Savršena sigurnost u kriptografiji

Majin, Ena

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ena Majin

SAVRŠENA SIGURNOST U KRIPTOGRAFIJI

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, rujan 2022.

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. _____

Sadržaj

Sadržaj **iii**

Uvod **1**

1 Savršena sigurnost **3**
1.1 Potreba za definicijom 3
1.2 Claude Shannonova teorija komunikacije 3
1.3 Uvodne definicije i teoremi iz teorije vjerojatnosti 5
1.4 Definicija savršene sigurnosti 5
1.5 Primjer šifre koja nije savršeno sigurna 6
1.6 Shannonova karakterizacija savršene sigurnosti 7

2 Jednokratna bilježnica **11**
2.1 Definicija jednokratne bilježnice 11
2.2 Nastanak jednokratne bilježnice 12
2.3 Dokaz savršene sigurnosti Vernamove jednokratne bilježnice 13
2.4 Nedostatci jednokratne bilježnice 14

3 Entropija **17**
3.1 Definicija i primjeri 17
3.2 Uvjetna entropija 22

4 Veza entropije i savršene sigurnosti **25**
4.1 Drugi zahtjev Shannonovog teorema 25
4.2 Višeznačnost ključa 25
4.3 Prvi zahtjev Shannonovog teorema 27
4.4 Maksimalna entropija kriptosustava 27

Bibliografija **29**

Uvod

U ovom radu bavit ćemo se savršenom sigurnosti u kriptografiji.

U prvom poglavlju ćemo definirati savršenu sigurnost i reći nešto o znanstveniku koji je donio tu definiciju. Zatim ćemo dati primjer šifre koja nije savršeno sigurna i na kraju dokazati Shannonov teorem o nužnim i dovoljnim uvjetima savršene sigurnosti. Za ovo poglavlje ćemo uglavnom koristiti literaturu [4] i [2] za definicije, iskaze i neke primjere. Koristit ćemo i članak [7] za priču o Shannonu, ocu teorije komunikacije.

U drugom poglavlju ćemo iznijeti definicije i iskaze koji će nam biti potrebni u ostatku rada. Koristit ćemo definicije i iskaze iz [5]. Zatim ćemo govoriti o Vernamovoj jednokratnoj bilježnici, najpoznatijoj savršeno sigurnoj šifri. Definirat ćemo ju, ispričati priču o njenom nastanku i dokazati njenu savršenu sigurnost. Također ćemo navesti razloge zašto se jednokratna bilježnica u stvarnosti ne koristi često. U ovom poglavlju su također glavne literature [4] i [2].

Treće poglavlje bavit će se pojmom entropije oslanjajući se na [4]. Vidjet ćemo nekoliko primjera koji služe za približavanje pojma i stvaranje intuicije. Navest ćemo i razna svojstva entropije i uvjetne entropije.

U četvrtom poglavlju ćemo povezati ono što smo naučili o entropiji s onim što znamo o savršenoj sigurnosti. Definirat ćemo višeznačnost ključa. I vidjet ćemo da se upravo entropija nalazi u pozadini zahtjeva Shannonovog teorema. I u ovom poglavlju glavna je literatura [4].

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Savršena sigurnost

1.1 Potreba za definicijom

Kriptirana komunikacija uglavnom služi jednom cilju - omogućavanju sigurne komunikacije bez straha od prisluškivanja. U takvoj komunikaciji uvijek postoje dva tipa kriptoanalitičara, jedni koji šifriraju poruku kako bi ju zaštitili i drugi koji tu poruku žele dešifrirati.

Metode dešifriranja poruke nazivamo napadima i dijelimo ih u četiri grupe: *napad samo šifrat*, *napad poznat otvoreni tekst*, *napad odabrani otvoreni tekst* i *napad odabrani šifrat*. Za svrhe ovog rada najzanimljiviji je *napad samo šifrat*, odnosno napad u kojemu kriptoanalitičar ima pristup šifratu te pokušava saznati otvoreni tekst iz kojega je taj šifrat dobiven. Pri tome pretpostavljamo da kriptoanalitičar ima neograničena sredstva i alate koje može koristiti za izvršavanje napada.

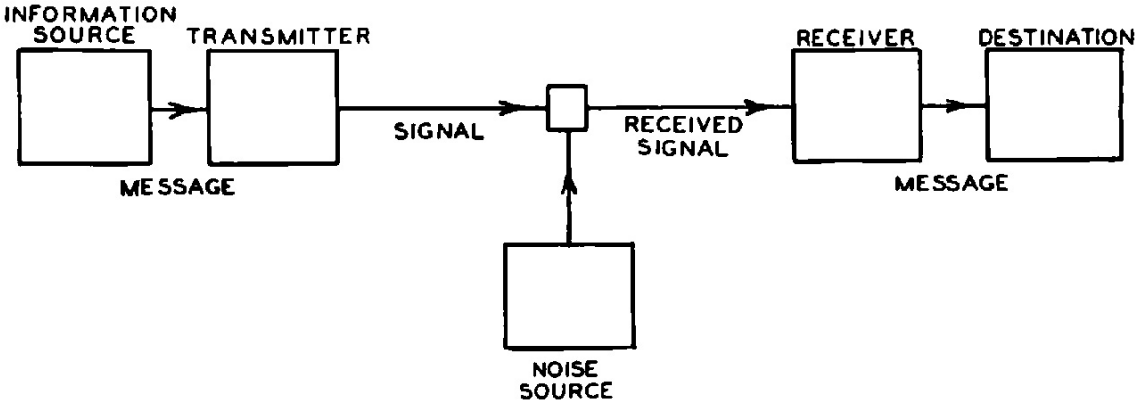
Dok su kriptoanalitičari špijuni razrađivali metode za dešifriranje, druga strana je osmišljala nove šifre. Pokušavali su kreirati šifru otpornu na napade kako bi postigli potpuno sigurnu komunikaciju. Naime, to nije jednostavan zadatak. Više puta se za neku šifru tvrdilo da je neprobojna, ali s vremenom bi se obično pokazalo suprotno. Nakon takvih pogrešnih tvrdnji postala je očita potreba za definicijom "neprobojne" šifre. Tu se istaknuo Claude Shannon, matematičar i inženjer koji je sredinom dvadesetog stoljeća, između ostalog, donio definiciju *savršene sigurnosti*.

1.2 Claude Shannonova teorija komunikacije

Claude E. Shannon rođen je 1916. godine, odrastao je u Gaylordu, Michigan, diplomirao je matematiku i elektrotehniku na Sveučilištu Michigan, zatim magistrirao na sveučilištu Massachusetts Institute of Technology. U magistarskom radu je primijenio Booleovu algebru na digitalne sklopove i tako postao jedan od začetnika dizajna digitalnih sklopova. Nakon studija je većinu života radio za (ili u suradnji s) *Bells Laboratories* gdje je radio

na poboljšanju komunikacije telefonom. Osim u vrijeme Drugog svjetskog rata kada je pauzirao rad u *Bell Laboratories* kako bi koristio svoju stručnost za aktivno sudjelovanje u obrani SAD-a. U životu je dva puta nominiran za Nobelovu nagradu za fiziku, a danas je poznat kao otac teorije informacija.

Njegov najpoznatiji rad je članak iz 1948. godine, *Matematička teorija komunikacije [6]*, u kojemu je izdvojio osnovne elemente komunikacije: izvor komunikacije, odašiljač, kanal preko kojeg se odvija komunikacija, prijemnik i odredište. To je donijelo veliki preokret jer su inženjeri prije Shannona komunikaciju promatrali ovisno o mediju preko kojega se izvodila, a sada su ju mogli apstraktizirati.



Slika 1.1: Shannonov graf komunikacije objavljen u časopisu The Bell System Technical Journal

Glavna tema rada bilo je određivanje minimalnog kapaciteta kanala za komunikaciju koji može prenijeti signal bez gubitka informacija.

Godinu dana kasnije, izdao je novi rad, *Matematička teorija kriptografije*, u kojemu se bavi sigurnim kriptosustavima. Na tome je počeo raditi još ranije, dok je razvijao šifre za korištenje u Drugom svjetskom ratu. U ovom radu je iznio temeljne koncepte za kriptografiju i savršeno sigurne sustave u tri dijela. Prvi dio se bavio osnovnom matematičkom strukturom kriptosustava, drugi dio savršenom sigurnošću, a treći kriptografijom u praksi. Za kriptografiju u praksi nudi načine koji osiguravaju da se kriptosustav, koji nije savršeno siguran, što više osigura od razbijanja tako što uvelike komplicira pronalazak ključa čak i onda kada se zna da jedinstveni ključ nije nemoguće pronaći.

1.3 Uvodne definicije i teoremi iz teorije vjerojatnosti

Definicija savršene sigurnosti se temelji na uvjetnim vjerojatnostima. U ovom poglavlju ćemo se prisjetiti nekih pojmova koji će nam biti potrebni za bolje razumijevanje daljnjeg teksta. Sve definicije i teoremi koji su ovdje iskazani mogu se pronaći u [5].

Definicija 1.3.1 (Uvjetna vjerojatnost)**.** *Neka je* $(\Omega, \mathcal{F}, \mathbb{P})$ *proizvoljan vjerojatnosni prostor i* $A \in \mathcal{F}$ *takav da je* $\mathbb{P}(A) > 0$*. Definirajmo funkciju* $\mathbb{P}_A : \mathcal{F} \to [0,1]$ *ovako:*

$$\mathbb{P}_A(B) := \mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)},\ B \in \mathcal{F}.$$

Lako je provjeriti da je $\mathbb{P}_A$ *vjerojatnost na* $\mathcal{F}$ *i nju zovemo* ***uvjetna vjerojatnost uz uvjet A****. Broj* $\mathbb{P}(B \mid A)$ *zovemo* ***vjerojatnost od B uz uvjet da se A dogodio*** *ili, kraće,* ***vjerojatnost od B uz uvjet A****.*

Definicija 1.3.2 (Potpun sistem događaja)**.** *Konačna ili prebrojiva familija* $(H_i, i = 1, 2, \ldots)$ *događaja u vjerojatnosnom prostoru* $(\Omega, \mathcal{F}, \mathbb{P})$ *jest* ***potpun sistem događaja*** *ako je* $H_i \neq \emptyset$ *za svako i,* $H_i \cap H_j = \emptyset$ *za* $i \neq j$ *(tj. događaji* H_i *uzajamno se isključuju) i* $\bigcup_i H_i = \Omega$*.*

Drugim riječima, potpun sistem događaja konačna je ili prebrojiva particija skupa Ω *s tim da su elementi particije događaji.*

Teorem 1.3.3 (Formula potpune vjerojatnosti)**.** *Neka je* $(H_i, i = 1, 2, \ldots)$ *potpun sistem događaja u vjerojatnosnom prostoru* $(\Omega, \mathcal{F}, \mathbb{P})$*. Tada za proizvoljno* $A \in \mathcal{F}$ *vrijedi*

$$\mathbb{P}(A) = \sum_i \mathbb{P}(H_i)\mathbb{P}(A \mid H_i). \tag{1.1}$$

Teorem 1.3.4 (Bayesova formula)**.** *Neka je* $(H_i, i = 1, 2, \ldots)$ *potpun sistem događaja u vjerojatnosnom prostoru* $(\Omega, \mathcal{F}, \mathbb{P})$ *i* $A \in \mathcal{F}$ *takav da je* $\mathbb{P}(A) > 0$*. Tada za svako i vrijedi*

$$\mathbb{P}(H_i \mid A) = \frac{\mathbb{P}(H_i)\,\mathbb{P}(A \mid H_i)}{\sum_j \mathbb{P}(H_j)\,\mathbb{P}(A \mid H_j)}.$$

1.4 Definicija savršene sigurnosti

Da bismo definirali savršenu sigurnost, prvo moramo iznijeti preciznu definiciju za kriptosustave, odnosno šifre, kako smo ih do sada nazivali. Koristit ćemo definiciju i popratnu napomenu iz [2].

Definicija 1.4.1. ***Kriptosustav*** *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, gdje je* $\mathcal{P}$ *konačan skup svih mogućih osnovnih elemenata otvorenog teksta,* $\mathcal{C}$ *konačan skup svih mogućih osnovnih*

elemenata šifrata, $\mathcal{K}$ konačan skup svih mogućih ključeva, $\mathcal{E}$ skup svih funkcija šifriranja i $\mathcal{D}$ skup svih funkcija dešifriranja.

Za svaki $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : \mathcal{P} \to C$ i $d_K : C \to \mathcal{P}$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki $x \in \mathcal{P}$.

Sljedeća lema pokazuje jedno bitno svojstvo kriptosustava.

Lema 1.4.2. *Svaka funkcija šifriranja e_K je injekcija.*

Dokaz. Pretpostavimo suprotno, neka je e_K funkcija šifriranja za koju postoje $x_1, x_2 \in \mathcal{P}$ takvi da $x_1 \neq x_2$ i $e_K(x_1) = y$, $e_K(x_2) = y$ za neki $y \in C$. Primijetimo da je iz ovako definirane funkcije šifriranja nemoguće odrediti otvoreni tekst iz šifrata y, jer bi mogao biti x_1 ili x_2. Dakle, svojstvo $d_K(e_K(x)) = x$ je narušeno. □

Proučavajući kriptosustave, Shannon je primijetio da kriptosustav ne može biti siguran ako se iz šifrata može saznati bilo što o otvorenom tekstu iz kojega je dobiven. Drugim riječima, i najmanja informacija o otvorenom tekstu je dovoljna da naruši sigurnost kriptosustava. Dakle, da bi kriptosustav bio savršeno siguran, otvoreni tekst ne smije biti ništa poznatiji nakon proučavanja šifrata nego što je bio prije.

Shannon je ovu tvrdnju zapisao u terminima vjerojatnosti i iznio sljedeću definiciju.

Definicija 1.4.3. *Neka je $S = (\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kriptosustav. Pretpostavimo da se u prostoru otvorenih tekstova $\mathcal{P}$ otvoreni tekst x pojavljuje s vjerojatnošću $\mathbb{P}(x)$ te da se u prostoru šifrata C šifrat y pojavljuje sa vjerojatnošću $\mathbb{P}(y)$. Kažemo da je kriptostustav S **savršeno siguran** ako vrijedi:*

$$(\forall x \in \mathcal{P})\,(\forall y \in C) \quad \mathbb{P}(x \mid y) = \mathbb{P}(x).$$

1.5 Primjer šifre koja nije savršeno sigurna

Neke od poznatijih vrsta šifri iz klasične kriptografije su supstitucijske šifre. One su i jedne od najstarijih šifri koje su se ikad koristile, a najpoznatija od njih je Cezarova šifra. Dugo su se razvijala poboljšanja supstitucijskih šifri u nadi da će se neka od njih pokazati neprobojnom, ali s vremenom su sve razbijene. Sada ćemo dokazati da takve šifre ne mogu biti savršeno sigurne. Za početak, definirajmo supstitucijsku šifru.

Definicija 1.5.1. *Neka je $S = (\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kriptosustav i $\mathcal{P} = C = \mathcal{K} = \mathbb{Z}_{26}$. Prostor ključeva $\mathcal{K}$ se sastoji od svih permutacija skupa $\{0, 1, 2, \ldots, 25\}$. Za svaku permutaciju $\pi \in \mathcal{K}$ definiramo **supstitucijsku šifru** sa*

$$e_\pi(x) = \pi(x), \quad d_\pi(y) = \pi^{-1}(y),$$

gdje je π^{-1} inverzna permutacija od π.

Šifra je definirana nad $\mathbb{Z}_{26}$ jer koristimo 26 slova engleske abecede te svako slovo ima svoj numerički ekvivalent.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Primijetimo da se šifriranje vrši tako da se svako slovo zamijeni nekim drugim slovom, ili istim, ovisno o odabranoj permutaciji. Već intuitivno možemo vidjeti da ovo nije savršeno sigurna šifra. Ako uzmemo šifrat u kojemu se uzastopno ponavlja isto slovo, jasno je da je taj šifrat morao doći iz otvorenog teksta koji također sadrži neko uzastopno ponovljeno slovo. Na ovaj način smo iz šifrata vrlo lako dobili informaciju o otvorenom tekstu. Sada ćemo samo pokazati istu stvar eksplicitnim primjerom.

Primjer 1.5.2. *Neka je $S = (\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kriptosustav supstitucijskih šifri, $\mathcal{P} = C = \mathcal{K} = \mathbb{Z}_{26}$ i neka je vjerojatnosna distribucija nad $\mathcal{P}$ za otvorene tekstove duljine 2 dana sa*

$$\mathbb{P}(AA) = \frac{1}{2}, \quad \mathbb{P}(AB) = \frac{1}{2}.$$

Jednostavnosti radi, pretpostavimo da je vjerojatnost svih ostalih otvorenih tekstova duljine 2 jednaka nuli.

Uzmimo otvoreni tekst $x = AB$ i šifrat $y = CC$. Očito je $\mathbb{P}(AB \mid CC) = 0$ jer šifrat CC nikako ne može biti dobiven iz otvorenog teksta AB. Očito vrijedi

$$\mathbb{P}(AB \mid CC) = 0 \neq \frac{1}{2} = \mathbb{P}(AB).$$

Prema tome, S nije savršeno siguran jer ne zadovoljava definiciju 1.4.3.

1.6 Shannonova karakterizacija savršene sigurnosti

Shannon je u *Matematičkoj teoriji kriptografije* iskazao i sljedeći teorem koji daje nužne i dovoljne uvjete za garantiranje savršene sigurnosti.

Teorem 1.6.1. *Neka je $S = (\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kriptosustav za koji vrijedi $|C| = |\mathcal{K}|$ i $\mathbb{P}(x) > 0$ za svaki $x \in \mathcal{P}$. Tada je S savršeno siguran ako i samo ako vrijedi:*

1. *za svaki $x \in \mathcal{P}$ i za svaki $y \in C$, postoji jedinstveni ključ $K \in \mathcal{K}$ takav da $e_K(x) = y$*

2. *ključevi u $\mathcal{K}$ su uniformno distribuirani.*

Dokaz. $\boxed{\implies}$ Pretpostavimo da S postiže savršenu sigurnost. Pokazat ćemo da su uvjeti 1 i 2 ispunjeni.

Da bismo dokazali prvi uvjet, fiksirajmo proizvoljni otvoreni tekst $x \in \mathcal{P}$. Pretpostavimo da postoji šifrat $y \in C$ takav da niti jedan ključ ne šifrira x u y. Odnosno, nije moguće iz otvorenog teksta x dobiti šifrat y, vrijedi $\mathbb{P}(x \mid y) = 0$. Prema pretpostavci teorema znamo $\mathbb{P}(X) > 0$. Sada imamo sljedeće

$$\mathbb{P}(x) \neq 0 = \mathbb{P}(x \mid y).$$

Dobili smo kontradikciju s pretpostavkom da je S savršeno siguran kriptosustav. Dakle, vrijedi

$$(\forall y \in C)\ (\exists K \in \mathcal{K}) \quad e_K(x) = y.$$

Koristeći pretpostavku $|C| = |\mathcal{K}|$ i činjenicu da su funkcije šifriranja injekcije, dobivamo da svaki šifrat $y \in C$ ima *jedinstveni* ključ $K \in \mathcal{K}$ takav da $e_K(x) = y$. Prvi uvjet je ispunjen.

Da bismo dokazali drugi uvjet, fiksirajmo proizvoljan šifrat $y \in C$. Po Bayesovom teoremu (1.3.4) slijedi da za svaki $x \in \mathcal{P}$ vrijedi

$$\mathbb{P}(x \mid y) = \frac{\mathbb{P}(x)\,\mathbb{P}(y \mid x)}{\mathbb{P}(y)}$$

Za svaki otvoreni tekst $x \in \mathcal{P}$, neka je $K(x)$ jedinstven ključ K takav da $e_K(x) = y$. Gore smo dokazali da takav K postoji. Vjerojatnost da je iz x dobiven y jednaka je vjerojatnosti da je korišten ključ K, tj. $\mathbb{P}(K(x)) = \mathbb{P}(y \mid x)$.

$$\implies \mathbb{P}(x \mid y) = \frac{\mathbb{P}(x)\,\mathbb{P}(K(x))}{\mathbb{P}(y)}$$

Budući da S garantira savršenu sigurnost, znamo $\mathbb{P}(x \mid y) = \mathbb{P}(x)$.

$$\implies \mathbb{P}(x) = \frac{\mathbb{P}(x)\,\mathbb{P}(K(x))}{\mathbb{P}(y)}$$

I konačno,

$$\mathbb{P}(K(x)) = \mathbb{P}(y), \tag{1.2}$$

Kako jednakost (1.2) vrijedi za svaki $x \in \mathcal{P}$, a y je fiksiran, dobili smo da su vjerojatnosti $\mathbb{P}(K)$ jednake za sve $K \in \mathcal{K}$, što znači $\mathbb{P}(K) = \frac{1}{|\mathcal{K}|}$, $\forall K \in \mathcal{K}$. Dakle, ključevi u $\mathcal{K}$ su uniformno distribuirani i drugi uvjet je ispunjen.

$\boxed{\impliedby}$ Obratno, pretpostavimo da su oba uvjeta ispunjena. Pokazat ćemo da je S savršeno sigurna.

Neka je $K = K(x, y)$ jedinstveni ključ $K \in \mathcal{K}$ takav da $e_K(x) = y$ za neke $x \in \mathcal{P}$ i $y \in C$. Iz Bayesovog teorema znamo:

$$\mathbb{P}(x \mid y) = \frac{\mathbb{P}(x)\,\mathbb{P}(y \mid x)}{\mathbb{P}(y)}.$$

Jer je K jedinstveni ključ pomoću kojega se iz x dobije y, jasno je da vrijedi $\mathbb{P}(K(x,y) = \mathbb{P}(y \mid x))$.

$$\implies \mathbb{P}(x \mid y) = \frac{\mathbb{P}(x)\,\mathbb{P}(K(x,y))}{\mathbb{P}(y)}$$

Iskoristimo formulu za potpun sustav događaja na nazivnik u gornjoj jednakosti:

$$\implies \mathbb{P}(x \mid y) = \frac{\mathbb{P}(x)\,\mathbb{P}(K(x,y))}{\sum_{z\in\mathcal{P}} \mathbb{P}(z)\,\mathbb{P}(K(z,y))}. \tag{1.3}$$

S obzirom da su, prema drugom uvjetu, ključevi uniformno distribuirani, vrijedi $\mathbb{P}(K(x,y)) = \frac{1}{|\mathcal{K}|}$. Raspišimo nazivnik desne strane gornje jednadžbe:

$$\sum_{z\in\mathcal{P}} \mathbb{P}(z)\,\mathbb{P}(K(z,y)) = \frac{\sum_{z\in\mathcal{P}} \mathbb{P}(z)}{|\mathcal{K}|} = \frac{1}{|\mathcal{K}|}.$$

Uvrštavanjem gornje jednakosti u (1.3) dobijemo

$$\mathbb{P}(x \mid y) = \mathbb{P}(x).$$

Budući da su x i y proizvoljni, možemo zaključiti da je kriptosustav S savršeno siguran. □

Poglavlje 2

Jednokratna bilježnica

U ovom poglavlju ćemo opisati jednu poznatu savršeno sigurnu šifru, Vernamovu jednokratnu bilježnicu. Zatim ćemo dokazati njenu savršenu sigurnost na dva ničina, pomoću karakterizacije savršene sigurnosti te direktno iz definicije savršene sigurnosti. Prije dokaza ćemo saznati zanimljivosti oko nastanka ove šifre i njenog naziva.

2.1 Definicija jednokratne bilježnice

Definicija 2.1.1. *Fiksirajmo alfabet* $\Sigma = \{0,1\}^n$ *i definirajmo prostore otvorenih tekstova, šifrata i ključeva sa*

$$\mathcal{P} = C = \mathcal{K} = \{0,1\}^n$$

za neku duljinu bloka $n \in \mathbb{N}$*. Ključevi su uniformno distribuirani na* $\{0,1\}^n$*. Za svaki ključ* $K \in \{0,1\}^n$*, definiramo funkciju šifriranja* $e_K : \{0,1\}^n \to \{0,1\}^n$ *i funkciju dešifriranja* $d_K : \{0,1\}^n \to \{0,1\}^n$ *sa*

$$e_K(x) = x \oplus K,$$
$$d_K(y) = y \oplus K,$$

gdje $\oplus$ *označava zbrajanje modulo 2 po bitovima.*

U idućem primjeru je prikaz šifriranja pomoću jednokratne bilježnice.

Primjer 2.1.2 (Jednokratna bilježnica)**.** *Želimo šifrirati otvoreni tekst "SHANNON". Za šifriranje jednokratnom bilježnicom koristimo ključ koji je jednake duljine kao otvoreni tekst, dakle duljine 7. Ključ također treba biti nasumičan niz slova zbog univerzalne distribucije. Recimo da je naš ključ "VEDHZBG" nasumično generiran nekim vanjskim alatom.*

Numerički ekvivalent otvorenog teksta je 18 7 0 13 13 14 13. Svaki broj ćemo prebaciti u binarni zapis duljine 5, jer je 5 bitova dovoljno za zapis brojeva manjih od 26 ($26 < 2^5$*).*

*Tako dobiveni binarni zapis otvorenog teksta je "*10010 | 00111 | 00000 | 01101 | 01101 | 01110 | 01101*". Isto napravimo za ključ čiji je numerički ekvivalent 21 24 3 7 25 1 6, odnosno binarni zapis "*10101 | 00100 | 00011 | 01010 | 11001 | 00001 | 00110*".*

$$\begin{array}{rl} & 10010 \mid 00111 \mid 00000 \mid 01101 \mid 01101 \mid 01110 \mid 01101 \\ & 10101 \mid 00100 \mid 00011 \mid 01010 \mid 11001 \mid 00001 \mid 00110 \\ \oplus & \text{-----------------------------} \\ & 00111 \mid 00011 \mid 00011 \mid 00111 \mid 10100 \mid 01111 \mid 01011 \end{array}$$

Rezultat primjene operacije XOR prebacimo u decimalni zapis te dobijemo 7 3 3 7 20 15 11. Zatim ga prebacimo u slova abecede da bi dobili šifrat "HDDHUPL".

Preostaje još dešifriranjem provjeriti rezultat. Dešifriranje se vrši primjenom operacije XOR na binarne zapise šifrata i ključa.

$$\begin{array}{rl} & 00111 \mid 00011 \mid 00011 \mid 00111 \mid 10100 \mid 01111 \mid 01011 \\ & 10101 \mid 00100 \mid 00011 \mid 01010 \mid 11001 \mid 00001 \mid 00110 \\ \oplus & \text{-----------------------------} \\ & 10010 \mid 00111 \mid 00000 \mid 01101 \mid 01101 \mid 01110 \mid 01101 \end{array}$$

Dešifriranjem smo dobili originalni otvoreni tekst "SHANNON".

2.2 Nastanak jednokratne bilježnice

Kada govorimo o jednokratnoj bilježnici, sve zasluge obično dajemo Gilbertu S. Vernamu i Josephu O. Mauborgneu jer su ju oni uveli 1917. godine. U to vrijeme nije bilo ASCII koda nego se za komunikaciju teleprinterom koristio njegov prethodnik, Baudotov kod koji je koristio 5 bitova za prikaz jednog znaka. Vernam je smislio uređaj koji obavlja XOR operacije na bitovima s papirnate vrpce na kojima je bio otisnut Baudotov kod generiran slovima natipkanima na tipkovnici. On i Mauborgne su shvatili da, ako su znakovi na papirnatoj traci potpuno generički, i ako se koriste najviše jednom, da su onda prikazane poruke potpuno tajne te ih je nemoguće anlizirati bez ključa. I bili su u pravu.

Vernam i Mauborgne se najčešće spominju kao izumitelji jednokratne bilježnice jer su njih dvojica prvi iznijeli ispravne i matematički dokazive tvrdnje. I jer su ju oni patentirali. No, oni nisu bili prvi koji su došli do ideje za ovakvu šifru. Iako se jednokratna bilježnica često spominje kao "Vernamova šifra", postoje tvrdnje da je ta šifra nastala puno prije Vernama. Prema članku *Frank Miller: Inventor of the One-Time Pad* [1], Frank Muller ih

je preduhitrio oko 35 godina. On je opisao šifru poput jednokratne bilježnice u svom radu *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*.

Ipak, nije potpuno jasno možemo li sada sve zasluge pripisati Franku Mulleru. U teoriji, njegova šifra jest poput jednokratne bilježnice jer također koristi jednokratni ključ i ima ista svojstva kao jednokratna bilježnica. No, u stvarnosti, nema dokaza da je itko, pa čak niti Frank Muller, ikad koristio tu šifru u stvarnom životu. Štoviše, moguće je da nitko osim Mullera i njegovih prijatelja nije niti znao za njeno postojanje.

Zanimljivo je i da u vrijeme kada je izumljena jednokratna bilježnica nije bilo moguće dokazati njenu sigurnost jer je definicija savršene sigurnosti donesena tek 50-ak godina kasnije. A ipak se kasnije pokazalo da je upravo jednokratna bilježnica najbolji primjer savršeno sigurnog kriptosustava te da svi drugi savršeno sigurni kriptosustavi moraju imati svojstva koja ima jednokratna bilježnica.

2.3 Dokaz savršene sigurnosti Vernamove jednokratne bilježnice

Dokaz preko Shannonovog teorema

Primjer 2.3.1. *Fiksirajmo prirodan broj l takav da je $\mathcal{P} = C = \mathcal{K} = \{0,1\}^l$. Ključevi su uniformno distribuirani na $\{0,1\}^n$. Neka su e_K i d_K funkcije šifriranja i dešifriranja iz definicije 2.1.1.*

Koristeći Shannonov teorem, vidimo da jednokratna bilježnica postiže savršenu sigurnost jer su ključevi u $\mathcal{K}$ uniformno distribuirani i jer za svaki otvoreni tekst $x \in \{0,1\}^l$ i svaki šifrat $y \in \{0,1\}^l$, postoji jedinstveni ključ $K \in \{0,1\}^l$ takav da $y = x \oplus K$.

Znamo da taj ključ postoji i jedinstven je jer su operacije zbrajanje modulo 2 i oduzimanje modulo 2 nad $\mathbb{Z}_{26}$ jednake te ga lako možemo izračunati, $K = x \oplus y$.

Jednokratna bilježnica zadovoljava definiciju savršene sigurnosti

U sljedećem primjeru ćemo pokazati da jednokratna bilježnica zadovoljava definiciju savršene sigurnosti tako što ćemo izračunati potrebne vjerojatnosti.

Primjer 2.3.2. *Fiksirajmo, kao u prethodnom dokazu, prirodan broj l takav da je $\mathcal{P} = C = \mathcal{K} = \{0,1\}^l$. Ključevi su uniformno distribuirani na $\{0,1\}^n$. Neka su e_K i d_K funkcije šifriranja i dešifriranja iz definicije 2.1.1.*

Prvo ćemo izračunati vjerojatnost $\mathbb{P}(x \mid y)$ za proizvoljne $y \in C$ i $x \in \mathcal{P}$ takve da $\mathbb{P}(x) > 0$. Budući da su ključevi u $\mathcal{K}$ uniformno distribuirani, vjerojatnost odabira ključa $K \in \mathcal{K}$ je točno 2^{-l}.

Iz definicije Vernamove šifre slijedi iduća jednakost.

$$\mathbb{P}(y \mid x) = \mathbb{P}(K \oplus x = y \mid x)$$

Operacija $\oplus$ *je simetrična možemo koristiti* $\mathbb{P}(K \oplus x = y \mid x) = \mathbb{P}(K = x \oplus y \mid x)$.

$$\mathbb{P}(y \mid x) = \mathbb{P}(K = x \oplus y \mid x)$$

Iskoristmo činjenicu da K dolazi iz univerzalno distribuiranog skupa od l elemenata i neovisna je o x:

$$\mathbb{P}(y \mid x) = 2^{-l}. \tag{2.1}$$

Sada ćemo izračunati $\mathbb{P}(y)$ *da bismo pomoću nje i Bayesovog teorema mogli dobiti* $\mathbb{P}(x \mid y)$. *Fiksiramo neku distribuciju nad* $\mathcal{P}$. *Koristeći formulu potpune vjerojatnosti* (1.1) *i rezultat gore* (2.1)*, vidimo da za svaki* $y \in C$ *vrijedi*

$$\begin{aligned} \mathbb{P}(y) &= \sum_{x \in \mathcal{P}} \mathbb{P}(y \mid x) \cdot \mathbb{P}(x) \\ &= 2^{-l} \cdot \sum_{x \in \mathcal{P}} \mathbb{P}(x) \\ &= 2^{-l,} \end{aligned} \tag{2.2}$$

gdje je suma po $x \in \mathcal{P}$ *takvim da* $\mathbb{P}(x) \neq 0$.

Uvrstimo (2.1) *i* (2.2) *u Bayesovu formulu:*

$$\begin{aligned} \mathbb{P}(x \mid y) &= \frac{\mathbb{P}(y \mid x) \cdot \mathbb{P}(x)}{\mathbb{P}(y)} \\ &= \frac{2^{-l} \cdot \mathbb{P}(x)}{2^{-l}} \\ &= \mathbb{P}(x). \end{aligned}$$

Dakle, Vernamova šifra je savršeno sigurna po definiciji savršene sigurnosti.

2.4 Nedostatci jednokratne bilježnice

Jednokratna bilježnica također ima mane, naime nije baš najpraktičnija za korištenje. Jedan pogled na definiciju je dovoljan za uočiti prvi i najveći nedostatak. Vernamova bilježnica koristi ključ koji je jednake duljine kao otvoreni tekst. Drugi nedostatak su jednokratni ključevi. A generiranje novog ključa za svaku novu poruku je iznimno bitno zato što je ova šifra simetrična. Ako osoba koja prisluškuje poruke uspije dobiti šifrat i barem jedan otvoreni tekst, neće joj biti teško saznati ključ. Razlog ovome je sljedeći

$$x \oplus y = x \oplus x \oplus K = K.$$

Zamislite da nekome želite poslati kriptiranu poruku. Prvo morate generirati i poslati ključ kojim će ta osoba dešifrirati vašu poruku. Kada je taj ključ jako dug, postaje upitno kako uopće sigurno poslati ključ i niste li isto tako mogli poslati nekriptiranu poruku. Da sve bude kompliciranije, ako poželite poslati još jednu poruku, morate prvo ponovno generirati i poslati novi ključ duljine nove poruke.

Odmah nam se nameće pitanje, ako već moramo koristiti jednokratne ključeve, možemo li ih barem skratiti? Pa, pokazat ćemo da je duljina ključa zapravo posljedica savršene sigurnosti i da se u ovako definiranom kriptosustavu ne može izbjeći. U idućem teoremu ćemo dokazati da svaka šifra koja postiže savršenu sigurnost, mora imati prostor ključeva veći ili jednak prostoru otvorenih tekstova. S obzirom da su kod jednokratne bilježnice svi otvoreni tekstovi fiksne duljine i svi ključevi jednake duljine, ovo povlači potrebu da ključ mora biti barem onoliko dug koliko je dug otvoreni tekst.

Teorem 2.4.1. *Ako je S neki savršeno siguran kriptosustav s prostorom otvorenih tekstova $\mathcal{P}$ i prostorom ključeva $\mathcal{K}$, tada vrijedi $|\mathcal{K}| \geq |\mathcal{P}|$.*

Dokaz. Pretpostavimo suprotno, $|\mathcal{K}| < |\mathcal{P}|$. Promotrimo uniformnu distribuciju nad $\mathcal{P}$ i fiksirajmo neki $y \in C$ šifrat za koji vrijedi $\mathbb{P}(y) > 0$. Neka je $\mathcal{P}(y)$ skup svih mogućih otvorenih tekstova koje je moguće dobiti dešifraranjem iz y, odnosno

$$\mathcal{P}(y) := \{x \mid x = d_K(y),\ K \in \mathcal{K}\}.$$

Iz ovoga očito vrijedi $|\mathcal{P}(y)| \leq |K|$. Sada iz pretpostavke $|\mathcal{K}| < |\mathcal{P}|$ slijedi da postoji neki $x' \in \mathcal{P}$ takav da $x' \notin \mathcal{P}(y)$. No, onda šifra nije savršeno sigurna zbog

$$\mathbb{P}(x' \mid y) = 0 \neq \mathbb{P}(x').$$

□

Usprkos nedostatcima, jednokratna bilježnica se ipak koristila za slučajeve kad je sigurnost od iznimne važnosti - u diplomatske i vojne svrhe. Postoje glasine da se jednokratna bilježnica koristila u Hladnom ratu za komunikaciju između Moskve i Washingtona. A dosta je zanimljivo pročitati i o VENONA projektu u [3], dobrom primjeru onoga što se dogodi kad se ključevi upotrebljavaju više puta.

Poglavlje 3

Entropija

Kod motivacije za definiciju savršene sigurnosti, govorili smo o informacijama koje se mogu saznati o otvorenom tekstu iz šifrata. Sada ćemo se zapitati, što je to uopće informacija? Kako možemo mjeriti informacije? Za odgovore na ta pitanja, uvodimo entropiju - još jedan pojam kojim se Shannon puno bavio. Kasnije ćemo vidjeti koliko je entropija usko povezana sa savršenom sigurnosti.

3.1 Definicija i primjeri

Iznosimo Shannonovu definiciju entropije.

Definicija 3.1.1 (Entropija)**.** *Neka je X slučajna varijabla koja poprima vrijednosti u $X = \{x_1, x_2, \ldots, x_n\}$. Za svaki $1 \leq i \leq n$, neka je $p_i = \mathbb{P}(X = x_i)$ vjerojatnost da X poprima vrijednost x_i.* ***Entropiju slučajne varijable X*** *definiramo sa*

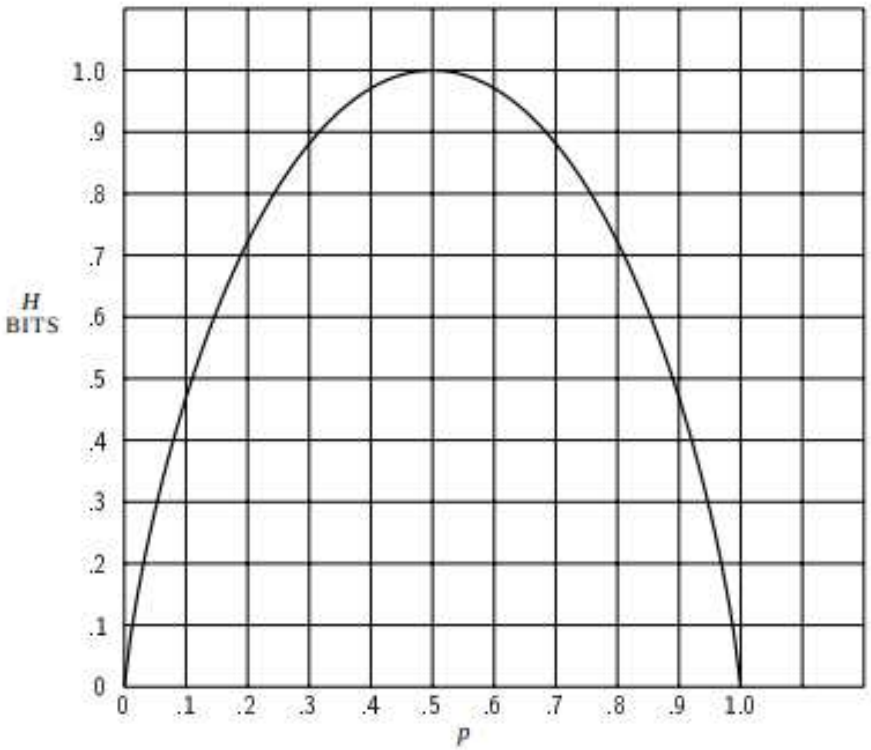
$$\mathcal{H}(X) = -\sum_{i=1}^{n} p_i \log_2 p_i. \tag{3.1}$$

Po dogovoru, koristimo da je $0 \log_2 0 = 0$.

Pojasnimo intuitivno razmišljanje o ovoj formuli koja ima formu kao matematičko očekivanje. Entropiju možemo gledati na dva načina. Ako gledamo prije izvođenja pokusa, entropija izražava stupanj nesigurnosti rezultata. No, ako gledamo nakon izvođenja pokusa, entropija je mjera prosječne količine informacije dobivene izvođenjem. Drugim riječima, ako se i-ti događaj dogodi u pokusu iz definicije 3.1.1, količina dobivenih informacija je $-\log_2 p_i$, odnosno $\log_2 \frac{1}{p_i}$. Ako su događaji nezavisni, njihove vjerojatnosti se množe, pa se po svojstvima logaritama odgovarajuće količine informacija zbrajaju.

Uz ovako definiranu entropiju koristimo *bit* kao mjernu jedinicu za količinu informacije. Kad bi umjesto logaritma po bazi 2 koristili logaritam po nekoj drugoj bazi, morali

bi koristiti neku drugu mjernu jedinicu. Shannon ih je popisao nekoliko, ali u današnje vrijeme je *bit* najbolje prihvaćena. Primijetimo da je upravo Shannon bio prvi znanstvenik u povijesti koji je u znanstvenom radu koristio pojam "bit" za količinu informacije.



Slika 3.1: Graf entropije za slučajnu varijablu s dvije moguće vrijednosti s vjerojatnostima p i $(1-p)$, objavljen u časopisu The Bell System Technical Journal

Primjer 3.1.2. *(Entropija) Bacanje novčića je slučajni pokus s dva moguća ishoda: pismo ili glava. Neka je X slučajna varijabla koja poprima rezultat ovog pokusa: $X = 1$ ako je pala glava, $X = 0$ ako je palo pismo. Uz pretpostavku da se radi o simetričnom novčiću, oba događaja su jednako vjerojatna, odnosno $p_1 = p_2 = \frac{1}{2}$. Uvrstimo li to u formulu za*

entropiju (3.1)*, dobijemo sljedeće:*

$$\begin{aligned}\mathcal{H}(X) &= -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right)\\ &= -\log_2\frac{1}{2}\\ &= \log_2 2\\ &= 1.\end{aligned}$$

Dakle, količina informacije dobivena bacanjem simetričnog novčića je točno jedan bit.

Primjer 3.1.3. *Nastavno na prethodni primjer, uzmimo novčić koji nije simetričan te ima vjerojatnost* $p_1 = \frac{1}{4}$ *da padne glava i* $p_2 = \frac{3}{4}$ *da padne pismo. Sada imamo:*

$$\mathcal{H}(X) = -\left(\frac{1}{4}\log_2\frac{1}{4} + \frac{3}{4}\log_2\frac{3}{4}\right) \approx 0.8113$$

Primijetimo da se entropija smanjila na 0.8113 *bita.*

Bacanje novčića je najjednostavniji pokus za razumijevanje entropije. Pogledajmo što se dogodi kada računamo entropiju pokusa bacanja simetrične kockice.

Primjer 3.1.4. *(Entropija) Bacanje kockice je slučajni pokus sa šest mogućih ishoda. Neka je* X *slučajna varijabla koja poprima rezultat ovog pokusa* $X = 1$ *ako je pala jedinica,* $X = 2$ *ako je pala dvojka,* $\ldots$*,* $X = 6$ *ako je pala šestica. Uz pretpostavku da se radi o simetričnom novčiću, svih šest događaja su jednako vjerojatni, odnosno* $p_1 = p_2 = p_3 = p_4 = p_5 = p_6 = \frac{1}{6}$*. Uvrstimo li to u formulu za entropiju* (3.1)*, dobijemo sljedeće:*

$$\begin{aligned}\mathcal{H}(X) &= -\left(\frac{1}{6}\log_2\frac{1}{6} + \frac{1}{6}\log_2\frac{1}{6} + \frac{1}{6}\log_2\frac{1}{6} + \frac{1}{6}\log_2\frac{1}{6} + \frac{1}{6}\log_2\frac{1}{6} + \frac{1}{6}\log_2\frac{1}{6}\right)\\ &= -\log_2\frac{1}{6}\\ &= \log_2 6\\ &= 2.585.\end{aligned}$$

Dakle, količina informacije dobivena bacanjem simetrične kockice je 2.585 bit.

U ovom primjeru smo dobili veću entropiju nego za simetričan novčić. Intuitivno to ima smisla jer postoji više mogućih rezultata pa je i nesigurnost veća.

Primijetimo da je entropija uvijek najveća kad je distribucija prostora uniformna jer je tada najteže pogoditi rezultat. Drugim riječima, tada je stupanj nesigurnosti rezultata najveći. Kasnije ćemo vidjeti zašto nam je ovo bitno.

Idući primjer će pokazati kako se opisuju razne komponente kriptosustava pomoću njihovih entropija.

Primjer 3.1.5. *(Entropija kriptosustava) Neka je* $S = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *kriptosustav takav da*

$$\mathcal{P} = \{A, B\}, \quad \mathcal{K} = \{+, -\}, \quad \mathcal{C} = \{X, Y\}$$
$$e_+(A) = X, \ e_-(A) = Y,$$
$$e_+(B) = Y, \ e_-(B) = X$$

s vjerojatnostima

$$\mathbb{P}(A) = \frac{3}{5}, \ \mathbb{P}(B) = \frac{2}{5},$$
$$\mathbb{P}(+) = \frac{1}{3}, \ \mathbb{P}(-) = \frac{2}{3}.$$

O ključu možemo razmišljati kao o slučajnoj varijabli K *koja poprima vrijednosti u* $K = \{+, -\}$*, i na taj način joj možemo izračunati entropiju. Slično, neka su* P *i* C *slučajne varijable koje opisuju otvoreni tekst i šifrat, te poprimaju vrijednosti u* $\mathcal{P}$ *i* $\mathcal{C}$*. I njima možemo računati entropiju.*

Prvo računamo vjerojatnosti za sve moguće kombinacije otvorenih tekstova i ključeva

$$\mathbb{P}(A, +) = \mathbb{P}(A) \cdot \mathbb{P}(+) = \frac{3}{5} \cdot \frac{1}{3} = \frac{1}{5},$$
$$\mathbb{P}(A, -) = \mathbb{P}(A) \cdot \mathbb{P}(-) = \frac{3}{5} \cdot \frac{2}{3} = \frac{2}{5},$$
$$\mathbb{P}(B, +) = \mathbb{P}(B) \cdot \mathbb{P}(+) = \frac{2}{5} \cdot \frac{1}{3} = \frac{2}{15},$$
$$\mathbb{P}(B, -) = \mathbb{P}(B) \cdot \mathbb{P}(-) = \frac{2}{5} \cdot \frac{2}{3} = \frac{4}{15}.$$

Dalje računamo vjerojatnosti šifrata

$$\mathbb{P}(X) = \mathbb{P}(A, +) + \mathbb{P}(B, -) = \frac{1}{5} + \frac{4}{15} = \frac{7}{15}$$
$$\mathbb{P}(Y) = \mathbb{P}(A, -) + \mathbb{P}(B, +) = \frac{2}{5} + \frac{2}{15} = \frac{8}{15}.$$

Konačno, entropije varijabli $\mathcal{K}$, $\mathcal{P}$ i C mogu se izračunati na sljedeći način:

$$\begin{aligned}\mathcal{H}(\mathcal{P}) &= -\left(\mathbb{P}(A)\log_2\mathbb{P}(A) + \mathbb{P}(B)\log_2\mathbb{P}(B)\right)\\ &= -\left(\frac{3}{5}\cdot\log_2\frac{3}{5} + \frac{2}{5}\cdot\log_2\frac{2}{5}\right)\\ &\approx 0.97096,\end{aligned}$$

$$\begin{aligned}\mathcal{H}(\mathcal{K}) &= -\left(\mathbb{P}(+)\log_2\mathbb{P}(+) + \mathbb{P}(-)\log_2\mathbb{P}(-)\right)\\ &= -\left(\frac{1}{3}\cdot\log_2\frac{1}{3} + \frac{2}{3}\cdot\log_2\frac{2}{3}\right)\\ &\approx 0.9183,\end{aligned}$$

$$\begin{aligned}\mathcal{H}(C) &= -\left(\mathbb{P}(X)\log_2\mathbb{P}(X) + \mathbb{P}(Y)\log_2\mathbb{P}(Y)\right)\\ &= -\left(\frac{7}{15}\cdot\log_2\frac{7}{15} + \frac{8}{15}\cdot\log_2\frac{8}{15}\right)\\ &\approx 0.9968.\end{aligned}$$

U sljedećem teoremu iskazat ćemo neka korisna svojstva entropije.

Teorem 3.1.6. (**Svojstva entropije**) *Neka je X slučajna varijabla koja može poprimiti n mogućih vrijednosti iz skupa $X = \{x_1, x_2, \ldots, x_n\}$. Za svaki $1 \le i \le n$, neka je $p_i = \mathbb{P}(X = x_i)$ vjerojatnost da X poprima vrijednost x_i.*

1. *$\mathcal{H}(X) \le \log_2 n$, gdje jednakost vrijedi ako i samo ako $(p_1, p_2, \ldots, p_n) = \left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right)$.*

2. *$\mathcal{H}(X) \ge 0$, gdje jednakost vrijedi ako i samo ako $p_i = 1$, za neki i, te $p_j = 0$ za $j \ne i$. Dakle, $\mathcal{H}(X) = 0$ znači da je ishod pokusa unaprijed određen s potpunom sigurnošću.*

3. *Neka je Y slučajna varijabla koja može poprimiti jednu od $n+1$ mogućih vrijednosti iz skupa $Y = \{y_2, y_2, \ldots, y_{n+1}\}$. Ako je $\mathbb{P}(Y = y_i) = p_i$ za $1 \le i \le n$ i $\mathbb{P}(Y = y_{n+1}) = 0$, tada $\mathcal{H}(Y) = \mathcal{H}(X)$.*

4. *Neka je $\pi \in \mathfrak{S}_n$ proizvoljna permutacija skupa $\{1, 2, \ldots, n\}$. Ako je Y slučajna varijabla takva da $\mathbb{P}(Y = x_i) = p_{\pi(i)}$, $1 \le i \le n$, tada $\mathcal{H}(Y) = \mathcal{H}(X)$.*

5. **(Grupirajuće svojstvo)** *Neka su Y i Z slučajne varijable takve da Y može poprimiti jednu od $n-1$ mogućih vrijednosti s vjerojatnostima $p_1 + p_2 \ldots, p_n$, dok Z može poprimiti jednu od dvije moguće vrijednosti s vjerojatnostima $p_1/(p_1+p_2)$ i $p_2/(p_1+p_2)$, tada vrijedi $\mathcal{H}(X) = \mathcal{H}(Y) + (p_1 + p_2)\mathcal{H}(Z)$.*

6. **(Gibbsova lema)** *Neka je Y slučajna varijabla koja može poprimiti n mogućih vrijednosti s vjerojatnostima $q_1, q_2, \ldots, q_n$ (primjerice, $0 \leq q_i \leq 1$ i $\sum_{i=1}^{n} q_i = 1$, tada*

$$\mathcal{H}(X) \leq -\sum_{i=1}^{n} p_i \log_2 q_i,$$

gdje jednakost vrijedi ako i samo ako je $(p_1, p_2 \ldots, p_n) = (q_1, q_2, \ldots, q_n)$.

7. **(Subaditivnost)** *Neka je $Z = (X_1, X_2, \ldots, X_n)$ slučajna varijabla koja može poprimiti vrijednosti n-torki oblika $(x_1, x_2, \ldots, x_n)$, primjerice x_i je vrijednost slučajne varijable X_i. Tada:*

$$\mathcal{H}(Z) \leq \mathcal{H}(X_1) + \mathcal{H}(X_2) + \ldots + \mathcal{H}(X_n),$$

gdje jednakost vrijedi ako i samo ako su slučajne varijable X_i nezavisne, odnosno

$$\mathbb{P}(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) = \prod_{i=1}^{n} \mathbb{P}(X_i = x_i).$$

3.2 Uvjetna entropija

Slično kao što smo definirali uvjetnu vjerojatnost, sada ćemo definirati uvjetnu entropiju. Intuitivno, uvjetna entropija mjeri količinu informacije koju slučajna varijabla Y otkriva o slučajnoj varijabli X. Ovaj pojam će biti koristan za kvantificiranje informacije koju kriptoanalitičar može saznati o korištenom ključu ako mu je poznat šifrat.

Definicija 3.2.1 (Uvjetna entropija)**.** *Neka su X i Y dvije slučajne varijable takve da X može poprimiti jednu od n mogućih vrijednosti iz skupa $X = \{x_1, x_2, \ldots, x_n\}$, a Y može poprimiti jednu od m mogućih vrijednosti iz skupa $Y = \{y_1, y_2, \ldots, y_m\}$. Za svaki i i j, $1 \leq i \leq n$ i $1 \leq j \leq m$, definiramo uvjetne vjerojatnosti p_{ij} i vjerojatnosti q_j sa*

$$p_{ij} = \mathbb{P}(X = x_i \mid Y = y_j),$$
$$q_j = \mathbb{P}(Y = y_j).$$

Za fiksirani j, $1 \leq j \leq m$, neka X_j označava slučajnu varijablu na X koja je distribuirana prema $p_{1j}, p_{2j}, \ldots, p_{nj}$. Očito vrijedi

$$\mathcal{H}(X_j) = -\sum_{i=1}^{n} p_{ij} \log_2 p_{ij}.$$

Uvjetnu entropiju *definiramo formulom*

$$\mathcal{H}(X \mid Y) = \sum_{j=1}^{m} q_j \mathcal{H}(X_j) = -\sum_{j=1}^{m} \sum_{i=1}^{n} q_j p_{ij} \log_2 p_{ij}.$$

Intuitivno, uvjetna entropija $\mathcal{H}(X \mid Y)$ je težinski prosjek entropija $\mathcal{H}(X_j), 1 \leq j \leq m$ (s obzirom na vjerojatnosnu distribuciju na Y). Kratko navodimo neka korisna svojstva uvjetne entropije.

Teorem 3.2.2. $\mathcal{H}(X, Y) = \mathcal{H}(Y) + \mathcal{H}(X \mid Y)$.

Korolar 3.2.3. $\mathcal{H}(X, Y) \leq \mathcal{H}(X)$*, gdje jednakost vrijedi ako i samo ako su X i Y nezavisne.*

Poglavlje 4

Veza entropije i savršene sigurnosti

U ovom poglavlju ćemo pojasniti da se entropija nalazi u pozadini Shannonove karakterizacije savršene sigurnosti. Kako bi komunikacija bila što sigurnija, cilj nam je uvesti što više nereda i nesigurnosti u šifrate. Odnosno, želimo uvesti maksimalnu moguću entropiju.

4.1 Drugi zahtjev Shannonovog teorema

Otvoreni tekstovi su obično riječi nekog jezika ili neki numerički podaci koji imaju smisla. Zato na prostore otvorenih tekstova ne možemo baš utjecati. Njihova vjerojatnosna distribucija je takva kakva je. Budući da želimo da nam prostor šifrata bude što nesigurniji, trudimo se uvesti maksimalnu moguću entropiju šifriranjem. Za to koristimo prostor ključeva s velikom entropijom jer se u kriptosustav može unijeti najviše onoliko entropije koliko je ima u prostoru ključeva. Prisjetimo se, ranije smo rekli da univerzalna distribucija uvijek daje maksimalnu entropiju. Upravo ovo leži u pozadini uvjeta (2) u karakterizaciji savršene sigurnosti: želimo koristiti univerzalno distribuirane ključeve kako bi dobili maksimalnu moguću entropiju u šifratima.

4.2 Višeznačnost ključa

U primjeru 3.1.4 smo vidjeli da za dani kriptosustav $S = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ možemo razmišljati o ključu, otvorenom tekstu i šifratu kao o slučajnim varijablama K, P i C kojima možemo računati entropije. Sada nas zanima određivanje uvjetne entropije $\mathcal{H}(K \mid C)$ koju nazivamo **višeznačnost ključa u** S, a interpretiramo ju kao količinu informacije koju šifrat daje o ključu. Sljedeći rezultat pokazuje kako izračunati višeznačnost ključa nekog kriptosustava.

Teorem 4.2.1. *Neka je* $S = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *neki kriptosustav i neka su K,P i C slučajne*

varijable koje odgovaraju $\mathcal{K}, \mathcal{P}$ i C. Tada

$$\mathcal{H}(K \mid C) = \mathcal{H}(K) + \mathcal{H}(P) - \mathcal{H}(C).$$

Dokaz. Primjenom teorema 3.2.2 na $X = C$ i $Y = (K, P)$ dobivamo

$$\mathcal{H}(C, K, P) = \mathcal{H}(K, P) + \mathcal{H}(C \mid K, P).$$

Budući da je S kriptosustav, dani ključ $K \in \mathcal{K}$ i otvoreni tekst $p \in \mathcal{P}$ jedinstveno određuju šifrat $c = e_K(p)$. Dakle, $\mathcal{H}(C \mid K, P) = 0$. Iz toga slijedi

$$\mathcal{H}(C, K, P) = \mathcal{H}(K, P).$$

No, budući da su slučajne varijable K i P nezavisne, subaditivnost entropije (svojstvo 7 u teoremu 3.1.6) daje $\mathcal{H}(K, P) = \mathcal{H}(K) + \mathcal{H}(P)$. Dakle,

$$\mathcal{H}(C, K, P) = \mathcal{H}(K, P) = \mathcal{H}(K) + \mathcal{H}(P). \tag{4.1}$$

Slično, dani ključ $K \in \mathcal{K}$ i šifrat $c \in C$ jedinstveno određuju otvoreni tekst $p = D_K(c)$. Dakle, $\mathcal{H}(P \mid K, C) = 0$. Slijedi da je

$$\mathcal{H}(C, K, M) = \mathcal{H}(K, C). \tag{4.2}$$

Po teoremu 3.2.2, jednakosti (4.1) i (4.2) povlače

$$\begin{aligned} \mathcal{H}(K \mid C) &= \mathcal{H}(K, C) - \mathcal{H}(C) \\ &= \mathcal{H}(C, K, P) - \mathcal{H}(C) \\ &= \mathcal{H}(K) + \mathcal{H}(P) - \mathcal{H}(C), \end{aligned}$$

što je upravo tvrdnja teorema. □

Sada možemo izračunati višeznačnost ključa kriptosustava. Nastavljamo sa kriptosustavom S iz primjera 3.1.4.

Primjer 4.2.2. *Ranije smo odredili entropije slučajnih varijabli K, P **i** C koje odgovaraju prostorima ključeva, otvorenih tekstova i šifrata:*

$$\begin{aligned} \mathcal{H}(K) &\approx 0.97096, \\ \mathcal{H}(P) &\approx 0.9183, \\ \mathcal{H}(C) &\approx 0.9968. \end{aligned}$$

Korištenjem teorema 4.2.1 računamo uvjetnu entropiju:

$$\begin{aligned} \mathcal{H}(K \mid C) &= \mathcal{H}(K) + \mathcal{H}(P) - \mathcal{H}(C) \\ &\approx 0.97096 + 0.9183 - 0.9968 \\ &\approx 0.89246. \end{aligned}$$

Dakle, ako u kriptosustavu S znamo šifrat, iz njega možemo dobiti 0.7497 *bit informacija o ključu.*

4.3 Prvi zahtjev Shannonovog teorema

Poznavanje entropije nam je dalo novu razinu razumijevanja jednog uvjeta Shannonove karakterizacije. Sada ćemo isto tako pojasniti uvjet (1) karakterizacije. Pogledajmo prvi uvjet:

za svaki $x \in \mathcal{P}$ i za svaki $y \in C$, postoji jedinstveni ključ $K \in \mathcal{K}$ takav da $e_K(x) = y$.

On traži da za svaki šifrat i svaki otvoreni tekst postoji jedinstveni ključ pomoću kojega se iz otvorenog teksta dobije šifrat. Pogledajmo bolje što to točno znači. Svaki šifrat je moguće dobiti iz svakog otvorenog teksta pomoću nekog ključa. Zbog toga postaje gotovo nemoguće utvrditi iz kojeg je otvorenog teksta dobiven neki šifrat. Ovaj uvjet osigurava upravo maksimalnu moguću višeznačnost ključa.

4.4 Maksimalna entropija kriptosustava

Do sada smo vidjeli da korištenje univerzalnog prostora ključeva unosi visoku entropiju u sustav šifrata. Zatim smo utvrdili da korištenje višeznačnih ključeva također doprinosi sigurnosti kriptosustava. Preostalo je samo povezati prethodne dvije opaske. Dakle, uvođenje maksimalne entropije u šifrate postiže se kombinacijom maksimalno entropičnog prostora ključeva i maksimalnom višeznačnosti ključeva. Sada vidimo da Shannonov teorem zapravo daje upute za građenje savršeno sigurnog kriptosustava pomoću metoda koje osiguravaju da se u kriptosustav unese najviše entropije.

Bibliografija

[1] S. M. Bellovin, *Frank Miller: Inventor of the One-Time Pad*, Cryptologia **35** (2011), 203–222.

[2] D. Dujella i M. Maretić, *Kriptografija*, Element, 2007.

[3] J. E. Haynes, H. Klehr i H. Klehr, *Venona: decoding Soviet espionage in America*, Yale University Press, 1999.

[4] J. Rothe, *Complexity Theory and Cryptography. An Introduction to Cryptocomplexity*, Springer, 2005.

[5] N. Sarapa, *Teorija vjerojatnosti*, Školska knjiga, 2001.

[6] C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal **27** (1948), br. 3, 379–423, https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1948.tb01338.x.

[7] D. Tse, *How Claude Shannon Invented the Future*, (2020), https://www.quantamagazine.org/how-claude-shannons-information-theory-invented-the-future-20201222.

Sažetak

U ovom radu je detaljno objašnjena savršena sigurnost kriptosustava. Dan je primjer kriptosustava koji nije savršeno siguran te je definiran i prikazan jedan savršeno siguran kriptosustav, Vernamova jednokratna bilježnica. Iskazan je i dokazan Shannonov teorem o nužnim i dovoljnim uvjetima savršene sigurnosti kriptosustava. Definirani su pojmovi entropije, uvjetne entropije i višeznačnosti ključa uz popratne primjere za razumijevanje. Na kraju je pojam entropije povezan sa savršenom sigurnosti.

Summary

This thesis explains perfect secrecy of cryptosystems in detail. It gives an example of a cryptosystem that is not perfectly secret, and it defines and shows a cryptosystem that is perfectly secret - Vernam cipher known as one-time pad. Shannon's theorem about neccessary and sufficient conditions for prefectly secret cryptosystems is stated and proven in the thesis. Terms of entropy, conditional entropy and key equivocation are introduced with supporting examples for better understanding. In the end, the thesis explains the connection of entropy and perfect secrecy.

Životopis

Ena Majin rođena je 14. kolovoza 1995. godine u Požegi. Nakon završene osnovne škole Antuna Kanižlića, upisuje opći smjer Gimnazije u Požegi. Nakon prvog razreda prebacuje se na matematički smjer iste škole. Prirodoslovno-matematički fakultet upisala je 2014. godine, gdje je završila preddiplomski sveučilišni studij Matematika. Obrazovanje nastavlja na diplomskom smjeru Računarstvo i matematika. Tijekom studiranja radila je brojne studentske poslove, a trenutno se bavi razvojem softvera.