathbb{Z}_p$, a tajna je slobodni koeficijent tog polinoma. Blakley je koristio geometrijski pristup kako bi konstruirao $(t, n)-$shemu praga. On pretpostavlja da je tajna neka točka u $t-$dimenzionalnom prostoru nad konačnim poljem $\mathbb{Z}_p$ i da su dionice tajne n različitih međusobno neparalelnih hiperravnina koje prolaze kroz tu tajnu točku.

Kod Blakeyeve i Shamirove sheme, rekonstrukcija tajne, uz poznavanje t dionica tajne, se svodi na rješavanje sustava od t linearnih jednadžbi s t nepoznanica pa su obje ove sheme *linearne sheme praga*. Međutim, Blakleyeva metoda, za razliku od Shamirove, nije savršena jer bez obzira na to što $t-1$ hiperravnina (dionica tajne) nije dovoljno za rekonstrukciju tajne, one ipak daju dovoljno informacija o tajnoj točki budući znamo da ona leži u presjeku tih $t-1$ hiperravnina.

Shamirova shema, uz to što je savršena, ona je i idealna jer je veličina dionica jednaka veličini tajne (dionice tajne i sama tajna su iz skupa $\mathbb{Z}_p$).

U ovom radu nećemo se baviti Shamirovom i Blakleyevom metodom nego ćemo opisati dvije sheme praga koje koriste Kineski teorem o ostacima. Pokazat ćemo da je jedna od tih shema savršena, dok druga nije.

4. Kineski teorem o ostacima i dijeljenje tajne

Kineski teorem o ostacima je čest alat u kriptografiji. Njegovu primjenu možemo naći u brojnim kriptografskim algoritmima pa tako i u metodama za podjelu tajne koje ćemo u nastavku detaljnije opisati. No, prije toga, podsjetit ćemo se kako glasi Kineski teorem o ostacima.

Teorem 4 (**Kineski teorem o ostatcima**). *Neka su m_1, m_2, ..., m_t u parovima relativno prosti prirodni brojevi te neka su $a_1, a_2, ..., a_t$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \ldots, \quad x \equiv a_t \pmod{m_t} \qquad (1)$$

ima rješenje. Ako je x_0 jedno rješenje, onda su sva rješenja sustava dana s $x \equiv x_0 \pmod{m_1 m_2 \cdots m_t}$.

Ako su $m_1, m_2, ..., m_t$ u parovima relativno prosti prirodni brojevi, Kineski teorem o ostacima nam kaže da onda postoji jedinstveno rješenje sustava (1) koje se nalazi između 0 i $m_1 \cdots m_t - 1$, odnosno u skupu $\mathbb{Z}_{m_1 \cdots m_t}$. Sam dokaz Teorema 4 nam daje i način kako to rješenje pronaći (vidjeti npr. [2], str. 49). Ideja je da se konstruira shema koja će omogućiti da uz bilo kojih t dionica tajne S (u ovom slučaju ostataka od S modulo m_i) možemo otkriti traženu tajnu, dok s manje od t dionica to

ne možemo učiniti. Tajna se može rekonstruirati rješavanjem odgovarajućeg sustava od t linearnih kongruencija pomoću Kineskog teorema o ostatcima kako bi se dobilo jedinstveno rješenje tog sustava (u zadanom intervalu), koje je zapravo tražena tajna. Pogledajmo sada kako su korištenjem ove ideje konstruirane dvije metode za podjelu tajne, a to su *Mignotteova* i *Asmuth-Bloomova* shema praga.

4.1. Mignotteova shema praga

Mignotteova shema praga koristi poseban niz cijelih brojeva takozvani *Mignotteov niz*, koji se sastoji od n u parovima relativno prostih prirodnih brojeva takvih da je produkt t najmanjih od njih veći od trostrukog produkta $t-1$ najvećih među njima. Taj uvjet je jako važan jer se shema temelji na odabiru tajne kao cijelog broja između ta dva produkta. Ovaj uvjet također osigurava da je najmanje t dionica tajne potrebno za rekonstrukciju tajne, bez obzira na to koje su dionice odabrane.

Definicija 5. *Neka su dani prirodni brojevi n i t takvi da je $2 \leq t \leq n$. Za niz u parovima relativno prostih prirodnih brojeva $m_1 < m_2 < \cdots < m_n$ kažemo da je $(t, n)-$Mignotteov niz ako vrijedi*

$$3m_{n-t+2} \cdots m_n < m_1 \cdots m_t. \tag{2}$$

Mignotteovu shemu možemo opisati na sljedeći način:

Mignotteova $(t, n)-$shema praga

1. **Inicijalizacija.** Neka je dan $(t, n)-$Mignotteov niz $m_1 < m_2 < \cdots < m_n$ i neka je tajna S je slučajno odabran prirodan broj takav da je $\beta < S < \alpha$, gdje je $\alpha = m_1 \cdots m_t$ i $\beta = m_{n-t+2} \cdots m_n$.

2. **Raspodjela dionica.** Za svaki $i = 1, ..., n$, djelitelj tajne $\mathcal{D}$ računa vrijednosti $I_i = S \bmod m_i$ i daje dionicu tajne I_i sudioniku podjele P_i.

3. **Rekonstrukcija tajne.** Pomoću t različitih dionica tajne $I_{i_1}, \ldots, I_{i_t}$, tajna S se može rekonstruirati rješavanjem sustava kongruencija

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_t} \pmod{m_{i_t}} \tag{3}$$

korištenjem Kineskog teorema o ostacima. Tajna S je rješenje sustava (3) koje leži u skupu $\mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$.

Uočimo da, prema Teoremu 4, sustav kongruencija (3) ima točno jedno rješenje u skupu $\mathbb{Z}_{m_{i_1}\cdots m_{i_t}}$. Iz konstrukcije dionica I_i vidimo da je tajna S jedno rješenje sustava (3), no kako ono leži u $\mathbb{Z}_{m_{i_1}\cdots m_{i_t}}$ jer je $0 < \beta < S < \alpha \leq m_{i_1}\cdots m_{i_t}$, prema Teoremu 4, tajna S je jedino rješenje sustava (3) koje leži u $\mathbb{Z}_{m_{i_1}\cdots m_{i_t}}$. Stoga, tajnu S možemo rekonstruirati pomoću t različitih dionica tajne.

Pokažimo sada da se tajna S ne može otkriti s $t-1$ (ili manje) dionica. Pretpostavimo da tajnu S želimo rekonstruirati sa s dionica $I_{i_1}, \ldots, I_{i_s}$, za neke $i_1, \ldots, i_s \in \{1, 2, \ldots, n\}$, gdje je $1 \leq s \leq t-1$. Neka je x_0' jedinstveno rješenje sustava

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_s} \pmod{m_{i_s}}$$

u skupu $\mathbb{Z}_{m_{i_1}\cdots m_{i_s}}$. Očito je

$$S \equiv x_0' \pmod{m_{i_1}\cdots m_{i_s}}, \tag{4}$$

ali kako je

$$S > \beta = m_{n-t+2}\cdots m_n \geq m_{i_1}\cdots m_{i_s} > x_0',$$

onda je $S \neq x_0'$. Iz (4) slijedi da je S oblika $x_0' + km_{i_1}\cdots m_{i_s}$ za neki $k \in \mathbb{Z},\ k \neq 0$ takav da je $\beta < x_0' + km_{i_1}\cdots m_{i_s} < \alpha$, tako da postoji što više mogućih vrijednosti za tajnu S. Naime, kako je

$$1 < \frac{x_0'}{\beta} + k\frac{m_{i_1}\cdots m_{i_s}}{\beta} < \frac{\alpha}{\beta},$$

i $3\beta < \alpha$, onda postoje barem dvije moguće vrijednosti za tajnu S budući da je $\frac{\alpha-\beta}{\beta} = \frac{\alpha}{\beta} - 1 > 2$. Iz ovoga očito slijedi da $t-1$ (ili manje) sudionika ne može rekonstruirati tajnu S, ali ipak mogu dobiti nekakvu informaciju o toj tajni pa Mignotteova metoda je *nije savršena.* Zbog toga, kako bismo osigurali veću razinu sigurnosti, odgovarajući $(t, n)-$Mignotteov niz bi morao imati što veći faktor $\frac{\alpha-\beta}{\beta}$, tako da postoji što više mogućih vrijednosti za tajnu S ako se tajna želi rekonstruirati s manje od t dionica.

Uočimo da je kod Mignotteove metode svaka dionica I_i, $i = 1, ..., n$, puno manja od tajne S budući da vrijedi

$$0 \leq I_i < m_i \leq m_n \leq m_{n-t+2}\cdots m_n < S < m_1\cdots m_t.$$

Stoga, premda nije savršena, Mignotteova se metoda ipak koristi u primjenama i to u situacijama kada je veličina dionica odlučujući faktor.

Primjer 1. *Neka je zadan niz:* $m_1 = 11$, $m_2 = 13$, $m_3 = 17$, $m_4 = 19$, $m_5 = 23$. *Ovaj niz je* $(3, 5)$ - *Mignotteov niz budući da su brojevi* m_1, $..., m_5$ *u parovima relativno prosti prirodni brojevi i budući da je*

$$3\beta = 3m_4m_5 = 1311 < 2431 = m_1m_2m_3 = \alpha.$$

Neka je tajna $S = 1965$, *koja očito zadovoljava potreban uvjet* $\beta = 437 < S < 2431 = \alpha$. *Tada su pripadne dionice tajne redom*

$$I_1 = 1965 \bmod 11 = 7,\ I_2 = 1965 \bmod 13 = 2,\ I_3 = 1965 \bmod 17 = 10$$
$$I_4 = 1965 \bmod 19 = 8,\ I_5 = 1965 \bmod 23 = 10.$$

Pomoću tri različite dionice možemo rekonstruirati tajnu S. *Odaberimo dionice* I_1, I_3 *i* I_4. *Pomoću Kineskog teorema o ostacima rješavamo sustav kongruencija*

$$x \equiv 7 \pmod{11},\ x \equiv 10 \pmod{17},\ x \equiv 8 \pmod{19}. \tag{5}$$

Neka je $N = 11 \cdot 17 \cdot 19 = 3553$, $N_1 = 17 \cdot 19 = 323$, $N_2 = 11 \cdot 19 = 209$ *te* $N_3 = 11 \cdot 17 = 187$. *Tada je jedno rješenje sustava (5) oblika*

$$x_0 = 323x_1 + 209x_2 + 187x_3,$$

gdje x_1, x_2, x_3 *zadovoljavaju*

$$323x_1 \equiv 7 \pmod{11}, \quad 209x_2 \equiv 10 \pmod{17}, \quad 187x_3 \equiv 8 \pmod{19},$$

odnosno

$$4x_1 \equiv 7 \pmod{11}, \quad 5x_2 \equiv 10 \pmod{17}, \quad 16x_3 \equiv 8 \pmod{19}.$$

Rješavanjem linearnih kongruencija dobivamo da je $x_1 = 10$, $x_2 = 2$, $x_3 = 10$ *pa je*

$$x_0 = 323 \cdot 10 + 209 \cdot 2 + 187 \cdot 10 = 5518.$$

Stoga su sva rješenja sustava (5) dana s

$$x \equiv 5518 \equiv 1965 \pmod{3553}.$$

Budući da je $1965 \in \mathbb{Z}_{3553}$, *onda je tajna* $S = 1965$. *Uočimo da su sva rješenja sustava (5) dana s* $x_k = 1965 + 3553k$, $k \in \mathbb{Z}$, *a mi tražimo ono koje se nalazi u intervalu* $(437, 2431)$ *i to je očito samo* $x_0 = 1965$. *Pretpostavimo sada da tajnu* S *želimo rekonstruirati pomoću dionica* I_4 *i* I_5. *Rješavanjem sustava*

$$x \equiv 8 \pmod{19},\ x \equiv 10 \pmod{23}$$

dobili bismo da je $S \equiv 217 \pmod{437}$. *Iz ovoga vidimo da se tajna* S *nalazi u skupu*

$$\begin{aligned} & \{217 + 437k : 437 < 217 + 437k < 3553,\ k \in \mathbb{Z}\} \\ = \ & \{654,\ 1091,\ 1528,\ 1965,\ 2402,\ 2839,\ 3276\}. \end{aligned}$$

Dakle, sudionici podjele tajne P_4 *i* P_5 *ne mogu rekonstruirati tajnu* S, *ali ipak mogu dobiti neke informacije o toj tajni.*

Mignotteovu shemu podjele tajni možemo poopćiti pomoću *generaliziranog Mignotteovog niza* čiji članovi nisu nužno u parovima relativno prosti. U tom slučaju, za rekonstrukciju tajne, koristi se općenitija verzija Kineskog teorema o ostacima, a shema se konstruira isto kao $(t, n)-$Mignotteova shema.

Napomena 6. *U više korištenih literaturnih naslova (npr. [1], [3], [4], [5], [7], [6], [12], [20], [21]) u definiciji* $(t, n)-$*Mignotteova niza (vidjeti Definiciju 5) umjesto uvjeta (2) imamo uvjet*

$$m_{n-t+2} \cdots m_n < m_1 \cdots m_t, \tag{6}$$

što bi povlačilo da se u Mignotteovim $(t, n)-$*shemama praga kod kojih je* $\beta < \alpha \leq 3\beta$, *tajna može rekonstruirati i s manje od* t *dionica. Primjerice, niz* $m_1 = 3$, $m_2 = 5$, $m_3 = 11$ *za* $t = 2$ *zadovoljava uvjet (6), ali ne zadovoljava uvjet (2) pa je dovoljno znati npr. dionicu tajne* $I_3 = S \bmod 11$ *za rekonstrukciju tajne* S.

4.2. Asmuth-Bloomova shema praga

Asmuth-Bloom shemu podjele tajne predložili su 1983. godine Asmuth i Bloom i ona se također temelji na Kineskom teoremu o ostacima. Za razliku od Mignotteove $(t, n)-$sheme praga, za koju smo zaključili da nije savršena, Asmuth-Bloomova shema je *savršena.*

Asmuth-Bloomova shema praga također koristi specijalan niz cijelih brojeva kojeg definiramo na sljedeći način.

Definicija 7. *Neka su* t *i* n *prirodni brojevi takvi da je* $2 \leq t \leq n$ *i neka su* $r, m_1, m_2, \ldots, m_n$ *u parovima relativno prosti prirodni brojevi takvi da je* $m_1 < m_2 < \ldots < m_n$. *Kažemo da je taj niz* $(t, n)-$*Asmuth-Bloomov niz ako vrijedi*

$$r \cdot m_{n-t+2} \cdots m_n < m_1 \cdots m_t. \tag{7}$$

Opišimo sada Asmuth-Bloomovu shemu praga.

Asmuth-Bloomova $(t, n)-$shema praga

1. **Inicijalizacija.** Neka je dan $(t, n)-$Asmuth-Bloomov niz r, m_1, m_2, ... , m_n i neka je tajna S neki element iz skupa $\mathbb{Z}_r$.

2. **Raspodjela dionica.** Za svaki $i = 1, ..., n$, djelitelj tajne $\mathcal{D}$ računa vrijednosti $I_i = (S + \gamma \cdot r) \bmod m_i$, gdje je γ tajni cijeli broj kojeg bira $\mathcal{D}$ i za kojeg vrijedi

$$0 < S + \gamma \cdot r < \prod_{i=1}^{t} m_i$$

te daje dionicu I_i sudioniku P_i.

3. **Rekonstrukcija tajne.** Pomoću t različitih dionica tajne $I_{i_1}, \ldots, I_{i_t}$, korištenjem Kineskog teorema o ostacima, nađemo jedinstveno rješenje $x_0 \in \mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$ sustava

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_t} \pmod{m_{i_t}}. \tag{8}$$

Tada je tajna $S = x_0 \bmod r$.

Uočimo da je $S + \gamma \cdot r$ jedno rješenje sustava (8). No, kako je

$$0 < S + \gamma \cdot r < m_1 \cdots m_t \leq m_{i_1} \cdots m_{i_t},$$

onda je i $S + \gamma \cdot r \in \mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$ pa je, po Teoremu 4, $S + \gamma \cdot r = x_0$. Stoga je $x_0 \bmod r = S$.

Pokažimo sada da je Asmuth-Bloomova shema savršena. Pretpostavimo da tajnu S želimo rekonstruirati s $t - 1$ dionica $I_{i_1}, \ldots, I_{i_{t-1}}$, za neke $i_1, \ldots, i_{t-1} \in \{1, 2, \ldots, n\}$. Neka je x_0' jedinstveno rješenje sustava

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_{t-1}} \pmod{m_{i_{t-1}}} \tag{9}$$

u skupu $\mathbb{Z}_{m_{i_1} \cdots m_{i_{t-1}}}$. Budući da je $m_{i_1} \cdots m_{i_{t-1}} \leq m_{n-t+2} \cdots m_n$, iz (7) slijedi da je

$$r \cdot m_{i_1} \cdots m_{i_{t-1}} < m_1 \cdots m_t$$

pa je

$$x_0' + j m_{i_1} \cdots m_{i_{t-1}} < m_1 \cdots m_t \text{ za } 0 \leq j < r.$$

Budući da je $nzd\left(r, m_{i_1} \cdots m_{i_{t-1}}\right) = 1$, brojevi $S_j \in \mathbb{Z}_r$, $0 \leq j < r$, definirani s

$$S_j = \left(x_0' + j m_{i_1} \cdots m_{i_{t-1}}\right) \bmod r, \tag{10}$$

su svi različiti, a kako ih ima r, onda je $\{S_j : 0 \leq j < r\} = \mathbb{Z}_r$. Na taj način smo pokazali da uz poznavanje $t-1$ dionica tajne, svaki element iz $\mathbb{Z}_r$ može biti tajna S. Naime, iz (10) slijedi da za svaki j, $0 \leq j < r$ postoji $\gamma_j \in \mathbb{Z}$ takav da je $S_j + \gamma_j \cdot r = x_0' + jm_{i_1} \cdots m_{i_{t-1}}$. Tada je

$$S_j + \gamma_j \cdot r \equiv x_0' \pmod{m_{i_1} \cdots m_{i_{t-1}}},$$

pa je $S_j + \gamma_j \cdot r$ rješenje sustava (9) za koje vrijedi

$$\begin{aligned} 0 &< S_j + \gamma_j \cdot r = x_0' + jm_{i_1} \cdots m_{i_{t-1}} < (j+1)\, m_{i_1} \cdots m_{i_{t-1}} \\ &\leq rm_{i_1} \cdots m_{i_{t-1}} < m_1 \cdots m_t, \end{aligned}$$

što pokazuje da svaki S_j, $0 \leq j < r$, može biti tajna. Stoga, bilo kojih $t-1$ sudionika ne može otkriti tajnu S te niti jednu informaciju o toj tajni, što znači da je Asmuth-Bloomova shema savršena. Razlog tome je odabir cijelog broja γ koji je neovisan o tajni S.

Može se pokazati da je kod Asmuth-Bloomova sheme veličina dionica veća od veličine tajne (posebno za dovoljno male module $m_1, m_2, \ldots, m_n$), stoga Asmuth-Bloomova shema nije idealna. Ali je pokazano da je Asmuth-Bloomova shema s modulima koji su uzastopni prosti brojevi *asimptotski idealna.*

Primjer 2. *Neka su zadani u parovima relativno prosti prirodni brojevi:* $r = 3, m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19$. *Primijetimo da vrijedi*

$$r \cdot m_3 \cdot m_4 = 3 \cdot 17 \cdot 19 < 11 \cdot 13 \cdot 17 = m_1 \cdot m_2 \cdot m_3,$$

stoga je navedeni niz $(3,4)$*-Asmuth-Bloomov niz.*
Neka je tajna $S = 2 \in \mathbb{Z}_3$. *Odaberimo tajni cijeli broj* γ *za kojeg vrijedi*

$$0 < 2 + \gamma \cdot 3 < m_1 \cdot m_2 \cdot m_3 = 2431.$$

Neka je $\gamma = 51$. *Tada je* $S + \gamma \cdot r = 2 + 51 \cdot 3 = 155$ *pa su pripadne dionice redom*

$$\begin{aligned} I_1 &= 155 \bmod 11 = 1, \quad & I_2 &= 155 \bmod 13 = 12, \\ I_3 &= 155 \bmod 17 = 2, \quad & I_4 &= 155 \bmod 19 = 3. \end{aligned}$$

Tajnu možemo rekonstruirati koristeći bilo koje tri dionice korištenjem Kineskog teorema o ostatcima. Uzmimo dionice $I_1 = 1, I_2 = 12$ *i* $I_3 = 2$. *Odgovarajući sustav kongruencija je*

$$x \equiv 1 \pmod{11}, \quad x \equiv 12 \pmod{13}, \quad x \equiv 2 \pmod{17}. \tag{11}$$

Sva rješenja sustava su dana s

$$x \equiv 5017 \equiv 155 \pmod{2431}$$

pa je $S + 3\gamma = 155$. *Stoga je tajna* $S = 155 \bmod 3 = 2$.

Pretpostavimo sada da tajnu S *želimo rekonstruirati pomoću dionica* I_1 *i* I_4. *Rješavanjem sustava*

$$x \equiv 1 \pmod{11},\ x \equiv 3 \pmod{19}$$

dobili bismo da je $S+3\gamma \equiv 155 \pmod{209}$. *Stoga je* $S+3\gamma = 155+209k$, *za neki* $k \in \{0, 1, ..., 10\}$ *jer je* $0 < S + 3\gamma < 2431$. *Kako je* $S \in \mathbb{Z}_3$ *dovoljno je promatrati* $k = 0, 1, 2$, *da bismo uočili kako za svaki* $S \in \mathbb{Z}_3$ *postoji* $\gamma \in \mathbb{Z}$ *takav da je* $S + 3\gamma = 155 + 209k$. *Za* $k = 0, 1, 2$, *redom dobivamo* $(S, \gamma) = (2, 51)\,,\ (1, 121)\,,\ (0, 191)\,$. *Ovo pokazuje da dva sudionika ne mogu otkriti tajnu* S *te niti jednu informaciju o toj tajni jer svaki element iz* $\mathbb{Z}_3$ *može biti tajna.*

I Asmuth-Bloomova metoda se može poopćiti tako da se promatra *generalizirani Asmuth-Bloomov* kod kojeg prirodni brojevi $r, m_1, m_2, \ldots, m_n$ ne moraju nužno biti u parovima relativno prosti.

Zahvala Autorice zahvaljuju anonimnom recezentu na uočenoj grešci u poglavlju 4.1 koja se javlja i u više korištenih literaturnih naslova (vidjeti Napomenu 6). Njegove/Njezine sugestije su bitno poboljšale prvu verziju rukopisa.

Literatura

[1] J. Despotović, *Metode za podjelu tajne*, diplomski rad, Prirodoslovno-matematički fakultet u Splitu, Split, 2021.

[2] A. Dujella, Teorija brojeva, Školska knjiga, Zagreb, 2019.

[3] A. Endurthi, O. B. Chanu, A. N. Tentu, V. C. Venkaiah, *Reusable Multi-Stage Multi-Secret Sharing Schemes Based on CRT*, Journal of Communications Software and Systems, **11(1)** (2015), 15-24.

[4] L. Harn, M. Fuyou, *Multilevel threshold secret sharing based on the chinese remainder theorem*. Information processing letters **114(9)** (2014), 504-509

[5] L. Harn, M. Fuyou, C-C. Chang: *Verifiable secret sharing based on the Chinese remainder theorem*, Security Comm. Networks **7** (2014)., 950–957.

[6] S. Iftene, *General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting*, Electronic Notes in Theoretical Computer Science, **186** (2007), 67-84.

[7] S. Iftene, I. C. Boureanu, *Weighted threshold secret sharing based on the Chinese remainder theorem.* Sci. Ann. Cuza Univ. **15** (2005), 161–172

[8] K. Kaya, A. A. Selcuk, Z. Tezcan, *Threshold Cryptography Based on Asmuth-Bloom Secret Sharing*, Computer and Information Sciences - ISCIS 2006, Lecture Notes in Computer Science, **4263** (2006), 935-942, Springer, Berlin, Heidelberg.

[9] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[10] M. Mignotte, *How to Share a Secret.* In: Beth, T. (eds) Cryptography. EUROCRYPT 1982. Lecture Notes in Computer Science, vol **149** (1983), 371-375, Springer, Berlin, Heidelberg.

[11] Y. Ning, F. Miao, W. Huang, K. Meng, Y. Xiong, X. Wang., *Constructing Ideal Secret Sharing Schemes Based on Chinese Remainder Theorem*, Advances in Cryptology - ASIACRYPT 2018, Lecture Notes in Computer Science, **11274** (2018), 310-331, Springer, Cham.

[12] D. Pasaila, V. Alexa, S. Iftene, *Cheating Detection And Cheater Identification in CRT-Based Secret Sharing Schemes*, Computing, **9 (2)** (2010), 107-117.

[13] M. Quisquater, B. Preneel, J. Vandewalle, *On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem*, Public Key Cryptography, Lecture Notes in Computer Science, **2274** (2002), 199-210, Springer, Berlin, Heidelberg.

[14] M. Rosulek, *The Joy of Cryptography, Chapter 3. Secret Sharing*, skripta preddiplomskog kolegija. Preuzeto 20.10.2020. s

`https://web.engr.oregonstate.edu/~rosulekm/crypto/chap3.pdf`

[15] K. N. Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari, *A Review of Secret Sharing Schemes*, Research Journal of Information Technology, **5** (2013), 67-72.

[16] A. Shamir, *How to share a secret*, Communications of the ACM **22** (1979), 612-613.

[17] D. R. Stinson, Cryptography: Theory and Practice. 3rd edition. Chapman and Hall/CRC, Taylor and Francis Group, 2006.

[18] *Secret sharing.* (bez dat.). U Wikipedia. Preuzeto 12.10.2020. s `https://en.wikipedia.org/wiki/Secret_sharing`

[19] *Shamir's Secret Sharing.* (bez dat.). U Wikipedija. Preuzeto 12.10.2020. s https://en.wikipedia.org/wiki/Shamir%27s_-Secret_Sharing

[20] *Secret sharing using the Chinese remainder theorem.* (bez dat.). U Wikipedija. Preuzeto 12.10.2020. s https://en.wikipedia.org/wiki/Secret_sharing_using_-the_Chinese_remainder_theorem

[21] *Secret Shares with CRT (Mignotte threshold secret sharing)* (bez dat.). Preuzeto 10.10.2023. s https://asecuritysite.com/shares/sss_crt2

Josipa Despotović
studentica, Sveučilište u Splitu, Prirodoslovno-matematički fakultet, Ruđera Boškovića 33, Split
E-mail adresa: jdespotov@pmfst.hr

Borka Jadrijević
Sveučilište u Splitu, Prirodoslovno-matematički fakultet, Ruđera Boškovića 33, Split
E-mail adresa: borka@pmfst.hr