

Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva

By Dejan Cizelj

4

UNIVERZITET SINGIDUNUM

BEOGRAD

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKA DISERTACIJA

Sinteza efikasnih izvora zajedničke
slučajnosti za potrebe generisanja i distribuciju
tajnih kriptografskih ključeva

MENTOR:

Prof. dr Miljan Vučetić

DOKTORAND:

Dejan Cizelj

Broj indeksa: 460042/2022

2

Beograd, 2025. godine

PODACI O MENTORU I ČLANOVIMA KOMISIJE

Mentor:

1. Prof. dr Miljan Vučetić, mentor, redovni profesor Univerziteta Singidunum, naučni savetnik Institut Vlatacom

Članovi komisije:

2. Prof. dr Mladen Veinović, redovni profesor Univerziteta Singidunum
3. Dr Tomislav Unkašević, naučni saradnik, Institut Vlatacom, komentor
4. Dr Branko Kovačević, profesor emeritus

² Datum odbrane disertacije:

ZAHVALNICA

Zahvaljujem se mentoru prof. dr Miljanu Vučetiću kao i komentoru dr Tomislavu Unkaševiću, na kontinuiranoj podršci, dragocenim savetima i učestvovanju tokom izrade ove doktorske disertacije. Prof. dr Milanu Milosavljeviću dugujem veliku zahvalnost za znanje koje mi je nesebično prenosio iz oblasti kriptologije i nesebičnu pomoć pri pisanju ove ²disertacije.

Veliku zahvalnost dugujem Institutu Vlatacom, koji mi je pružio priliku i omogućio vreme i resurse za vršenje istraživanja, kao i veliku podršku tokom izrade disertacije.

REZIME

U ovoj disertaciji razvijen je novi teorijski okvir i praktično primenljiv model za autonomnu destilaciju tajnog ključa (SKD), koji se zasniva na deterministički oblikovanoj zajedničkoj slučajnosti. Za razliku od klasičnih pristupa koji se oslanjaju na fizičke izvore entropije ili složene protokole razmene informacija, predloženi model kombinuje determinističke generatore pseudoslučajnih nizova, inicijalizovane zajedničkim tajnim ključem (GPSN(K)), sa lokalno generisanim Bernulijevim šumom kao dodatnim izvorom nesimetrične entropije. Ova arhitektura omogućava sintezu izlaznih sekvenci koje su statistički neodvojive od izlaza u Mauerovom satelitskom modelu, uz mogućnost precizne kontrole nad bezbednosnim metrikama kao što su Shannon-ova entropija, nivo ekvivokacije i brzina curenja informacija.

Ključni teorijski doprinos rada ogleda se u izvođenju zatvorene forme donje granice ekvivokacije, kojom se određuje bezbedna operativna oblast sistema. U toj oblasti nije neophodno koristiti dodatne procedure za predobradu kao što je destilacija prednosti AD, što dodatno pojednostavljuje implementaciju. Takođe, disertacija predlaže i optimizovanu primenu Winnow protokola prilagođenu za veoma kratke blokove podataka ($N = 8$), čime se postiže visok stepen rekonsilijacije uz minimalnu stopu greške i optimalno korišćenje resursa.

Analitičkom evaluacijom identifikovana su dva funkcionalna režima rada: režim idealne i režim perfektne tajnosti, u kojima sistem ostvaruje brzine generisanja tajnog ključa i do 22%, istovremeno zadovoljavajući stroge uslove bezbednosti – stopu greške u rekonsilijaciji $KDR < 10^{-5}$ i stopu curenja informacija $LR < 10^{-10}$. Ovim se omogućava dizajn potpuno samostalnih SKD sistema koji ne zavise od fizičke složenosti komunikacionog kanala niti od spoljnih izvora entropije, što predstavlja značajan napredak u oblasti bezbedne razmene informacija.

Naučna oblast: Telekomunikacije, računarstvo i informatika

SUMMARY

This dissertation introduces a novel theoretical framework and practically viable model for autonomous secret key distillation (SKD), grounded in deterministically synthesized common randomness. Departing from conventional approaches that depend on physical entropy sources or intricate key exchange protocols, the proposed solution integrates pseudorandom sequence generators seeded with a shared secret key (GPSN(K)) and enhances them with locally produced Bernoulli noise as a source of asymmetrical randomness. This configuration ensures that the resulting key sequences are statistically indistinguishable from those produced by the classical Mauer satellite model, while allowing fine-grained control over crucial security metrics such as entropy, equivocation, and information leakage.

The central theoretical contribution lies in the derivation of a closed-form lower bound for key equivocation. This result makes it possible to delineate a well-defined operational region in which long-term security can be guaranteed without relying on pre-processing phases such as advantage distillation, AD. Additionally, the dissertation presents an optimized implementation of the Winnow protocol tailored for short data blocks ($N = 8$), thereby achieving high reconciliation efficiency with low error rates and resource consumption.

Through rigorous analysis, two principal operational modes of the system were identified: ideal secrecy and perfect secrecy. Within these regimes, the proposed scheme achieves key generation rates of up to 22%, all while maintaining strict security guarantees—namely, a key disagreement rate (KDR) below 10^{-5} and a leakage rate (LR) below 10^{-10} . As a result, the proposed framework enables the design of self-contained SKD systems that operate independently of communication channels or external entropy sources, representing a significant advancement in secure communications technology.

Scientific field: Telecommunications, computing and information science

SADRŽAJ

SPISAK TABELA.....	9
SPISAK SLIKA	10
LISTA SKRAĆENICA	13
1. UVOD.....	17
2. OSNOVE TEORIJE KRIPTOGRAFSKIH KLJUČEVA.....	21
2.1 Istorijski pregled	21
2.1.1 Antička kriptografija i srednji vek	21
2.1.2 Mehaničko doba i drugi svetski rat	21
2.1.3 Teorijska formalizacija i standardi (posle 1949).....	21
2.1.4 Teorijske osnove i definicije.....	22
2.2 Osnove kriptografskih ključeva u teoriji informacija	22
2.2.1 Klasifikacija i primena kriptografskih ključeva	24
2.2.2 Tajni ključevi u destilaciji i sintezi zajedničke slučajnosti	25
2.2.3 Savremeni simetrični algoritmi.....	26
2.2.4 Distribucija i zamena tajnog ključa	28
2.2.5 Moderni napadi:.....	29
2.2.6 Novi pravci razvoja – kvantna i postkvantna otpornost.....	33
3. PREGLED RELEVANTNE LITERATURE I MODELA IZVORA ZAJEDNIČKE SLUČAJNOSTI.....	36
3.1 Zajednička slučajnost (Common Randomness – CR).....	39
3.2 Satelitski scenario kao izvor zajedničke slučajnosti	41
3.2.1 Primene satelitskog scenarija.....	42
3.3 Osvrt na upotreba velikih jezičkih modela (LLM)	42
3.3.1 Osnove pristupa: LLM kao izvor zajedničke slučajnosti	42
3.3.2 Osobine pristupa zasnovanog na LLM	43
3.3.3 Ograničenja i izazovi pristupa.....	44

3.3.4	Perspektive i potencijalna primena	44
3.4	Formalizacija izvora zajedničke slučajnosti	45
3.4.1	Nezavisnost.....	45
3.4.2	Korelacija.....	45
3.4.3	Kovarijanca i korelacija	45
3.4.4	Skalarna slučajna promenljiva (SKD)	46
3.4.5	Uslovna verovatnoća	46
3.4.6	Deterministički GPSN i Bernulijeva šumna injekcija: GPSN (Generalizovani Poissonov šum)	46
3.4.7	Bernulijeva šumna injekcija	46
3.4.8	Primer formalizacije	46
4.	ARHITEKTURA NOVOG PERFEKTNO TAJNOG KRIPTO SISTEMA	48
4.1	Arhitektura sistema sa GPSN(K).....	48
4.2	Statističko mapiranje na Mauero model.....	50
4.3	Konstrukcija i podešavanje parametara	52
5.	INFORMACIONO-TEORIJSKA ANALIZA IZVORA ZAJEDNIČKE SLUČAJNOSTI 55	
5.1	Destilacija tajnog ključa i informatička rekonsilijacija	59
6.	OPTIMALNI SKD SISTEM ZASNOVAN NA CR KSG I WINNOW IR PROTOKOLU	65
6.1	Od idealne do perfektne bezbednosti korišćenjem SKD zasnovanog na CR KSG i Winnow IR protokola	76
6.2	Postupak sinteze	82
7.	ANALIZA BEZBEDNOSTI I PRAKTIČNI ASPEKTI PRIMENE	85
7.1	Faza generisanja zajedničke slučajnosti (CR).....	88
7.2	Poređenje operative složenosti po bitu tajnog ključa u SKD sistemima .	89
7.3	Eksperimentalna verifikacija	91
8.	ZAKLJUČAK I PRAVCI BUDUĆIH STRAŽIVANJA.....	97

9. LITERATURA.....	101
--------------------	-----

SPISAK TABELA

Tabela 2-1 Pregled osobina simetričnih, asimetričnih i hibridnih kript sistema	24
Tabela 6-1 Maksimalna efektivna brzina generisanja kriptografskih ključeva $ \tilde{K}_s _{max}$ i odgovarajuća dužina bloka n_{IR0} , za tipične vrednosti dužine ključa $ K_G $ i stepen kompresije $t = 34$	75
Tabela 6-2 Maksimalna efektivna brzina generisanja kriptografskih ključeva $ \tilde{K}_s _{max}$ i odgovarajuća dužina bloka n_{IR0} , za tipične vrednosti dužine ključa $ K_G $ i stepen kompresije $t = 34$	82
Tabela 7-1 Mogući generatori ključa za SDK sisteme	89

SPISAK SLIKA

Slika 4-1 Autonomni SKD sistemi koji koriste sintetički izvor zajedničke slučajnosti zasnovan na zajedničkom generatoru ključeva $KSG(K_G)$ i lokalnoj čistoj slučajnosti.48

Slika 4-2 Parametar ε pomoću koga se može postići željeni BER..... 50

Slika 4-3 Ekvivalentni Mauerov satelitski scenario. Satelit emituje ključ za šifrovanje C_K , a na tri nezavisna kanala ka Alisi, Bobu i Evi deluju šumovi E_A , E_B i $\tilde{E}_E$, respektivno. 51

Slika 5-1 Ilustracija jednog normalizovanog dopustivog regiona $\tilde{D}$ u funkciji inicijalnog BER p_{IRO} između Alisinog i Bobovog niza na početku IR protokola. Za dato $p_{IRO}^* \in \tilde{D}$ pokazani su $|\tilde{K}_S|$, $\tilde{A}_{K_G}$, $|\tilde{K}_G|$ i $\tilde{t}$ u slučaju maksimalne moguće brzine destilacije tajnog ključa..... 62

Slika 6-1 Promena $\mu_{IR}^{Win}(p_{IRO})$ kroz 4 iteracije Winnow protokola 69

Slika 6-2 Promena normalizovanih vrednosti $\tilde{n}_p = \frac{n_p}{n_{IRO}}$, $\tilde{n}_b = \frac{n_b}{n_{IRO}}$ i $\tilde{n}_H = \frac{n_H}{n_{IRO}}$, u funkciji p_{IRO} nakon 4. iteracije Winnow protokola..... 69

Slika 6-3 Promena konačnog BER p_{IR_end} između Alisinog i Bobovog niza na kraju prve 4 iteracije Winnow protokola. 70

Slika 6-4 Odnos između parametra $p_{IRfinal} = \delta = 10^{-4}$ i $p_{IRO}(\delta)=0.0995$. b) Dopustiva oblast za $CR KSG_W$ sistem, sa parametrima Winnowog protokola $N=8$, , $max\ iter = 4$ i gornjom granicom KDR $\delta \leq 10^{-4}$. c) Funkcija $f(p_{IRO})$ i njen maksimum $f(p_{IRO_max})$, koji se postiže za $p_{IRO_max} = 0.0905$, odnosno korespondentno $\varepsilon_{max} = 0.0525$ 72

Slika 6-5 Zavisnost efektivnog kapaciteta tajnosti $ \tilde{K}_s $ od parametra r datog sa (4.14), za različite vrednosti K_G . Za parametar kompresije t je uzeta vrednost $t = 34$.	74
Slika 6-6 Zavisnost osnovne dužine bloka podataka n_{IRO} od parametra r za različite vrednosti $ K_G $.	74
Slika 6-7 Sistem perfektne bezbednosti zasnovan na destilaciji tajnog ključa (SKD) korišćenjem izvora zajedničke slučajnosti realizovanog putem determinističkog generatora (KSG) i IR protokola tipa Winnow.	77
Slika 6-8 Zavisnost maksimalnog efektivnog kapaciteta tajnosti $ \tilde{K}_s _{max}$ od dužine tajnog ključa $ K_G $ (gornja slika). Na istoj slici prikazana je njena asimptotska vrednost $0.5 \cdot (C2 - C1) = 0.5 * 0.1136$. Zavisnost neophodne dužine osnovnog bloka podataka n_{IRO} od iste veličine (donja slika). Step kompresije heš funkcije G je standardno $t = 34$.	81
Slika 7-1 Zavisnost mere opterećenosti javnog kanala E_{BC} u režimu rada idealne sigurnosti	86
Slika 7-2 Zavisnost mere opterećenosti javnog kanala E_{BC} u režimu perfektne sigurnosti.	87
Slika 7-3 Generička šema bezbedne komunikacije sa niskom brzinom prenosa podataka korišćenjem MELPe koda.	92
Slika 7-4 Proširenje generičke šeme prikazane sa lokalnom MELPe sintezom na strani predajnika. Sa $CR(\hat{S}_1, \hat{S})$ je označen izvor zajedničke slučajnosti, formiran od lokalno sintetizovanog govornog signala $\hat{S}_1$ na strani predajnika i govornog signala $\hat{S}$.	92
Slika 7-5 Vlatacom lična kripto platforma za šifrovanje govora dizajnirana za upotrebu u bilo kom dostupnom komunikacionom sistemu	93

Slika 7-6 Generator slučajnih nizova Vlatacoma zasnovan na izvoru entropije prirodnog procesa sa ugrađenom proverom slučajnosti.	93
Slika 7-7 Empirijsko rasprostiranje za jednu sigma standardne devijacije za merene stope generisanja tajnog ključa u režimu perfektne tajnosti, tokom 1000 simulacionih ciklusa predloženog SKD sistema zasnovanog na zajedničkoj slučajnosti (CR), sa početnom vrednošću $n_{IR0} = 2000$ bita.	95
Slika 7-8 Histogram generisanih perfektno tajnih dužina ključeva tokom 1000 simulacija (puna linija). Vertikalna isprekidana linija označava teoretski očekivanu vrednost brzine tajnog ključa $ \tilde{K}_s _{max} = 0.1051$. Mala varijansa pokazuje izuzetno slaganje između eksperimentalnih i teorijskih rezultata..	96

LISTA SKRAĆENICA

AD	Advantage Distillation	Destilacija prednosti
APS-VCS	¹⁰ Autonomous Perfectly Secure Low-Bit-Rate Voice Communication System	Autonomni perfektni bezbedan sistem za govornu komunikaciju sa niskim protokom
BP	Bit Parity	Bit parnosti
BER	Bit Error Rate	Procenat pogrešno prenesenih bita
CR	Common Randomness	Zajednička slučajnost
ECC	Error Correcting Code	Kod za ispravljanje grešaka
¹¹ FIFO	First In First Out	Prvi ušao – prvi izašao
GPSN	Generalized Poisson noise	Generalizovana Poasonova raspodela šuma
IR	Information Reconciliation	Usklađivanje informacija
ISAR	Ideally Secret Autonomous Robust Ciphering	Idealno tajno autonomno robusno šifrovanje
IZS	Source of common coincidence	Izvor zajedničke slučajnosti
JPDF	Joint Probability Density Function	Zajednička funkcija gustine verovatnoće
KAR	Key Acceptance Rate	Veličina prihvatanja ključeva
KDR	Key Disagreement Rate	Veličina neslaganja ključeva
KR	Key Rate	Brzina generisanja ključeva
KSG	Key Stream Generator	Generator ključa
KSG(K)	Shared secret key	Zajednički tajni ključ
LLM	Large language model	Veliki jezički model
LP	Linear prediction	Linearna predikcija
LR	Leakage Rate	Brzina curenja informacija
LSP	Linear Spectral Pairs	Linearni spektralni par

MELPe	Mixed-Excitation Linear Prediction voice coder	Govorni koder sa mešovitom pobudom i linearnom predikcijom
OTP	One-Time-Pad	Jednokratna šifra
PA	Privacy Amplification	Povećanje privatnosti
PKI	Public Key Infrastructure	Infrastruktura javnih ključeva
PRG	Deterministic random sequence generator	Deterministički generator pseudoslučajnih nizova
QKD	Quantum Key Distribution	Kvantna distribucija ključeva
RSSI	Received Signal Strength Indicator	Pokazatelj jačine primljenog signala
SCR	Source of Common Randomness	Izvor zajedničke slučajnosti
SKD	Sequential Key Distillation	Sekvencijalna destilacija ključeva
² SNR	Signal-to-Noise Ratio	Odnos signal šum
ToA	Time of arrival	Vreme dolaska signala
⁵ vPCP-V	Vlacom Personal Crypto Platform for Voice encryption	Vlacom krypto platforma za šifrovanje govora
⁵ vTRNG	Vlacom True Random Number Generator	Vlacom generator slučajnih brojeva
¹³ VoIP	Voice over Internet Protocol	Prenos govora preko internet protokola
K_G	¹ Part of distilled secret key used for refreshing	Deo destilovanog tajnog ključa koji se koristi za osvežavanje
N	Block length of Winnow protocol	Dužina bloka Winnow protokola
K	Distilled secret key	Destilovani tajni ključ
K_S	³ Part of secret key used for encryption	Deo tajnog ključa koji se koristi za šifrovanje
X	Random sequence	Slučajni niz
C_K	Running key (or keystream)	Ključ u upotrebi
Y	Sequence generated by performing a bitwise modulo-2 addition (XOR) of the sequences X and C_K	Niz generisan izvršavanjem sabiranja bit po bit, po modulu 2 (XOR) nizova X i C_K

ε	¹ Parameter of the Bernoulli distribution	Parametar Bernulijeve raspodele
C_S	Secrecy capacity	Kapacitet tajnosti
S	Total information that Eve obtains by observing the public channel during the execution of the SKD protocol	Ukupne informacije koje Eva dobija posmatranjem javnog kanala tokom izvršavanja SKD protokola
Δ_{K_G}	Predetermined K_G equivocation margin	Unapred određena K_G margina ekvivokacije
n_p	¹ Number of total information that Eve obtains by observing the public channel during the execution of the SKD protocol	Ukupan broj informacija koje Eva dobija posmatranjem javnog kanala tokom izvršavanja SKD protokola
m_i	³ binary vector — mask associated with each S_i	binarni vektor — maska povezana sa svakim S_i
$\tilde{C}_i$	Equivalent keystream	Ekvivalentni ključ
$\tilde{X}_i$	Equivalent plaintext	Ekvivalentni otvoreni tekst
t	Security margin	Bezbednosna margina
n_{IRO}	¹ Length of initial Alice and Bob strings before starting IR protocol	Dužina početnih Alisinih i Bobovih nizova pre pokretanja IR protokola
μ_{IR}	Data remaining efficiency	Podaci preostale efikasnosti
n_{IR}	¹ Length of reconciliated sequences after completion of the IR protocol	Dužina usklađenih sekvenci nakon završetka IR protokola
D	Admissible region	Dozvoljeni ¹ region
$\tilde{x}$	Normalized variable	Normalizovana promenljiva
Ψ_U	Upper bound of admissible region	Gornja granica dozvoljenog regiona
Ψ_L	Lower bound of admissible region	Donja granica dozvoljenog regiona
p_{IRO}	Initial BER between Alice's and Bob's sequence	Početni BER između Alisine i Bobove sekvence
W	Sequence after IR protocol	Sekvenca nakon IR protokola

n_b	¹ Number of parity blocks of length N sent by Alice	Broj blokova parnosti dužine N koje je poslala Alisa
n_H	³ Number of transmitted syndromes by Alice	Broj sindroma koje je poslala Alisa
S_b	¹ Class of parity bits computed for each block of length N	Klasa bita parnosti izračunata za svaki blok dužine N
S_H	³ Class of parity bits representing syndrome	Klasa bitova parnosti koji predstavljaju sindrom
p_{IR_end}	¹ BER between Alice's and Bob's sequences at the end of the IR protocol	BER između Alisine i Bobove sekvence na kraju IR protokola
C_1	³ Lower bound of key equivocation at $\epsilon_{max} = 0.0525$	Donja granica ekvivokacije ključa pri $\epsilon_{max}=0,0525$
C_2	Data remaining efficiency at $\epsilon_{max} = 0.0525$	Efikasnost preostalih podataka pri $\epsilon_{max}=0,0525$
r	Parameter equal to $\frac{\Delta K_G}{K_G}$	Parametar jednak $\frac{\Delta K_G}{K_G}$
G	Universal heš function	Univerzalna Haš funkcija
Z	Ciphertext	Šifrat

1. UVOD

Predmet ove doktorska disertacija je nova sinteza izvora zajedničke slučajnosti (IZS) koju važe sledeći uslovi:

1. Opšta dostupnost: Obe strane (Alisa i Bob) mogu efikasno implementirati i posmatrati izvor zajedničke slučajnosti
2. Integritet: Protivnik (Eva) ne može da kontroliše niti menja parametre sintetisanog izvora zajedničke slučajnosti.
3. Optimalnost: Parametri sinteze IZS omogućavaju maksimizaciju kapaciteta tajnosti destilovanih ključeva .
4. Bezbednost ključa: Sintetizovani IZS i pripadajući protokol za sekvencijalnu destilaciju ključeva (SKD) putem javnog kanala garantuju i stopu generisanja ključa i gornju granicu stope curenja informacija prema protivniku. Pretpostavlja se da Eva primenjuje optimalnu strategiju zaključivanja zasnovanu na svim dostupnim javnim informacijama i poznavanju sistema.

Predloženi pristup podrazumeva da Alisa i Bob sintetišu IZS na osnovu generatora ključeva zasnovanog na zajedničkom tajnom ključu, KSG(K). Ukoliko se sekvence generisane ovim generatorom lokalno poremete korišćenjem nezavisnih izvora čiste slučajnosti, rezultujući izvor ponaša se kao ekvivalent Maurer-ovog satelitskog scenarija. Ključna prednost ovog pristupa je što se svi značajni parametri IZS, kao i sam SKD protokol, mogu izraziti u zatvorenoj analitičkoj formi uz teorijsku strogoću. Glavna ranjivost ovog sistema je napad Eva na početni tajni ključ K koji koristi generator. Neizvesnost ovog ključa iz Evine perspektive definiše se preko ekvivokacije mere koju je Šenon označio kao centralnu za procenu bezbednosti sistema sa simetričnim ključem. U ovom radu konstruišemo i analiziramo klasu IZS za koje se može postaviti donja granica na ekvivokaciju ključa K, čime se omogućava bezbedna destilacija ključeva u širokom spektru operativnih parametara.

Koncept destilacije kriptografskih ključeva iz korelisanih izvora prvi je formalizovao Ueli Maurer, koristeći satelitski scenario radi istraživanja kapaciteta tajnosti u prisustvu prislušivača. Od tada je sproveden veliki broj istraživanja praktičnih realizacija ove ideje, posebno u okviru kvantne distribucije ključeva (QKD) i bezbednosti na fizičkom sloju.

Poznati protokoli za usklađivanje kao što su Cascade i Winnow razvijeni su da bi se sekvence između legitimnih strana uskladile uz minimalno curenje informacija. Ovi protokoli su značajno optimizovani, naročito za primenu u uslovima ograničene komunikacije ili visokog nivoa šuma. Analize zasnovane na ekvivokaciji, inspirisane Šenonovim radom, sve češće se koriste za procenu bezbednosti generisanja ključeva . Ipak, većina praktičnih sistema ne poseduje mehanizme za održavanje kontrolisanog nivoa ekvivokacije tokom vremena.

Veštačko generisanje IZS pomoću pseudoslučajnih konstrukata istraživano je, ali retko sa fokusom na analitičku entropijsku ocenu ili povezivanje sa adaptivnim SKD protokolima. Ovaj rad popunjava tu prazninu uvođenjem novog teorijski utemeljenog, analitički obradivog i praktično primenljivog IZS zasnovanog na KSG(K). Ova disertacija uvodi struktuiran pristup sintezi veštačkih izvora zajedničke slučajnosti korišćenjem generatora ključeva sa zajedničkim ključem i lokalnom čistom slučajnošću.

Novi naučni doprinosi i inovativni aspekti ove disertacije obuhvataju sledeće:

Razvoj prilagodljivog izvora zajedničke slučajnosti sa proširenom parametarskom kontrolom, koji funkcioniše funkcionalno ekvivalentno sa poznatim Maurer-ovim modelom, ali uvodi dodatni stepen fleksibilnosti kroz mogućnost transformacije strukture izvora u skladu sa promenljivim uslovima sistema. Ovaj doprinos omogućava bolju optimizaciju performansi u realnim okruženjima i lakšu integraciju u različite bezbednosne arhitekture.

Izvođenje preciznih analitičkih izraza za donje granice ekvivokacije tajnog ključa u scenarijima gde napadač ima pristup delu komunikacije preko javnog kanala. Time se kvantitativno određuje stepen sigurnosti ključa u odnosu na količinu informacija koje mogu biti izložene, što predstavlja važan teorijski alat za dizajniranje sigurnosno robusnih sistema.

Uspostavljanje potpuno autonomne arhitekture sistema za generisanje i osvežavanje ključeva , u kojoj se bez spoljne intervencije vrši dinamička regeneracija kriptografskih ključeva i precizna separacija korisnih (upotrebljivih) od pomoćnih (sistemskih) ključeva . Time se obezbeđuje visok stepen otpornosti na kompromitaciju i omogućava dugoročno očuvanje sigurnosne koherencije.

Unapređenje efikasnosti WINNOW informaciono-rekonstruktivnog protokola kroz njegovu optimizaciju za rad sa kratkim binarnim blokovima. U kontekstu ograničenih resursa i visokih zahteva za vremensku efikasnost, ova optimizacija omogućava precizno i brzo usklađivanje binarnih nizova između krajnjih korisnika, uz minimalne gubitke i greške.

Eliminacija potrebe za tradicionalnom fazom „destilacije prednosti” (advantage distillation), koja je karakteristična za mnoge protokole za zajedničko generisanje ključeva je značajan rezultat. Predloženi metod omogućava direktnu sintezu sigurnih ključeva, bez kompromitovanja tajnosti, čime se značajno smanjuje kompleksnost sistema i ubrzava proces uspostavljanja sigurnog kanala. Disertacija je organizovana na sledeći način:

Nakon uvodnog poglavlja, u kojem su razmotreni ključni pojmovi, kontekst istraživanja i osnovne postavke rada, disertacija se sistematski razvija kroz devet međusobno povezanih poglavlja. Struktura je pažljivo osmišljena tako da prati logički sled razvoja koncepta, metodologije i dizajna sigurnosnog sistema koji je predmet istraživanja.

Drugo poglavlje bavi se teorijskim temeljima vezanim za generisanje, upotrebu i karakteristike kriptografskih ključeva unutar savremenih kriptografskih okvira. Poseban akcenat stavljen je na formalizaciju svojstava koje tajni ključevi moraju ispunjavati kako bi garantovali visoku sigurnost – uključujući dovoljnu količinu entropije, statističku nepredvidivost, kao i koncept takozvane „sveže entropije” (fresh entropy), koja je ključna za otpornost na napade koji se oslanjaju na prethodna saznanja napadača.

Treće poglavlje donosi kritički pregled aktuelne naučne i stručne literature iz oblasti izvora zajedničke slučajnosti (IZS) i tehnika za sintezu sigurnosnih ključeva. Analizirani su postojeći modeli i metode, pri čemu se identifikuju njihove slabosti, ograničenja i neusaglašenosti sa potrebama modernih informaciono-sigurnosnih arhitektura. Ova analiza predstavlja osnov za definisanje istraživačkog problema i obrazlaže potrebu za razvojem novog, efikasnijeg i sigurnijeg modela.

Četvrto poglavlje detaljno opisuje predloženi sistemski okvir, koji funkcioniše kao samostalna, kriptografski neprobojna jedinica za generisanje binarnih nizova sa unapred definisanim korelacionim svojstvima. Ova arhitektura omogućava da se tajni

ključevi kreiraju i distribuiraju u realnom vremenu, bez oslanjanja na komunikacione kanale ili konkretne kriptografske algoritme koji se koriste za zaštitu sadržaja.

Peto poglavlje fokusira se na informaciono-teorijsku analizu razvijenog izvora zajedničke slučajnosti. U okviru ovog poglavlja izvedene su ključne granice sigurnosti kroz metrika kao što su ekvivokacija i količina informacije dostupne neautorizovanim akterima. Takođe, predstavljen je optimalni model rekonstrukcije zasnovan na informacionom protokolu tipa Winnow, koji omogućava efikasnu sinhronizaciju između strane pošiljaoca i primaoca.

Šesto poglavlje se bavi konkretnom implementacijom sistema za generisanje sigurnosnih ključeva (SKD). Opisan je rad determinističkog generatora CR-KSG (Common Randomness Key Stream Generator), zajedno sa integracijom WINNOW-IR protokola. Prikazan je algoritamski postupak, uključujući sve tehničke komponente i operativne mehanizme sistema, kao i analiza njihovog doprinosa ukupnoj sigurnosti rešenja.

Sedmo poglavlje razmatra bezbednosne i implementacione aspekte celokupnog sistema. Diskutuju se praktični izazovi prilikom realne primene, kompromisi između performansi i sigurnosti, kao i uticaj različitih parametara sistema na njegovu robusnost u prisustvu smetnji, napada i drugih neidealnosti koje karakterišu realna komunikaciona okruženja.

Osmo poglavlje donosi sumarne uvide u ostvarene rezultate, naglašavajući originalne doprinose rada. Pored toga, identifikuju se otvoreni problemi i mogućnosti za unapređenje postojećeg modela, uključujući i pravce budućih istraživanja kako u teorijskom, tako i u praktičnom domenu bezbednosnih tehnologija.

Deveto poglavlje sadrži sve korišćene reference, obuhvatajući relevantnu naučnu, tehničku i metodološku literaturu koja je poslužila kao teorijska osnova za koncipiranje i izvođenje istraživačkih koraka predstavljenih u ovoj disertaciji.

2. OSNOVE TEORIJE KRIPTOGRAFSKIH KLJUČEVA

2.1 Istorijski pregled

Kriptografija sa tajnim (simetričnim) ključem jedna je od najstarijih i najtemeljnijih grana kriptografije, sa korenima koji sežu hiljadama godina unazad. Njena osnovna ideja je jednostavna: dva učesnika (Alisa i Bob) dele tajnu informaciju (ključ), koju koriste za šifrovanje i dešifrovanje poruka.

2.1.1 Antička kriptografija i srednji vek

Skitala (5. vek p.n.e.): korišćena u Sparti; cilindrični alat za transpoziciju teksta.

Cezarova šifra: jednostavna zamenska šifra sa fiksnim pomakom (klasičan primer monoalfabetske zamene).

Vigenèrova šifra (16. vek): koristi višestruke abecede prema ključnoj reči. Njenu ranjivost je otkrio Babbage (19. vek), iako je dugo smatrana neprobojnom.

2.1.2 Mehaničko doba i drugi svetski rat

Enigma (Nemačka, 1920–1945.): rotorska elektro-mehanička mašina; njeno razbijanje je predstavljalo istorijski proboj u kriptografiji, što je uradio Turing sa saradnicima 1942. godine.

2.1.3 Teorijska formalizacija i standardi (posle 1949)

Shannon (1949): u radu "Communication Theory of Secrecy Systems" [1], definisao je ključne pojmove: ekvivokacija, perfektna tajnost (perfect secrecy) i bezuslovnu tajnost (unconditional security).

DES (1977): prvi standard simetričnog šifrovanja, razvio IBM, usvojio NBS [2].

AES (2001): savremeni standard zasnovan na Rijndael algoritmu, podržava 128/192/256-bitne ključeva [3].

2.1.4 Teorijske osnove i definicije

Osnovni pojmovi kriptografskog sistema sa tajnim ključem:

Tajni ključ K

Tajni ključ K je poznat isključivo Alisi i Bobu. On predstavlja osnovu za proces šifrovanja i dešifrovanja poruka. Ukoliko treća strana dođe u posed ključa, sigurnost komunikacije je kompromitovana.

Šifrovanje

Proces pretvaranja izvorne poruke M (plaintext) u šifrovani tekst C (ciphertext) pomoću tajnog ključa K označava se kao:

$$C = \text{Enc}_K(M)$$

gde je Enc_K deterministička ili stohastička funkcija šifrovanja, u zavisnosti od algoritma.

Dešifrovanje

Obrnuti proces, u kojem Bob koristi isti tajni ključ K da iz šifrovane poruke C rekonstruiše originalnu poruku M, definiše se kao:

$$M = \text{Dec}_K(C)$$

Pod pretpostavkom da je ključ ispravan i da poruka nije izmenjena, važi:

$$\text{Dec}_K(\text{Enc}_K(M)) = M$$

2.2 Osnove kriptografskih ključeva u teoriji informacija

Ekvivokacija, međusobna informacija i perfektna tajnost u teoriji informacija

U teoriji informacija, ključna mera bezbednosti je tzv. ekvivokacija, označena kao:

$H(K | Z)$ — to je uslovna entropija tajnog ključa K, uzimajući u obzir informacije Z koje su poznate potencijalnom napadaču, koji se tradicionalno naziva Eva (Eve).

Ova veličina predstavlja meru nesigurnosti koju Eva ima u pogledu ključa nakon što je prikupila određene informacije Z , koje mogu poticati iz presretnutih komunikacija (npr. šifrovani tekst, pomoćne informacije, meta podaci i dr.).

Idealna bezbednost:

Za sistem koji poseduje idealnu bezbednost, važi uslov:

$$H(K | Z) = H(K)$$

To znači da informacija Z nije smanjila entropiju ključa — drugim rečima, Eva nije ništa saznala o ključu, čak i nakon što je dobila sve moguće dostupne podatke Z .

Međusobna informacija (mutual information):

Pored ekvivokacije, često se koristi i međusobna informacija između ključa K i poznatih podataka Z , označena kao:

$$I(K; Z) = H(K) - H(K | Z)$$

Ona meri količinu informacija o ključu K koja je sadržana u Z . Ako je međusobna informacija jednaka nuli:

$$I(K; Z) = 0$$

to znači da Z ne nosi nikakvu informaciju o K . U tom slučaju, napadač ne može smanjiti entropiju ključa, tj. ne može suziti skup mogućih vrednosti ključa na osnovu posmatranja. Ključ ostaje statistički tajan. Ovo je ekvivalentno gorepomenutom idealnom slučaju gde je $H(K|Z) = H(K)$.

Perfektna tajnost:

Perfektna tajnost (perfect secrecy), koju je definisao Claude Shannon 1949. godine, izražava se uslovom:

$$P(M | C) = P(M) \quad \forall M, C$$

gde je M — originalna poruka (plaintext), C — šifrovana poruka (ciphertext).

Ova relacija znači da poznavanje šifrovane poruke ne daje apsolutno nikakvu informaciju o izvornom tekstu. Dakle, šifrat je statistički nezavistan od poruke.

Uslov za postizanje perfektne tajnosti:

Shannon je dokazao da perfektna tajnost može biti matematički zagarantovana jedino ako (ako i samo ako) je ispunjen strogi uslov:

Dužina ključa $\geq$ Dužina poruke

U idealnom slučaju, ključ je potpuno slučajan, unapred podeljen između Alise i Boba i upotrebljen samo jednom (One-Time Pad).

Pojmovi poput ekvivokacije, međusobne informacije i perfektne tajnosti omogućavaju kvantitativno merenje sigurnosti kriptografskih sistema.

U praksi se obično ne zahteva savršena tajnost, već što veća ekvivokacija i što manja među informacija između ključa i podataka poznatih napadaču, čime se obezbeđuje visok nivo sigurnosti uz prihvatljive resurse.

2.2.1 Klasifikacija i primena kriptografskih ključeva

Tajni ključevi se koriste u:

- Simetričnim sistemima: AES, ChaCha20,
- Asimetričnim sistemima (za razmenu): RSA, ECC,
- Hibridnim protokolima: TLS, Signal.

Prednost simetričnih metoda: brzina i efikasnost.

Nedostatak: potreba za sigurnom distribucijom ključeva (Tabela 2-1).

Tabela 2-1 Pregled osobina simetričnih, asimetričnih i hibridnih kripto sistema

Tip sistema	Ključ poznat	Primeri	Prednosti	Nedostaci
Simetrični	Alisi i Bobu	AES,	Brza šifrovanje	Potreba za sigurnom distribucijom
Asimetrični	Privatni/javni	RSA, ECC	Laka distribucija ključeva	Sporija šifrovanje
Hibridni	Kombinovano	TLS/SSL, Signal	Efikasnost + sigurnost	Kompleksnost implementacije

2.2.2 Tajni ključevi u destilaciji i sintezi zajedničke slučajnosti

Destilacije tajnog ključa u teoriji informacija

U bezbednosnim komunikacionim sistemima, naročito u kriptografiji baziranoj na fizičkom sloju i kvantnoj kriptografiji, koristi se destilacije tajnog ključa (engl. secret key distillation) kako bi se od sirovih podataka koje dele dve strane (najčešće Alisa i Bob) dobio siguran, tajni ključ koji se može koristiti za šifrovanje.

Ovaj proces počiva na pretpostavci da Alisa i Bob raspolažu koreliranim nizovima podataka — tj. delimično zajedničkom informacijom, koja potiče iz tzv. izvora zajedničke slučajnosti (CR – Common Randomness). Takav izvor može biti, na primer, nivo šuma na komunikacionom kanalu, kvantne fluktuacije, signali RSSI (Received Signal Strength Indicator), vreme dolaska (Time of Arrival) i dr.

Faze protokola za destilaciju tajnog ključa

Destilacije tajnog ključa obično se sprovodi kroz sledeće ključne faze:

1. Estimiranje zajedničkih podataka (Information Estimation)

Alisa i Bob porede određeni deo svojih ulaznih podataka kako bi procenili nivo korelacije i kvalitet zajedničke informacije. Ovo omogućava procenu gubitka informacija usled šuma, grešaka u prenosu i prisustva treće strane (Eve).

2. Usklađivanje informacija (Information Reconciliation)

U ovoj fazi, Alisa i Bob koriste protokole za detekciju i ispravljanje grešaka (npr. Cascade, Winnow, LDPC), kako bi svoje nizove učinili identičnim. Proces se delimično odvija javno, što omogućava Evi da posmatra deo komunikacije. Cilj je da se minimizuje količina informacija otkrivena Evi tokom korekcije, uz istovremeno usklađivanje nizova između Alise i Boba.

3. Povećanje privatnosti (Privacy Amplification)

Nakon korekcije, koriste se kriptografske heš funkcije kako bi se iz zajedničkog niza izdvojio kraći, ali statistički sigurniji ključ K . Ova faza značajno smanjuje informaciju koju Eva može imati o finalnom ključu. Njena neizvesnost postaje veoma visoka.

4. Ekvivokacija finalnog ključa

U idealnim uslovima, tj. kada su estimiranje i korekcija uspešni, a funkcija za povećanje privatnosti korektno izabrana, dobija se destilovani ključ K koji ima visoku ekvivokaciju sa aspekta napadača.

Matematički, to se izražava kao:

$$H(K | Z) \geq t$$

gde je $H(K | Z)$ uslovna entropija ključa u odnosu na sve informacije Z koje Eva ima, a t predstavlja donju granicu sigurnosti.

Destilacije tajnog ključa je ključni proces u savremenoj teoriji sigurnosti, jer omogućava dobijanje kriptografski sigurnih ključeva čak i iz nesigurnih i šumovitih izvora.

Njena snaga leži u činjenici da koristi statističku strukturu zajedničkih podataka, uz primenu teorijskih alata za procenu, korekciju i zaštitu informacije, kako bi se obezbedila visoka sigurnost čak i u prisustvu napadača.

2.2.3 Savremeni simetrični algoritmi

Simetrični algoritmi predstavljaju osnovu većine praktičnih krypto sistema i koriste se za šifrovanje podataka kada isti ključ koristi i pošiljalac i primalac za šifrovanje i dešifrovanje. Savremeni simetrični algoritmi obuhvataju širok spektar konstrukcija, prilagođenih različitim aplikacijama — od visoko bezbednih sistema do uređaja sa ograničenim resursima (npr. IoT).

AES (Advanced Encryption Standard)

Podržava ¹⁶ dužine ključa od 128, 192 i 256 bita, što omogućava fleksibilan nivo sigurnosti.

Zasniva se na nizu iterativnih transformacija (rundi), koje uključuju sledeće korake:

- **SubBytes** — nelinearna zamena bajtova korišćenjem S-kutije,
- **ShiftRows** — permutacija redova u matrici podataka,
- **MixColumns** — linearna transformacija kolona radi širenja difuzije,
- **AddRoundKey** — dodavanje ključa korišćenjem XOR operacije.

AES je standardizovan od strane NIST-a i široko se koristi zbog svoje otpornosti na poznate kriptografske napade.

ChaCha20

Dizajniran kao alternativni sekvencijalni šifarski algoritam za visoke performanse i sigurnost.

Bazira se na ARX principima:

- **Add** (sabiranje po modulu),
- **Rotate** (rotacija bita),
- **XOR** (bitna ekskluzivna disjunkcija).

Odlikuje se velikom brzinom, visokom difuzijom i otpornošću na vremenske i bočne napade.

Koristi se u TLS protokolima i aplikacijama kao što su Google Chrome, WireGuard i dr.

Trivium, Grain, MICKEY

Dizajniran za uređaje sa ograničenim resursima (senzori, RFID, IoT).

Trivium koristi kombinaciju LFSR i nelinearnih povratnih sprega.

Grain kombinuje LFSR i NLFSR za postizanje nelinearnosti i sigurnosti.

MICKEY koristi promenljivu brzinu ažuriranja registara radi pojačane otpornosti na napade.

Iako laki, ovi algoritmi se pažljivo analiziraju kako bi se izbegli kompromisi u bezbednosti.

LFSR i NLFSR (Linearni i Nelinearni registri sa povratnom spregom)

Koriste se u mnogim generatorima pseudoslučajnih nizova i sekvencijalnim šiframa. LFSR je jednostavan i efikasan, ali podložan linearnim napadima ako se koristi samostalno. NLFSR uvodi nelinearnost u funkciju povratne sprege i značajno

povećava otpornost na kriptografske napade. Savremeni dizajni koriste nelinearne komponente da bi osigurali potreban nivo sigurnosti.

Savremeni simetrični algoritmi obuhvataju različite pristupe dizajnu, u zavisnosti od potreba aplikacije — bilo da se radi o visokoj sigurnosti (AES, ChaCha20), ili o energetskej efikasnosti i jednostavnosti (Trivium, Grain). Kritičan aspekt svakog algoritma jeste balans između sigurnosti, performansi i implementacione složenosti.

2.2.4 Distribucija i zamena tajnog ključa

Distribucija kriptografskih ključeva je jedan od najkritičnijih aspekata sigurnih komunikacionih sistema jer omogućava poverljivu distribuciju ključeva između komunikacionih partnera. Bez sigurne distribucije, i najsavremeniji kripto sistemi postaju ranjivi.

Postoje tri glavna pristupa distribuciji kriptografskih ključeva:

1. Fizička distribucija (prethodni dogovor)

Najjednostavniji i najdirektniji način: učesnici unapred fizički razmenjuju ili dogovaraju ključ.

Ovaj metod je praktičan za male mreže i kritične sisteme gde postoji fizička kontrola.

Glavni nedostatak: ne skalira se lako za veće sisteme ili dinamične mreže, a postoji rizik od kompromitacije tokom prenosa ili skladištenja.

2. Distribucija preko javnog ključa (asimetrična kriptografija)

Metode kao što su Difi-Helman(DH) i RSA omogućavaju sigurno uspostavljanje zajedničkog ključa putem nesigurnog kanala.

Difi-Helman protokol omogućava za dve strane da generišu zajednički ključ bez direktnog razmenjivanja ključa.

RSA se može koristiti za sigurno slanje simetričnih ključeva uz pomoć javnih ključeva primalaca.

Ove metode su široko primenjivane u modernim protokolima (TLS, VPN i dr.).

Izazovi: oslanjaju se na složene matematičke probleme (faktorizacija, diskretni logaritmi) i podložne su napadima kvantnih računara u budućnosti.

3. Korišćenje fizičkih izvora entropije

Pojava tehnologija koje koriste fizičke procese kao izvore entropije donela je nove metode za bezbednu distribuciju ključeva.

Primer je QKD (Quantum Key Distribution) — kvantna distribucija ključeva bazirana na principima kvantne fizike, koja pruža teorijski dokazanu sigurnost.

Ove metode omogućavaju generisanje i razmenu ključeva koji su nepredvidivi i otporni na presretanje.

Destilacije ključa u sistemima sa zajedničkom slučajnošću (CR)

U ovim sistemima, Alisa i Bob koriste zajedničku slučajnost (Common Randomness, CR), dobijenu preko komunikacionog kanala ili fizičkih izvora, kao osnovu za sintezu sigurnog ključa.

Kroz postupke estimacije, korekcije grešaka i povećanja privatnosti, iz ovih sirovih i delimično korelisanih podataka izvlače tajni ključ.

Takav pristup je naročito koristan u bežičnim mrežama i IoT sistemima gde je teško ili neekonomično prethodno dogovarati ključeve.

Fizička složenost i otpornost na napade

Distribucija ključeva zasnovana na fizičkim principima često donosi i veću otpornost na aktivne i pasivne napade, jer se oslanja na teško reproducibilne ili nepredvidive fenomene.

Međutim, složenost implementacije i zahtevi za specijalizovanom opremom (npr. kvantni kanali, PUF senzori) mogu predstavljati izazov za praktičnu upotrebu.

Bezbednost sistema zavisi od pravilne kalibracije i procene entropije izvora, kao i od otpornosti na manipulaciju i smetnje u kanalu.

2.2.5 Moderni napadi:

U savremenim kriptografskim sistemima, klasični matematički napadi (poput pokušaja rešavanja problema faktorizacije ili diskretnog logaritma) nisu jedini izvori bezbednosnih pretnji. Napredak tehnologije i sofisticiranost napadača doveli su do

razvoja sofisticiranih tehnika napada koje ciljaju fizičke implementacije krypto sistema. Ovi napadi se nazivaju side-channel i srodni napadi i mogu zaobići matematičke sigurnosne mehanizme analizom ili manipulacijom fizičkih karakteristika uređaja.

1. Side-channel napadi

Side-channel napadi ne ciljaju direktno matematičku sigurnost algoritma, već koriste informacije koje uređaj nehotice „curi“ tokom izvršenja kriptografskih operacija. To su, na primer:

Analiza potrošnje napona (Power Analysis):

Napadač meri potrošnju električne energije uređaja tokom kriptografskog procesa. Različite operacije i podaci mogu imati karakteristične obrasce potrošnje, koje je moguće analizirati da bi se rekonstruisali tajni ključevi.

Postoje dve osnovne vrste:

Simple Power Analysis (SPA) — posmatranje direktnih obrazaca potrošnje,

Differential Power Analysis (DPA) — statistička analiza velikog broja merenja radi otkrivanja sitnijih obrazaca.

Elektromagnetna analiza (Electromagnetic Analysis):

Uređaji tokom rada emituju elektromagnetno zračenje koje može sadržati informacije o internim operacijama. Napadač može koristiti senzore da presretne ove signale i na osnovu njih izvlači tajne podatke.

Analiza vremena izvršavanja (Timing Attacks):

Različiti ulazni podaci ili operacije mogu uzrokovati varijacije u vremenu trajanja kriptografskih funkcija. Merenjem preciznog vremena izvršavanja može se saznati informacija o ključu ili drugim tajnim vrednostima.

Akustična analiza:

U nekim slučajevima, čak i zvuk koji uređaj proizvodi tokom rada može otkriti informacije (npr. zvuk tastature ili zvuk prilikom elektronskih operacija).

2. Ubacivanje grešaka (Fault injection napadi)

Ovi napadi ciljaju na namerno izazivanje grešaka u hardveru ili softveru tokom kriptografskog procesa.

Na primer, napadač može koristiti elektromagnetne pulseve, visoke temperature, napon preko specifikacija ili lasersko zračenje da bi izazvao greške u memoriji ili procesoru.

Posmatranjem rezultata sa greškama, napadač može izvesti zaključke o unutrašnjoj strukturi sistema ili o samom ključu.

Ovaj pristup je naročito efikasan jer mnogi algoritmi ne predviđaju rad u uslovima grešaka i tada mogu otkriti delove tajnog ključa.

3. Ostatak podataka u memoriji (Memory Remanence)

Nakon korišćenja, tajni podaci (npr. kriptografski ključevi) mogu ostati u RAM memoriji uređaja u obliku koji je moguće rekonstruisati.

Ovo predstavlja rizik, posebno u uređajima gde se memorija ne briše sigurno ili gde napadač može pristupiti memoriji fizički ili putem softverskih hakova.

Ostatak podataka u memoriji može omogućiti napadaču da „izvuče“ ključ iako je on navodno uklonjen iz sistema.

Tehnike zaštite od naprednih napada

Da bi se zaštitili od ovih sofisticiranih napada, koriste se različite metode i tehnologije koje mogu biti hardverske, softverske ili kombinovane:

- **Maskiranje**

Maskiranje podataka i operacija je tehnika u kojoj se vrednosti ključeva ili drugih kriptografskih podataka kombinuju sa slučajnim vrednostima (maskama) tokom kriptografskog procesa.

Cilj je da se napadači na kanalu ne povezuju direktno sa stvarnim ključem, već sa njegovim slučajno promenjenim verzijama.

Ovo značajno otežava side-channel analizu jer napadač mora da rekonstruiše i slučajne maske da bi došao do ključa.

- **Fizička zaštita (TPM, ¹²HSM)**

TPM (Trusted Platform Module) i HSM (Hardware Security Module) su specijalizovani hardverski moduli dizajnirani da sigurno skladište i procesiraju kriptografske ključeve.

Ovi moduli imaju zaštitu od fizičkog pristupa i side-channel napada, uključujući senzore za detekciju nasilnog otvaranja, zaštitu od kvarenja i šifrovane interfejsa.

Korišćenjem TPM i HSM, ključevi se nikada ne izlažu u čistom obliku van sigurnog modula, što značajno povećava bezbednost.

- **Dinamička promena ključeva**

Redovna i dinamička promena kriptografskih ključeva značajno otežava napadačima da uspešno iskoriste informacije prikupljene o nekom ključu.

Čak i ako napadač uspe da kompromituje trenutni ključ, brzom zamenom ključeva njegovi napadi postaju beznačajni za buduće sesije.

Implementacije mogu koristiti protokole za automatsku rotaciju ključeva ili dinamičko generisanje novih ključeva na osnovu zajedničke slučajnosti.

Savremeni kriptografski sistemi suočavaju se sa složenim i sofisticiranim napadima koji ciljaju fizičku realizaciju algoritama. Efikasna zaštita zahteva

kombinaciju hardverskih i softverskih mera, uključujući maskiranje, specijalizovane hardverske module i pametnu upravu ključevima. Samo sveobuhvatan pristup može obezbediti sigurnost u realnim uslovima upotrebe.

2.2.6 Novi pravci razvoja – kvantna i postkvantna otpornost

Kvantni računari predstavljaju novu paradigmu računarskih mašina koje koriste principe kvantne mehanike (superpoziciju, uplitanje) za izvođenje računskih zadataka. Za razliku od klasičnih računara, kvantni računari mogu rešavati određene probleme znatno brže.

To ima ogroman uticaj na kriptografiju, jer mnogi klasični kriptografski algoritmi počivaju na matematičkim problemima koje kvantni računari mogu rešiti efikasno:

Shorov algoritam omogućava efikasno faktorizovanje velikih celobrojnih brojeva i računanje diskretnih logaritama, ugrožavajući time algoritme zasnovane na RSA, Difi-Helman i ElGamal sistemima.

Groverov algoritam daje kvadratno ubrzanje pretrage prostora ključeva, što znači da simetrični ključevi treba da budu duplo duži da bi održali isti nivo sigurnosti.

Kvantna otpornost

Kvantna otpornost označava sposobnost krypto sistema da ostane bezbedan čak i u prisustvu napadača koji koristi kvantni računar.

Simetrični algoritmi (npr. AES, ChaCha20) su u principu otporniji na kvantne napade jer Groverov algoritam smanjuje bezbednost za kvadratni koren, što se može kompenzovati dužim ključevima (npr. AES-256).

Algoritmi zasnovani na faktorizaciji i diskretnom logaritmu (RSA, DH) su ranjivi na Shorov algoritam i samim tim nisu kvantno otporni.

Postkvantna (post-quantum) kriptografija

Postkvantna kriptografija je grana kriptografije koja se bavi razvojem algoritama i protokola koji su sigurni i otporni na napade kvantnih računara. Cilj je dizajnirati kriptografske sheme koje:

1. Ne zavise od problema koje kvantni računari mogu lako rešiti (npr. nisu bazirane na faktorizaciji ili diskretnom logaritmu).

2. Mogu se implementirati na klasičnim računarima i uređajima već danas.
3. Obezbeđuju sličan ili bolji nivo sigurnosti.

Glavne kategorije postkvantnih algoritama

Neki od najvažnijih pravaca u postkvantnoj kriptografiji su:

a) Kriptografija zasnovana na rešetkama (Lattice-based cryptography)

Bazirana je na računskim problemima u matematičkim strukturama koje se nazivaju rešetke. Primeri: NTRU, Kyber, Dilithium. Ovi problemi su trenutno smatrani otpornim na kvantne napade. Efikasni su za enkripciju, potpis i ključnu razmenu.

b) Kodna kriptografija (Code-based cryptography)

Bazirana je na problemima kodne teorije, npr. teškoći dekodiranja linearnih kodova (McEliece šema). Veoma otporna na kvantne napade, ali imaju veće dužine ključeva.

c) Multi varijantna kriptografija (Multivariate cryptography)

Bazirana je na teškoći rešavanja sistema multi varijantnih polinomjalnih jednačina nad konačnim poljima.

Koristi se uglavnom za digitalne potpise.

d) Heš-based potpisni algoritmi

Potpisi bazirani na sigurnosti kriptografskih heš funkcija.

Jednostavni i sigurni, ali nisu pogodni za šifrovanje.

e) Ispravljanje grešaka i kvantna kriptografija (QKD)

Ne pripadaju direktno postkvantnoj klasičnoj kriptografiji, ali koriste kvantnu fiziku za direktnu distribuciju ključeva sa dokazivom sigurnošću.

Standardizacija postkvantnih algoritama

NIST (Nacionalni institut za standarde i tehnologiju SAD) vodi međunarodni proces standardizacije postkvantnih kriptografskih algoritama.

Nakon višegodišnjih evaluacija, NIST je odabrao nekoliko kandidata za ključnu razmenu i digitalne potpise koji su optimizovani za bezbednost i performanse u postkvantnom svetu.

Primena ovih standarda će omogućiti tranziciju ka sigurnim sistemima koji mogu izdržati buduće kvantne napade.

Izazovi tranzicije na postkvantnu kriptografiju

- Veće veličine ključeva i potpisa u odnosu na klasične algoritme stvaraju zahteve za dodatnim resursima u memoriji i prenosu.
- Kompatibilnost i interoperabilnost sa postojećim protokolima i sistemima.
- Procena dugoročne sigurnosti u odnosu na nove napade i implementacione rizike.

Obrazovanje i spremnost industrije i korisnika za promene.

Kvantni računari predstavljaju ozbiljan izazov za sadašnje kriptografske sisteme. Razvoj i implementacija postkvantnih algoritama su ključni za očuvanje sigurnosti informacija u budućnosti. Istovremeno, tranzicija mora biti pažljivo planirana kako bi se izbegli prekidi u sigurnosti i usluge.

3. PREGLED RELEVANTNE LITERATURE I MODELA IZVORA ZAJEDNIČKE SLUČAJNOSTI

Koncepcija sinteze ključeva iz korelisanih izvora nije nova – još je Ueli Maurer [6], uveo ovaj model koristeći metaforu satelitskog emitera, u kojem oba korisnika posmatraju istu emisiju sa različitim nivoima šuma, dok treća strana (napadač) ima lošiji ili različit pristup toj emisiji. Ovaj model poslužio je kao inspiracija mnogim daljim istraživanjima, posebno u oblastima kvantne kriptografije (QKD), gde je fizički sloj direktno uključen u bezbednosni model, i u razvoju mehanizama bezbednosti na nivou fizičkog sloja tradicionalnih komunikacionih sistema [4].

U okviru praktičnih realizacija, razvijeni su protokoli kao što su Cascade i Winnow, koji omogućavaju korekciju grešaka i sinhronizaciju sekvenci između komunikacionih strana, a da pri tom minimalizuju količinu otkrivene informacije. Ipak, većina postojećih protokola ne uzima u obzir dinamičku promenu ekvivokacije u vremenu, niti poseduje ugrađene mehanizme za njenu aktivnu kontrolu i adaptaciju [5].

U literaturi se može naći nekoliko pokušaja modelovanja veštačkih izvora zajedničke slučajnosti pomoću determinističkih generatora, ali retko uz teorijski preciznu analizu entropijskih karakteristika i još ređe sa ciljem povezivanja sa sistemima adaptivne destilacije kriptografskih ključeva (SKD). Upravo tu se nalazi originalni doprinos ove disertacije: predlaže se i formalno razrađuje nova metoda za projektovanje veštačkih izvora zajedničke slučajnosti koji su ne samo bezbednosno utemeljeni, već i kompatibilni sa postojećim standardima za distribuciju ključeva u različitim operativnim režimima.

Kao što je dobro poznato, Vernamova šifra [7] ili šifra sa jednokratnom lozinkom (OTP) zadovoljava uslov perfektne tajnosti, a cena koju treba platiti je da je brzina tajnog ključa jednaka brzini poruke. Potražnja za tajnim ključevima je proporcionalno manja ako je brzina poruke niža, što opravdava upotrebu glasovnih kodera sa niskom brzinom prenosa u praktičnim implementacijama [9], [10], [11]. Međutim, problem efikasnog generisanja i distribucije kriptografskih ključeva u slučaju Vernamove šifre je i dalje otvoren.

Dok fizička distribucija ključeva ostaje najjednostavnija, ali nepraktična opcija na velikim udaljenostima, moderniji pristupi, kao što su kvantna distribucija ključeva i korišćenje izvora fizičke entropije, nude obećavajuće metode za buduće sisteme. Kvantna distribucija ključeva je poznata po svojoj dokazivo bezbednoj prirodi, iako zahteva značajnu infrastrukturu [12].

U grupi metoda koje koriste fizičke izvore entropije, posebno mesto zauzimaju metode generisanja i distribucije kriptografskih ključeva korišćenjem protokola za sekvencijalnu destilaciju ključeva (SKD) putem javne diskusije [6], [13], [14]. Njihova implementacija zahteva dva preduslova:

- izvore deljene slučajnosti sa dovoljnim kapacitetom koje dele strane u komunikaciji (Alisa, Bob)
- dodatni autentifikovani komunikacioni kanal odgovarajućeg kapaciteta, koji može biti javan i za koji se pretpostavlja da ga napadač (Eva) prisluškuje.

Uglavnom, većina rešenja u ovoj kategoriji uzima sam bežični kanal kao fizički izvor deljene slučajnosti [15], [16], [17]. Međutim, ovaj pristup je isključen našim zahtevom za autonomijom sistema, što podrazumeva nezavisnost od korišćenog komunikacionog kanala. Mali broj preostalih radova je pretežno povezan sa različitim biometrijskim signalima kao izvorima deljene slučajnosti [18], [19], [20]. Međutim, ne postoje rešenja koja bi se zasnivala na zajedničkim izvorima slučajnosti nezavisno od korišćenih telekomunikacionih kanala, a istovremeno garantovala brzinu generisanja tajnog ključa jednaku brzinama vokodera sa niskom brzinom prenosa podataka od 1,2 kb/s ili 2,4 kb/s.

Dok većina postojećih radova istražuje protokole za generisanje ključeva u datom okruženju, vrlo malo njih se fokusira na zajednički dizajn generisanja ključeva i OTP-a. Jednostavan način bi bio kaskadno ili paralelno generisanje ključa i OTP-a, ali se u literaturi pojavljuju i složenije konstrukcije. Na primer, u [21] je dokazano da korišćenje neusklađenog ključa za OTP nadmašuje klasični OTP sa identičnim ključem.

Najnovija istraživanja su detaljno analizirala protokole za usaglašavanje ključeva i autentifikaciju u okruženjima Interneta stvari (IoT), kao i primenu inteligentnih reflektujućih površina u cilju poboljšanja generisanja tajnih ključeva na fizičkom sloju,

pri čemu su posebno istaknuti praktični izazovi bezbednog uspostavljanja ključeva u uslovima promenljive fizičke sredine.

Istovremeno, napredak u oblasti kvantne obrade informacija i integrisanih fotonskih platformi doveo je do razvoja visoko-performansnih heterodinskih prijemnika, koji omogućavaju sigurnu generaciju kvantnih slučajnih brojeva i distribuciju tajnih ključeva pomoću kvantne komunikacije sa kontinualnim varijablama (CV-QKD), pri čemu se postižu visoke brzine razmene tajnih ključeva.

Takođe su istražene tehnike za generisanje zajedničke slučajnosti na osnovu vremena povratnog putovanja paketa u mrežama za prenos podataka, što predstavlja inovativan pravac u bezbednosti fizičkog sloja. Ovaj pristup omogućava prilagođavanje nivoa tajnosti u zavisnosti od stepena podudarnosti zajedničke slučajnosti kod komunikacionih strana.

Pored toga, slučajna modulacija je iskorišćena za poboljšanje generisanja tajnih ključeva preko optičkih kanala u atmosferi, čime su demonstrirana praktična unapređenja u robusnosti i efikasnosti protokola za distribuciju ključeva.

Ova dostignuća u zbiru ukazuju na rastuće interesovanje za autonomne i adaptivne mehanizme generisanja tajnih ključeva, kako u klasičnim, tako i u kvantnim i hibridnim okruženjima. Time se dodatno potvrđuje i motivacija ove studije — razvoj skalabilnog SKD sistema sa ograničenim curenjem informacije i sposobnošću autonomnog rada.

U prvom koraku predloženog dizajna sistema, izabrali smo standardni MELPe vokoder sa niskom brzinom prenosa podataka od 1,2 kb/s [10], [22] i odgovarajući autentifikovani javni kanal, koji mora biti dostupan tokom rada sistema. U drugom koraku, na osnovu opsežnih testova ovog vokodera u realnim uslovima unutar vPCP-V sistema [23], identifikovali smo zajednički izvor slučajnosti pogodan za generisanje i distribuciju kriptografskih ključeva brzinama koje daleko prelaze 1,2 kb/s. Ovaj izvor se sastoji od lokalno sintetizovanog govornog signala na predajnoj strani (Alisa) i odgovarajućeg sintetizovanog signala na prijemnoj strani (Bob). Razlike između ovih signala potiču od različitih lokalnih izvora slučajnosti, koji se koriste za formiranje kompleksnog pobuđivanja MELP sintetizatora vokodera. Ovaj zajednički izvor slučajnosti može se koristiti u otvorenom režimu govora, koji, po pravilu, prethodi fazi bezbedne glasovne komunikacije. Sve informacije o ulaznom glasu koje teku kroz

javni kanal do Eve tokom izvršavanja SKD protokola nisu relevantne jer je komunikacija otvorena i preko glavnog kanala. Međutim, u fazi bezbedne komunikacije na glavnom kanalu, ove informacije bi značajno smanjile neizvesnost ulaznog niza. Stoga se za ovu fazu uvodi novi sintetizator na strani Alise i Boba, čiji se filteri podešavaju na osnovu tajnih, nasumično izabranih LSP parametara [22], [24]. Ove vrednosti su dostupne i Alisi i Bobu jer su formirane od prethodno destilovanih kriptografskih ključeva .

Pionir koncepta destilacije tajnog ključa iz koreliranih izvora je Ueli Maurer [6], koji je formalizovao satelitski scenario kako bi istražio kapacitet tajnosti u prisustvu prisluškivača. Od tada, brojne studije su istraživale praktične implementacije ove ideje, posebno u kontekstu kvantne distribucije ključeva (QKD) i bezbednosnih okvira fizičkog sloja.

Dobro poznati protokoli za pomirenje kao što su Cascade i Winnow razvijeni su kako bi se poravnali korelirani nizovi između legitimnih strana, uz minimiziranje curenja informacija. Ovi protokoli su prošli kroz opsežnu optimizaciju, posebno za upotrebu u okruženjima sa ograničenom komunikacijom ili visokim nivoom buke.

Analiza zasnovana na ekvivokaciji, inspirisana Šenonovim kapitalnim radom, sve se više primenjuje za procenu bezbednosti protokola za generisanje ključeva. Međutim, većini praktičnih sistema nedostaju mehanizmi za sprovođenje ili održavanje kontrolisanog nivoa ekvivokacije tokom vremena.

Veštačko generisanje CR korišćenjem pseudoslučajnih konstrukcija je istraživano, ali sa ograničenim fokusom na analizu entropije zatvorenog oblika ili integraciju sa adaptivnim SKD protokolima. Ovaj rad se bavi ovom prazninom uvođenjem teorijski ispravnog, analitički upotrebljivog i praktično implementiranog CR izvora zasnovanog na KSG(K).

3.1 Zajednička slučajnost (Common Randomness – CR)

Zajednička slučajnost (Common Randomness – CR) je termin koji označava skup (ili izvor) slučajnih varijabli koje dve (ili više) udaljenih strana – tradicionalno Alisa i Bob – mogu zajednički generisati ili izvesti iz sopstvenih lokalnih osmatranja, u cilju izgradnje međusobno deljenog tajnog ključa, dogovora ili sinhronizacije. Modeli zajedničke slučajnosti predstavljaju formalni okvir za:

- sintezu i ekstrakciju istovetnih (ili visoko korelisanih) bita kod različitih korisnika;
- otporne protokole protiv aktivnih ili pasivnih napadača (Eva);
- konstrukciju kriptografskih ključeva korišćenjem fizičkog sloja umesto (ili u kombinaciji sa) višim slojevima šifrovanja.

Osnovne komponente modela CR uključuju:

- **Izvor slučajnosti:** može biti fizički (npr. šum kanala, vremenska varijabilnost, fazni pomaci, itd.) ili virtuelni (iz matematičkog generatora).
- **Distribuirani pristup:** korisnici posmatraju sopstvene realizacije slučajnih varijabli koje su zavisne, ali ne nužno identične.
- **Nezavisni neprijatelj (Eva):** Eva može imati ograničen ili potpuni pristup komunikaciji, ali ne može u potpunosti rekonstruisati zajednički izvor.

Modeli se mogu klasifikovati u tri glavne grupe prema stepenu kontrole i pouzdanosti izvora:

a) Modeli zasnovani na fizičkom sloju (Physical Layer Security – PLS)

Iskorišćavaju inherentne varijacije u fizičkom kanalu – vremenske varijacije, fazni šum, fluktuacije snage, itd. Primeri:

- Recipročni šum u bežičnim kanalima (npr. Wi-Fi, LTE);
- Vremenski intervali (Time-of-Arrival);
- RSSI (Received Signal Strength Indicator).

b) Modeli zasnovani na determinističkim generatorima

- Alisa i Bob dele zajednički tajni ključ koji pokreće deterministički generator slučajnih nizova (PRG);
- Mogu simulirati zajednički izvor slučajnosti u neprijateljskom okruženju bez fizičkog šuma.

c) Modeli uz pomoć treće strane ili javnog izvora

- Koristi se javni kanal ili pomoćnik (npr. satelit, emitovanje signala);

- Informacije dostupne obema stranama, ali uz dodatne lokalne obrade kako bi se konstruisala CR.

3.2 Satelitski scenario kao izvor zajedničke slučajnosti

Satelitski scenario podrazumeva postojanje spoljnog emitera, npr. komunikacionog satelita, koji emituje signal dostupan Alisi i Bobu, ali sa različitim šumom i kašnjenjem. Eva takođe može da posmatra signal, ali iz različite pozicije i sa drugačijim šumom [6].

a) Model postavke

- Satelit emituje pseudonasumičan ili fizički šuman signal;
- Alisa i Bob posmatraju signal kroz svoje lokalne prijemnike, koji uvode nezavisne šumove;
- Zajednička slučajnost izvodi se iz korelacije signala i lokalnog šuma;
- Eva je prostorno udaljena i posmatra signal iz druge perspektive (dekorelisano u odnosu na Alisu i Boba).

b) Tehnički zahtevi i pretpostavke

- Satelitski kanal se modeluje kao širokopojasni kanal sa tri korisnika;
- Zahteva reciprocitet kanala ili postojanje odgovarajućeg recipročno šumnog efekta (npr. razlika u vremenu dolaska – ToA);
- Izvodi se kvantifikacija i ekstrakcija iz analognih merenja;
- Potrebna je sinhronizacija u vremenu i po frekvenciji;
- U nekim slučajevima koristi se i pomoćna infrastruktura na zemlji za potvrdu sinhronizacije.

c) Prednosti

- Nema potrebe za direktnim komunikacionim linkom između Alise i Boba;
- Obezbeđuje široko dostupnu zajedničku referencu u stvarnom vremenu;
- Korisno u geografskim sredinama bez infrastrukture (npr. vojne ili udaljene misije).

d) Ograničenja

- Visoki zahtevi za precizno vreme i frekvencijsku stabilnost;
- Potencijal za napade ukoliko Eva fizički približi poziciju Alise i Boba;
- Potrebna zaštita od **Replay napada** i **side-channel analiza**.

3.2.1 Primene satelitskog scenarija

- **Kvantna distribucija ključeva (QKD)** putem satelita;
- **Globalna sinhronizacija i izgradnja ključeva** u IoT mrežama;
- **Distribuirane senzorske mreže** i komunikacija između dronova, vozila ili brodova;
- **Bezbedna inicijalizacija uređaja** u neprijateljskom okruženju (bootstrapping).

Modeli zajedničke slučajnosti predstavljaju temelj bezbedne komunikacije zasnovane na fizičkom sloju. Uvođenje satelitskog scenarija kao globalno dostupnog izvora slučajnosti omogućava skalabilne, infrastrukturno nezavisne sisteme koji mogu pružiti pouzdanu osnovu za distribuciju kriptografskih ključeva. Međutim, implementacija ovakvih sistema mora pažljivo tretirati fizičke i sigurnosne izazove, posebno u pogledu sinhronizacije, napada i efikasnosti ekstrakcije.

Satelitski model zajedničke slučajnosti pruža izuzetne mogućnosti za konstrukciju kriptografskih ključeva u široko distribuiranim sistemima. Matematički, ovaj model se svodi na emitovanje signala koji korisnici posmatraju kroz lokalne šumne transformacije, a sinteza ključeva se oslanja na visoku korelaciju signala i efikasnu kvantizaciju. U poređenju sa recipročnim kanalima, satelitski modeli zahteva ju precizniju kontrolu ali nude bolju skalabilnost i otpornost u distribuiranim mrežama.

3.3 Osvrt na upotreba velikih jezičkih modela (LLM)

3.3.1 Osnove pristupa: LLM kao izvor zajedničke slučajnosti

Alisa i Bob mogu da koriste veliki jezički model (LLM) kao deterministički izvor entropije, čime se formira novi tip izvora zajedničke slučajnosti (IZS) koji nije zasnovan na fizičkom sloju već na semantičkoj korespondenciji generativnih odgovora [25], [26].

Ključne faze procesa:

(a) Inicijalizacija: Alisa i Bob počinju sa istim, javno dostupnim LLM-om (npr. GPT, LLaMA, Claude)

(b) Personalizacija modela: Svaki korisnik trenira svoj lokalni model dodavanjem ličnih obučavajućih podataka, čime se kreiraju dva srodna, ali različita modela.

(c) Upiti i odgovori: Kada Alisa i Bob postavljaju identične upite svojim personalizovanim LLM-ovima, njihovi odgovori su delimično preklapajući.

(d) Ekstrakcija binarnih nizova: Odgovori se mapiraju u binarne nizove (npr. ASCII kodiranje), a zatim permutuju pomoću unapred poznate zajedničke permutacije (npr. zasnovane na identitetu ili tajnom ključu).

(e) Destilacija: Dobijeni nizovi se tretiraju kao kandidati za zajednički ključ uz primenu standardnih SKD protokola: informaciono teorijska obrada, korekcija grešaka, povećanja sigurnosti (privacy amplification).

3.3.2 Osobine pristupa zasnovanog na LLM

(a) Deterministički, ali varijabilan izvor: LLM-ovi su po svojoj prirodi deterministički kada se koriste sa istim parametrima i inicijalnim stanjima, ali postaju razlikujući kroz personalizaciju. Ova razlika omogućava delimičnu entropiju, ali istovremeno očuvanje preklapanja odgovora.

(b) Sinteza entropije iz visokodimenzionalnog semantičkog prostora: Entropija se ne generiše fizičkim procesima već kroz divergenciju modela koji su trenirani na različitim korisničkim podacima. Preklapanje u odgovorima zavisi od tematske i semantičke sličnosti podataka kojima su modeli fino podešeni.

(c) Korišćenje prirodnog jezika kao izvora zajedničke informacije: Sistem ne zahteva fizički sinhronizovan kanal niti recipročne merenja. Javni kanal se koristi za koordinaciju upita, a tekstualna forma odgovora omogućava jednostavno mapiranje u binarni domen.

(d) Otpornost na pasivne napade: Pošto Eva nema pristup personalizovanim modelima Alise i Boba, teško može rekonstruisati njihove odgovore čak i ako zna upite. Korišćenje privatne permutacije dodatno štiti binarni niz.

3.3.3 Ograničenja i izazovi pristupa

(a) Entropijska neizvesnost i kontrola: Teško je kvantifikovati tačnu količinu zajedničke entropije koju dva modela dele. Nedovoljna entropija može dovesti do nesigurnog ključa ili nemogućnosti destilacije

(b) Stohastička stabilnost odgovora: Iako su LLM-ovi deterministički kada su temperature niske i parametri fiksirani, u praksi su često nesigurni pri generisanju. To može voditi do razlika u bitovima, čime raste potreba za kompleksnijom korekcijom grešaka.

(c) Bezbednosna analiza protiv naprednih napada: Ako Eva ima sličan LLM i zna strukturu personalizacije, može pokušati rekonstrukciju ili inferenciju odgovora. Potrebna je formalan model protivnika i analiza sigurnosti u pogledu dostupnog znanja o modelima.

(d) Operativna složenost i pouzdanost: Trening i održavanje dva personalizovana LLM-a zahteva znatne resurse. Upotreba LLM-a za SKD ne vrši se u realnom vremenu i zavisi od računarske infrastrukture.

3.3.4 Perspektive i potencijalna primena

Ovaj pristup otvara nove pravce za istraživanje:

Distribuirana generacija ključeva bez fizičke povezanosti; upotreba modela znanja za sintezu entropije u nepouzdanim okruženjima; bezbedna inicijalizacija uređaja bez deljenja fizičkog šuma; primena u scenarijima gde fizički kanali nisu dostupni (npr. tekstualna komunikacija, internet forumi, federativni sistemi).

Upotreba velikih jezičkih modela kao izvora zajedničke slučajnosti predstavlja inovativan, semantički orijentisan pristup destilaciji kriptografskih ključeva. Ključne prednosti uključuju fleksibilnost, nezavisnost od fizičkog sloja i mogućnost široke primene, dok glavni izazovi obuhvataju entropijsku neizvesnost, verifikaciju bezbednosti i operativnu pouzdanost. Ovaj metod zahteva razvoj novih teorijskih

alata za kvantifikaciju semantičke entropije i otpornosti na inferencijalne napade, što predstavlja važan istraživački pravac u modernoj teoriji informacija i kriptografiji i nije predmet ove disertacije.

3.4 Formalizacija izvora zajedničke slučajnosti

Formalizacija izvora zajedničke slučajnosti, u kontekstu statističke nezavisnosti i korelacije, obuhvata analizu odnosa između različitih izvora slučajnih varijabli i njihovu sposobnost da utiču jedni na druge. Postoje različiti načini za modeliranje i analizu takvih odnosa, uključujući korišćenje koncepta zajedničke slučajnosti, kao i analiza determinističkih GPSN i Bernulijevih šumova.

3.4.1 Nezavisnost

Dve slučajne varijable su statistički nezavisne ako znanje o jednoj ne menja verovatnoću druge. Matematički, to znači da je njihova zajednička verovatnoća jednaka proizvodu njihovih pojedinačnih verovatnoća.

3.4.2 Korelacija

Korelacija meri stepen linearnog odnosa između dve slučajne varijable. Pozitivna korelacija ukazuje na to da varijable rastu zajedno, dok negativna korelacija ukazuje na to da jedna varijabla raste kada druga pada. Korelacija ne implicira nužno uzročno-posledičnu vezu.

Formalizacija zajedničke slučajnosti vrši se korišćenjem zajedničke gustine verovatnoće (Joint Probability Density Function - JPDP). Naime, za dve ili više slučajnih varijabli, JPDP opisuje raspodelu verovatnoće zajedničkog pojavljivanja različitih kombinacija vrednosti tih varijabli.

3.4.3 Kovarijanca i korelacija

Kovarijanca i korelacija su mere koje kvantifikuju stepen zajedničke varijacije dve slučajne varijable.

3.4.4 Skalarna slučajna promenljiva (SKD)

U kontekstu formalizacije izvora zajedničke slučajnosti, SKD može se odnositi na koncept skalarnog slučajnog događaja, koji se može posmatrati kao jednodimenzionalna slučajna varijabla.

3.4.5 Uslovna verovatnoća

Uslovna verovatnoća meri verovatnoću događaja pod uslovom da se desio drugi događaj. Ona je ključna za analizu zavisnosti između slučajnih varijabli.

3.4.6 Deterministički GPSN i Bernulijeva šumna injekcija: GPSN (Generalizovani Poissonov šum)

GPSN je stohastički proces koji modelira slučajne događaje u kojima se javljaju rafali ili grupe impulsa. Može se koristiti za modeliranje različitih fenomena u kojima postoji tendencija da se događaji javljaju u grupama.

3.4.7 Bernulijeva šumna injekcija

Bernulijeva šumna injekcija je jednostavan način da se uvede slučajnost u deterministički sistem. Ona podrazumeva dodavanje slučajnih "injekcija" šuma (npr. slučajni impulsi) u signal ili sistem.

Obe metode se koriste za modeliranje i analizu slučajnosti u različitim sistemima, uključujući komunikacione mreže, finansijska tržišta i biološke sisteme.

3.4.8 Primer formalizacije

Razmotrimo dva izvora slučajnosti, X i Y . Ako su X i Y nezavisni, onda je zajednička gustina verovatnoće:

$$f(x, y) = f(x) * f(y)$$

gde je $f(x)$ gustina verovatnoće za X , a $f(y)$ gustina verovatnoće za Y .

Ako su X i Y zavisni, onda se zajednička gustina verovatnoće može izraziti korišćenjem uslovne verovatnoće:

$$f(x, y) = f(y|x) * f(x)$$

gde je $f(y|x)$ uslovna gustina verovatnoće za Y pod uslovom da je X jednak x .

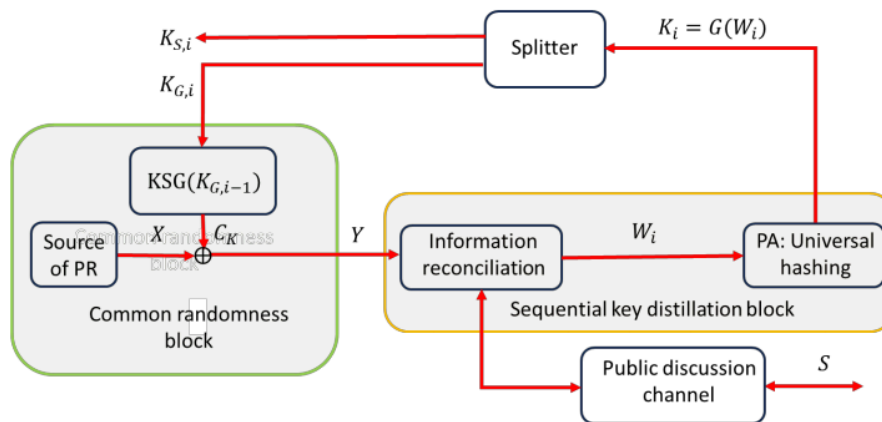
Formalizacija izvora zajedničke slučajnosti je važna za razumevanje i modeliranje kompleksnih sistema. Razumevanje statističke nezavisnosti i korelacije, kao i korišćenje alata kao što su JPDF, kovarijanca i uslovna verovatnoća, omogućava analizu i predviđanje ponašanja takvih sistema.

4. ARHITEKTURA NOVOG PERFEKTNO TAJNOG KRIPTO SISTEMA

Dokazaćemo kako je moguće projektovati novi autonomni, perfektно tajni sistem za prenos govora, čiji je sastavni deo podsistem za generisanje i distribuciju potrebne količine kriptografskih ključeva u realnom vremenu [5].

4.1 Arhitektura sistema sa GPSN(K)

Slika 4 1 Autonomni SKD sistemi koji koriste sintetički izvor zajedničke slučajnosti zasnovan na zajedničkom generatoru ključeva $KSG(G)$ i lokalnoj čistoj slučajnosti. Prikazana je opšta arhitektura predloženog autonomnog sistema za destilaciju kriptografskih ključeva na osnovu javne diskusije [5].



Slika 4-1 Autonomni SKD sistemi koji koriste sintetički izvor zajedničke slučajnosti zasnovan na zajedničkom generatoru ključeva $KSG(K_G)$ i lokalnoj čistoj slučajnosti.

Sistem se sastoji iz tri podsistema:

1. CR bloka koji vrši funkciju izvora zajedničke slučajnosti,
2. SKD bloka koji obavlja IR i PA funkciju,
3. Splitera koji raspodeljuje destilovani tajni ključ K na deo K_G za osvežavanje tajnog ključa $KSG(K_G)$ i deo K_S za dalju kriptografsku upotrebu. Dužine K_G i

K_S mogu biti proizvoljne, pod uslovom da njihova ukupna dužina zadovoljava

$|K| = |K_C| + |K_S|$, i obično se biraju prema operativnim zahtevima sistema.

U CR bloku se u svakom ciklusu rada sistema formira izlazni niz Y sabiranjem po modulu dva nizova X i C_K :

$Y = X \oplus C_K$	(4.1)
--------------------	-------

gde je X niz raspodeljen po Bernulijevoj raspodeli, generisan lokalnim izvorom čiste slučajnosti:

$X \sim B(\varepsilon), \varepsilon = Pr\{X = 1\}, 0 < \varepsilon \leq 1, ,$	(4.2)
---	-------

a niz C_K je tekući ključ generisan generatorom $KSG(K_C)$, sa tajnim ključem K_C .

Primedba 4.1

Ukoliko Alisa i Bob imaju unapred dogovoren zajednički tajni ključ K_C , tada mogu generisati svoje lokalne nizove Y_A i Y_B [5]:

$Y_A = X_A \oplus C_K, Y_B = X_B \oplus C_K.$	(4.3)
---	-------

Verovatnoća njihovog razlikovanja, odnosno BER je:

$p_{AB} = P(Y_A \oplus Y_B = 1) = P(X_A \oplus X_B = 1) = \varepsilon_A * \varepsilon_B,$	(4.4)
---	-------

gde je $*$ oznaka za binarnu konvoluciju:

$p * q = p(1 - q) + (1 - p)q, 0 \leq p, q \leq 1.$	(4.5)
--	-------

Ukoliko se usvoji da je $\varepsilon_A * \varepsilon_B = \varepsilon$, dobijamo:

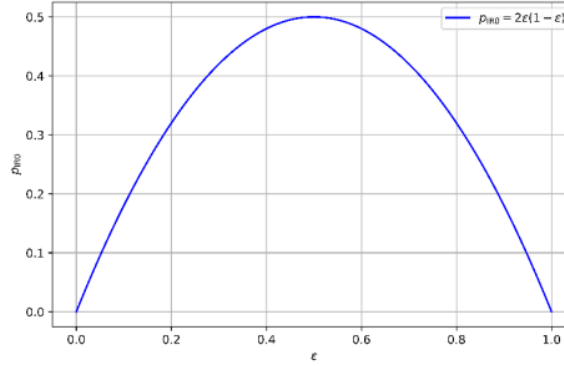
$p_{AB} = 2 \varepsilon (1 - \varepsilon).$	(4.6)
---	-------

odakle sledi, i veza u obrnutom smeru, koja će biti od interesa u daljem tekstu:

$\varepsilon = \frac{1}{2} (1 - \sqrt{1 - 2p_{AB}}).$	(4.7)
---	-------

4.2 Statističko mapiranje na Mauero model

Predloženi izvor CR, možemo smatrati svojevrsnim izvorom Maureovog satelitskog scenarija, u kome se kontrolom parametra ε , može postići bilo koji željeni BER između Alisinog i Bobovog niza, videti Slika 4-2 parametar ε pomoću koga se može postići željeni BER [5] .



Slika 4-2 Parametar ε pomoću koga se može postići željeni BER

Napomenimo da je ovakvu preciznu kontrolu korelacionih svojstava nizova generisanih u Mauerovom satelitskom scenariju, praktično nemoguće ostvariti, [29]. Štaviše, ukoliko Eva ne poseduje tajni ključ K_E , tada je verovatnoća greške između njenog i Alisinog ili Bobovog niza data sa:

$$p_{EA} = P(Y_E \oplus Y_A = 1) = P(X_E \oplus C_{KE} \oplus X_A \oplus C_K) = 0.5 \quad (4.8)$$

budući da je:

$$C_{KE} \oplus C_K \sim B(0.5), \quad (4.9)$$

gde je sa C_{KE} označen niz koji generiše $KSG(K_{KE})$, sa Evinim tajnim ključem $K_{KE} \neq K$.

Uslov (4.9) je obavezno svojstvo svakog dobrog kriptografskog algoritma $KSG(K)$, i u tesnoj vezi je sa tzv. lavinskim efektom. Na sličan način dobijamo da je:

$$p_{EB} = P(Y_E \oplus Y_B = 1) = P(X_E \oplus C_{KE} \oplus X_B \oplus C_K) = (\varepsilon_E * \varepsilon_B) * 0.5 = 0.5 \quad (4.10)$$

Slika 4-3 prikazuje ekvivalentni Maueroz satelitski scenario, u kome ulogu satelita igra $KSG(K_G)$, koji emituje ključ za šifrovanje C_K . Na ovaj signal se prema Alisi, Bobu i Evi superponiraju binarni aditivni šumovi, koji su u slučaju Alisinog i Bobovog kanala jednaki sekvencama lokalnih izvora čiste slučajnosti raspodeljenih shodno $B(\varepsilon)$. Evina optimalna strategija je da za X_E odabere sekvencu [5]:

$X_E = C_{KE} \oplus E_E, E_E \sim B(\varepsilon)$	(4.11)
--	--------

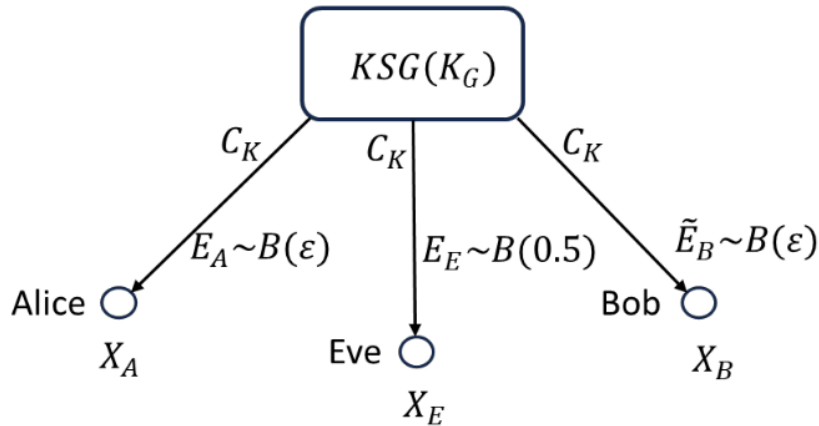
po strukturi jednaku Alisinoj i Bobovoj sekvenci X_A i X_B , ali sa svojim ključem za šifrovanje C_{KE} . Tada je Evin ekvivalentni binarni šum $\tilde{E}_E$ u odnosu na satelitski signal C_K jednak:

$X_E = C_{KE} \oplus E_E = C_K \oplus (C_{KE} \oplus C_K \oplus E_E) = C_K \oplus \tilde{E}_E$	(4.12)
--	--------

$\tilde{E}_E = C_{KE} \oplus C_K \oplus E_E$	(4.13)
--	--------

koja je raspodeljena po Bernuliju sa parametrom:

$\varepsilon_E = (0.5 * 0.5) * \varepsilon = 0.5 \cdot$	(4.14)
---	--------



Slika 4-3 Ekvivalentni Maueroz satelitski scenario. Satelit emituje ključ za šifrovanje C_K , a na tri nezavisna kanala ka Alisi, Bobu i Evi deluju šumovi E_A , E_B i $\tilde{E}_E$, respektivno.

4.3 Konstrukcija i podešavanje parametara

Dobro je poznato da u slučaju satelitskog scenarija, [8], kapacitet tajnosti, dakle, maksimalna dužina tajnog ključa koja može biti destilovana u prisustvu prislušivača je:

$$C_S = \min\{I(X_A; X_B), I(X_A; X_B | X_E)\}, \quad (4.15)$$

gde $I(X;Y)$ označava međusobnu informaciju između X i Y , dok $I(X;Y|Z)$ označava međusobnu informaciju uslovljenu sa Z . Imajući u vidu (4.8) i (4.10), zaključujemo da je Evin niz X_E nezavisan od Alisinog i Bobovog niza X_A i X_B , što redukuje (4.15) na:

$$C_S^{max} = I(X_A; X_B). \quad (4.16)$$

Prednost SKD strategije je dokazano postizanje svih stopa tajnog ključa nižih od kapaciteta tajnosti C_S , kao i njena eksplicitna praktična implementacija [6]. U SKD bloku se prvo primenjuje neki pogodno odabran algoritam za usklađivanje informacija (IR, Information Reconciliation) čija je osnovna funkcija eliminacija razlika koje postoje u Alisinom i Bobovom nizu razmenom različitih tipova pariti informacija po raspoloživom javnom autentifikovanom kanalu [28], [29], [6]. Kao rezultat ove faze, Alisa i Bob raspolažu sa velikom verovatnoćom identičnim nizovima W_i , slika 4.1. U finalnoj fazi SKD protokola, sprovodi se pojačavanje privatnosti (Privacy Amplification-PA), tako što se Alisa i Bob po javnom kanalu dogovore o izboru funkcije kompresije G da bi se iz W_i izdvojio kraći niz K_i o kome Eva ima samo zanemarljivu količinu informacija [30], [31].

U splitter bloku se iz destilovanog ključa K_i selektuje ključ K_{Gi} za zamenu unutrašnjeg ključa $KSG(K_{G,i-1})$ dajući obnovljeni $KSG(K_{G,i})$, dok se preostali deo K_{Si} izdvaja za odabranu dalju upotrebu. Sa stanovišta krajnje namene sistema, brzina generisanja upotrebljivih kriptografskih ključeva je jednaka brzini generisanja K_{Si} [5].

Brzina osvežavanja $KSG(K_{G,i})$ je tako izabrana da Evina ekvivokacija:

$H(K_{G,i} S_i) \geq \Delta_{KG}, 0 \leq \Delta_{KG} \leq K_{G,i} \text{ za } \forall i, i=0,1,2,\dots$	(4.17)
---	--------

nikada ne bude manja od unapred zadate margine Δ_{KG} za svako i , gde je sa S_i označena ukupna informacija koju Eva dobija opserviranjem javnog kanala u toku izvršenja SKD protokola za i -ti blok [5].

Na kraju, sažimamo osnovne pretpostavke koje stoje iza dizajna predloženog autonomnog sistema za destilaciju tajnog ključa (SKD), prikazanog na Slici 4-1. Predložena arhitektura funkcioniše pod sledećim uslovima:

- **Unapred podeljeni tajni ključ KG** dostupan je i Alisi i Bobu, koristi se za inicijalizaciju generatora toka ključeva KSG(KG), i obnavlja se bezbedno u svakoj komunikacionoj rundi.
- **Obe strane poseduju pouzdane lokalne izvore prave slučajnosti**, koji generišu nizove sa Bernulijevom raspodelom i podesivim parametrom ϵ , što omogućava precizno podešavanje stope grešaka u sistemu (BER), čime se simulira sintetička varijanta Maurerovog satelitskog modela.
- **Generator ključeva KSG(KG)** zadovoljava tzv. *avalanche* kriterijum — bez poznavanja ključa KG, izlaz iz generatora je statistički neprepoznatljiv od Bernulijevog niza sa verovatnoćom 0.5 za protivnika.
- **Na raspolaganju je autentifikovani javni kanal** koji se koristi za protokole korekcije grešaka (IR) i izravnivanja privatnosti (PA); pretpostavlja se da napadač može da ga posmatra, ali ne i da ga menja.
- **Napadač (Eva)** se modeluje kao entitet sa neograničenim računarskim mogućnostima (model informaciono-teorijske bezbednosti), sa potpunim pristupom javnom kanalu, ali bez pristupa tajnom ključu KG niti sinhronizovanom toku ključa.
- **Sistem koristi efikasne IR protokole**, koji omogućavaju Alisi i Bobu da usklade svoje nizove i tako postignu brzine generisanja tajnog ključa blizu teorijske granice tajnosti (secrecy capacity).
- **Faza izravnivanja privatnosti (PA)** oslanja se na univerzalne heš funkcije i pretpostavlja dovoljno veliku uslovnu Renijevu entropiju (ili Šenonovu

ekvivokaciju) između usklađenih nizova i onoga što Eva može da zaključi, čime se minimizira curenje informacija.

- **Bezbednost sistema se ostvaruje po svakom ciklusu posebno**, gde se svaki novi ključ KG, generisan preko KSG, ispunjava zadate kriterijume, održavajući potrebnu marginu tajnosti u odnosu na informacije koje Eva može prikupiti iz javnih komunikacija.

Ove pretpostavke omogućavaju da arhitektura funkcioniše samostalno i bez spoljne intervencije, obezbeđujući kontinuiranu i bezbednu destilaciju tajnog ključa pod realističnim ograničenjima informaciono-teorijskog modela bezbednosti.

5. INFORMACIONO-TEORIJSKA ANALIZA IZVORA ZAJEDNIČKE SLUČAJNOSTI

Teorema 1

Neka je skup informacija dostupan Evi po javnom kanalu u toku izvršenja IR faze nekog SKD protokola dat sa $S = \{S_i\}$, $|S| = n_p$, gde je [5]:

$S_i = \sum_{j=1}^{N_i} Y_j \cdot m_{ij}.$	(5.1)
--	-------

Sa m_i je označena binarni vektor maska pridružena svakom S_i , oblika:

$m_i = [m_{i1}, m_{i2}, \dots, m_{iN_i}], \quad m_{ij} \in \{0,1\}.$	(5.2)
--	-------

Tada je donja granica ekvivokacije tajnog ključa $KSG(K_G)$ na osnovu opservacija sa javnog kanala data sa:

$H(K_G S_1, S_2, \dots, S_{n_p}) \geq K_G - n_p \left(1 - \frac{1}{n_p} \sum_{i=1}^{n_p} h_b(\varepsilon_i) \right)$	(5.3)
---	-------

$\varepsilon_i = \frac{1}{2} \left(1 - (1 - 2\varepsilon)^{\sum_{j=1}^{N_i} m_{ij}} \right)$	(5.4)
---	-------

gde je ε parametar Bernulijeva raspodele $B(\varepsilon)$, po kojoj je raspodeljena slučajna veličina X , a h_b je oznaka za funkciju binarne entropije:

$h_b(x) = -p \log(p) - (1-p) \log(1-p), \quad p \in (0,1).$	(5.5)
---	-------

Dokaz

Shodno [1], za svaki simetrični šifarski sistem $\{K, X, Y\}$, gde je K tajni ključ, X poruke, a Y šifrat, važi [5]:

$H(K Y) = H(K) + H(X) - H(Y).$	(5.6)
----------------------------------	-------

S druge strane, na osnovu (3.1) važi:

$S_i = \sum_{j=1}^{N_i} (X_j \oplus C_j) \cdot m_{ij} = \sum_{j=1}^{N_i} X_j \cdot m_{ij} \oplus \sum_{j=1}^{N_i} C_j \cdot m_{ij} = \tilde{X}_i \oplus \tilde{C}_i.$	(5.7)
---	-------

Stoga se opservacije S_i na javnom kanalu mogu smatrati šifratom ekvivalentnog šifarskog sistema $\{K_G, \tilde{X}_i, S_i\}$, budući da je svaki od nizova $\tilde{C}_i$ generisan korespondentnim $GPSN_i(K_G)$ sa identičnim tajnim ključem K_G . Entropija ekvivalentnog otvorenog teksta $\tilde{X}_i$ data je sa [5]:

$H(\tilde{X}_i) = H(\sum_{j=1}^{N_i} X_j \cdot m_{ij}) = h_b(\varepsilon_i),$ $\varepsilon_i = \frac{1}{2} \left(1 - (1 - 2\varepsilon)^{\sum_{j=1}^{N_i} m_{ij}} \right).$	(5.8)
--	-------

Naime, (3.8) direktno sledi iz činjenice da je $\tilde{X}_i$ suma $\sum_{j=1}^{N_i} m_{ij}$ iid slučajnih veličina X_j raspodeljenih u skladu sa to $B(\varepsilon)$.

Ukoliko opservacije $\{S_i\}$ na javnom kanalu posmatramo kao šifrat šifarskog sistema $\{K_G, X, S\}$, tada su u važnosti sledeće jednakosti [5]:

$H(K_G S_1) = H(K_G) + h_b(\varepsilon_1) - H(S_1),$ $H(K_G S_2) = H(K_G) + h_b(\varepsilon_2) - H(S_2),$ $H(K_G S_{n_p}) = H(K_G) + h_b(\varepsilon_{n_p}) - H(S_{n_p}),$	(5.9)
---	-------

čijim sabiranjem dobijamo [5]:

$\sum_{i=1}^{n_p} H(K_G S_i) = n_p H(K_G) + \sum_{i=1}^{n_p} h_b(\varepsilon_i) - \sum_{i=1}^{n_p} H(S_i).$	(5.10)
---	--------

Budući da su S_i međusobno nezavisni, važi:

$\sum_{i=1}^{n_p} H(K_G S_i) = H(K_G S_1, S_2, \dots, S_{n_p}) - (n_p - 1)H(K_G),$	(5.11)
--	--------

što zamenom u (3.7) daje:

$H(K_G S_1, S_2, \dots, S_{n_p}) = H(K_G) + \sum_{i=1}^{n_p} h_b(\varepsilon_i) - \sum_{i=1}^{n_p} H(S_i).$	(5.12)
---	--------

Imajući u vidu da za entropiju važi nejednakost $H(S_i) \leq 1$, dobijamo:

$H(K_G S_1, S_2, \dots, S_{n_p}) \geq K_G + \sum_{i=1}^{n_p} h_b(\varepsilon_i) - n_p$	(5.13)
--	--------

što daje tvrdnju (3.3) teoreme. Ovim je dokaz završen [5].

Primedba 5.1

Poznavanje donje granice ekvivokacije tajnog ključa K_G , daje nam mogućnost da formulišemo uslove pod kojim ova granica nikada neće pasti ispod unapred zadatog praga Δ_{K_G} . Shodno (5.3), ako je ispunjen uslov:

$ K_G + \sum_{i=1}^{n_p} h_b(\varepsilon_i) - n_p \geq \Delta_{K_G}, \quad 0 \leq \Delta_{K_G} \leq K_G ,$	(5.14)
--	--------

tada Eva na osnovu opservacija $S = \{S_i\}$, $|S| = n_p$ sa javnog kanala u toku izvršenja datog IR protokola, ne može da smanji početnu neodređenost ključa K_G na manje od Δ_{K_G} , $0 \leq \Delta_{K_G} \leq |K_G|$.

Definicija 5.1

Dopustiva oblast $D(\varepsilon, \Delta_{K_G}, K_G, t, K_S)$ rada sistema sa slike definisana je sledećim ograničenjima:

$0 < \Delta_{K_G} < K_G$	(5.15)
--------------------------	--------

$H(K_G S_1, S_2, \dots, S_{n_p}) \geq \Delta_{K_G}$	(5.16)
---	--------

$ K = K_S + K_G $	(5.17)
-----------------------	--------

$ K + t \leq n_{IR0} \cdot \mu_{IR}$	(5.18)
$IE = n_{IR0} \cdot h_b(\varepsilon) + K_G \geq K $	(5.19)
$P\{K_A \neq K_B\} \leq \delta$	(5.20)

gde je t parametar sigurnosti, n_{IR0} je dužina početnih nizova koje poseduju Alisa i Bob pre početka IR protokola, dok je μ_{IR} takozvana efikasnost preostalih podataka, definisana kao odnos dužine n_{IR} rekonzilijovanih sekvenci nakon završetka rada IR protokola i dužine početnih nizova, tj.:

$\mu_{IR} = \frac{n_{IR}}{n_{IR0}}.$	(5.21)
--------------------------------------	--------

Sa IE je označena tzv. novi ne konvencionalni izvor entropije, inovativna ili osvežena entropija [3]. Za razmatrani sistem ona je jednaka količini entropije koju lokalni izvor slučajnosti ubacuje u sistem.

Uslov (5.15) obezbeđuje izbor donje granice ekvivokacije ključeva K_G , date sa (5.16). Uslov (5.17) obezbeđuje autonomnost sistema u pogledu održavanja ove donje granice. Ovo se ostvaruje kroz regularno obnavljanje (osvežavanje) ključeva K_G , nakon svakog bloka novo generisanih nizova $\{Y_i\}$ dužine n_{IR0} , pri čemu u svakom ciklusu sistem istovremeno destiluje i ključeva K_S za nezavisnu upotrebu. Uslov (5.18) dovodi u vezu dužinu destilovanih ključeva $|K|$, security marginu t , odnosno stepen kompresije PA bloka, sa dužinom usaglašanih sekvenci nakon IR faze, [6], [32]. Uslov (5.19) daje najstroži zahtev u pogledu dužine destilovanih ključeva i količine uvedene inovativne entropije u svakom ciklusu rada sistema. Preko uslova (5.20) kontroliše se veličina neslaganja ključeva (Key Disagreement Rate, KDR). Tipične vrednosti za t su reda 30 do 40, a za δ reda 10^{-5} .

Primedba 5.2

Dopustiva oblast $\tilde{D}$ se može definisati i nad veličinama koje su normalizovane dužinom n_{IRO} , što omogućava jasniju interpretaciju i vizualizaciju. Uvedimo sledeće oznake za normalizovane veličine od interesa:

$\tilde{\Delta}_{K_G} = \frac{\Delta_{K_G}}{n_{IRO}}, \tilde{K}_G = \frac{K_G}{n_{IRO}}, \tilde{K}_S = \frac{K_S}{n_{IRO}}, \tilde{K} = \frac{K}{n_{IRO}}, \tilde{IE} = \frac{IE}{n_{IRO}}, \tilde{t} = \frac{t}{n_{IRO}}$	(5.22)
--	--------

koje sada možemo interpretirati kao odgovarajuće veličine. Odgovarajuća definicija normalizovane dopustive oblasti $\tilde{D}(\varepsilon, \tilde{\Delta}_{K_G}, \tilde{K}_G, \tilde{t}, \tilde{K}_S)$ data je skupom uslova:

$0 < \tilde{\Delta}_{K_G} < \tilde{K}_G$	(5.23)
$\tilde{H}(K_G S_1, S_2, \dots, S_{n_p}) \geq \tilde{\Delta}_{K_G}$	(5.24)
$ \tilde{K} = \tilde{K}_S + \tilde{K}_G $	(5.25)
$ \tilde{K} + \tilde{t} \leq \mu_{IR}$	(5.26)
$\tilde{IE} = h_b(\varepsilon) + \tilde{K}_G \geq \tilde{K} $	(5.27)
$P\{K_A \neq K_B\} \leq \delta.$	(5.28)

Posebno je zgodno prikazati dopustivi region $\tilde{D}$ u koordinatama $(Rates, p_{IRO})$, gde je p_{IRO} inicijalni BER p_{AB} između Alisinog i Bobovog niza na početku IR protokola. Teorema 2 daje donu i gornju granicu dopustive oblasti $\tilde{D}$ u koordinatama $(Rates, p_{IRO})$ u opštem slučaju.

5.1 Destilacija tajnog ključa i informatička rekonsilijacija

Teorema 2 [5]

Neka je skup informacija dostupan Evi po javnom kanalu u toku izvršenja IR faze nekog SKD protokola dat sa $S = \{S_i\}$, $|S| = n_p$, gde je S_i dato sa (5.1), a m_i označava binarni vektor-masku pridruženu svakom S_i , oblika (3.2). Neka je n_{IRO} početna

dužina, a p_{IRO} početni BER između Alisinog i Bobovog niza. Tada je dopustiva oblast $\tilde{D}$ ograničena gornjom:

$$\Psi_U(p_{IRO}, \mu_{IR}) = \min \left\{ |\tilde{K}_G| + h_b \left(\frac{1}{2} (1 - \sqrt{1 - 2 p_{IRO}}) \right), \mu_{IR}(p_{IRO}) - \tilde{\epsilon} \right\}, \quad (5.29)$$

i donjom granicom:

$$\Psi_L(p_{IRO}, \mu_{IR}) = 1 - \mu_{IR}(p_{IRO}) - \frac{1}{n_{IRO}} \sum_{i=1}^{n_p} h_b \left(\frac{1}{2} \left(1 - (1 - 2 p_{IRO})^{\frac{1}{2} \sum_{j=1}^{N_i} m_{ij}} \right) \right) \quad (5.30)$$

gde je μ_{IR} stepen efikasnosti primenjenog IR protokola.

Dokaz

Za svako fiksirano p_{IRO} , gornja granica $\Psi_U(p_{IRO}, \mu_{IR})$ se podudara sa maksimalnim mogućim rate destilovanog ključa, odnosno:

$$\Psi_U(p_{IRO}, \mu_{IR}) = \max \{ |\tilde{K}| \}. \quad (5.31)$$

Na osnovu ograničenja (3.26) i (3.27) zaključujemo da istovremeno mora da važi:

$$|\tilde{K}| \leq \mu_{IR} - \tilde{\epsilon} \text{ i } |\tilde{K}| \leq \tilde{I\tilde{E}} = |\tilde{K}_G| + h_b(\epsilon), \quad (5.32)$$

odakle sledi:

$$\Psi_U(p_{IRO}, \mu_{IR}) = \min \{ |\tilde{K}_G| + h_b(\epsilon), \mu_{IR}(p_{IRO}) - \tilde{\epsilon} \}. \quad (5.33)$$

Donja granica se podudara sa minimalnim mogućim rate destilovanog ključa koji obezbeđuje autonomnost i zadatu donju granicu ekvivokacije tajnog ključa (5.24) za zadato p_{IRO} , odnosno:

$$\Psi_L(p_{IRO}, \mu_{IR}) = \min \{ |\tilde{K}| \}. \quad (5.34)$$

Iz (5.25) i (5.14) nakon normiranja sa n_{IRO} dobijamo:

$$|\tilde{K}| \geq \tilde{\Delta}_{K_G} + |\tilde{K}_S| - \frac{1}{n_{IRO}} \sum_{i=1}^{n_p} h_b(\epsilon_i) + \frac{n_p}{n_{IRO}}. \quad (5.35)$$

Imajući u vidu da je:

$$\frac{n_p}{n_{IRO}} = \frac{n_{IRO} - \mu_{IR} n_{IRO}}{n_{IRO}} = 1 - \mu_{IR}, \quad (5.36)$$

kao i da desna strana (5.35) ima minimalnu moguću vrednost za $\tilde{\Delta}_{K_G} = 0$ i $|\tilde{K}_S| = 0$, dobijamo:

$$\Psi_L(p_{IRO}, \mu_{IR}) = \min\{|\tilde{K}|\} = 1 - \mu_{IR} - \frac{1}{n_{IRO}} \sum_{i=1}^{n_p} h_b(\varepsilon_i). \quad (5.37)$$

Uzimajući u obzir (3.8) i (2.7), nalazimo da je:

$$\varepsilon_i = \frac{1}{2} \left(1 - (1 - 2\varepsilon)^{\sum_{j=1}^{N_i} m_{ij}} \right) = \frac{1}{2} \left(1 - (1 - 2 p_{IRO})^{\frac{1}{2} \sum_{j=1}^{N_i} m_{ij}} \right) \quad (5.38)$$

što zamenom u (5.37) daje tvrdnju (5.30). Ovim je dokaz teoreme završen.

Na osnovu teoreme 2, neposredno sledi da je za zadato $p_{IRO} = p_{IRO}^*$, $p_{IRO}^* \in \tilde{D}$, maksimalna brzina destilovanih ključeva:

$$|\tilde{K}|_{max} = \Psi_U(p_{IRO}^*, \mu_{IR}), \quad p_{IRO}^* \in \tilde{D}. \quad (5.39)$$

Za fiksirano $|\tilde{K}_G|$, s obzirom na uslov (5.25), maksimalna brzina upotrebljive komponente destilovanih ključeva je data sa:

$$|\tilde{K}_S|_{max} = |\tilde{K}|_{max} - |\tilde{K}_G| = \Psi_U(p_{IRO}^*, \mu_{IR}) - |\tilde{K}_G|, \quad p_{IRO}^* \in \tilde{D}, \quad (5.40)$$

a maksimalna moguća ekvivokacija za dodatno fiksirano $|\tilde{K}_S|$, s obzirom na (5.35) data sa:

$$\tilde{\Delta}_{K_G max} = |\tilde{K}|_{max} - |\tilde{K}_S| - \Psi_L(p_{IRO}^*, \mu_{IR}), \quad p_{IRO}^* \in \tilde{D}. \quad (5.41)$$

Kombinovanjem (5.40) i (5.41), dobijamo alternativni izraz:

$$\tilde{\Delta}_{K_G max} = |\tilde{K}_G| - \Psi_L(p_{IRO}^*, \mu_{IR}), \quad p_{IRO}^* \in \tilde{D}. \quad (5.42)$$

Konačno, iz (3.40) i (3.42) sledi:

$$|\tilde{K}_S|_{max} = \Psi_U(p_{IRO}^*, \mu_{IR}) - \Psi_L(p_{IRO}^*, \mu_{IR}) - \tilde{\Delta}_{K_G max}. \quad (5.43)$$

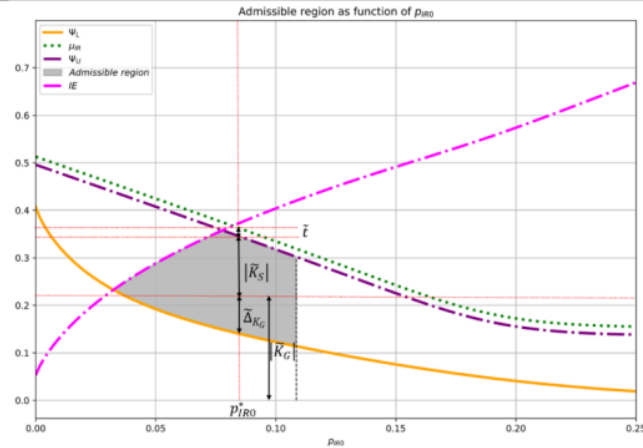
Na Slici 5-1 je ilustracija jednog normalizovanog dopustivog regiona $\tilde{D}$ u funkciji inicijalnog BER p_{IRO} između Alisinog i Bobovog niza na početku IR protokola. Za dato $p_{IRO}^* \in \tilde{D}$ pokazani su $|\tilde{K}_S|$, $\tilde{\Delta}_{K_G}$, $|\tilde{K}_G|$ i $\tilde{\epsilon}$ u slučaju maksimalne moguće brzine destilacije tajnog ključa. Ilustrovani su odnosi i međuzavisnosti veličina $|\tilde{K}|_{max}$, $|\tilde{K}_S|_{max}$, $\tilde{\Delta}_{K_G max}$, $\Psi_L(p_{IRO}^*, \mu_{IR})$ i $\Psi_U(p_{IRO}^*, \mu_{IR})$ za proizvoljno odabrano $p_{IRO}^* \in \tilde{D}$, dati relacijama (3.39) – (3.43). Budući da ima smisla razmatrati samo maksimalne vrednosti za veličine $|\tilde{K}|$, $|\tilde{K}_S|$ i $\tilde{\Delta}_{K_G}$, u daljem tekstu ćemo ih označavati bez posebne naznake da se radi o maksimalnim vrednostima.

Na osnovu (5.43) možemo formulisati sledeću važnu teoremu.

Teorema 3 [5]

Maksimalna brzina destilovanja kriptografskih ključeva $\tilde{K}_S$ za dalju upotrebu dostiže se za p_{IRO} datu sa:

$$p_{IROmax} = \arg \max_{p_{IRO} \in \tilde{D}} \{\Psi_U(p_{IRO}, \mu_{IR}) - \Psi_L(p_{IRO}, \mu_{IR})\}. \quad (5.44)$$



Slika 5-1 Ilustracija jednog normalizovanog dopustivog regiona $\tilde{D}$ u funkciji inicijalnog BER p_{IRO} između Alisinog i Bobovog niza na početku IR protokola. Za dato $p_{IRO}^* \in \tilde{D}$ pokazani su $|\tilde{K}_S|$, $\tilde{\Delta}_{K_G}$, $|\tilde{K}_G|$ i $\tilde{\epsilon}$ u slučaju maksimalne moguće brzine destilacije tajnog ključa

Za autonomiju predloženog sistema od presudne važnosti je da sukcesivno generisani ključevi budu međusobno nezavisni.

Teorema 4 [5]

Neka se u toku autonomnog rada sistema generiše niz destilovanih ključeva $\{K_i\}$, $|K_i| = |K|$, $i = 1, 2, \dots$. Tada važi

$I(K_i; K_{i-1}) \leq \frac{1}{\ln 2} 2^{-t}$	(5.45)
---	--------

$t = n_{IRO} \cdot \mu_{IR} - K $	(5.46)
------------------------------------	--------

gde je n_{IRO} dužina bloka sekvence $\{Y_i\}$ nad kojom se izvršava IR protokol, a μ_{IR} je njegova efikasnost u pogledu preostalih podataka data sa (5.21).

Dokaz

Primenom lančanog pravila (chain rule) za entropiju može se napisati

$\begin{aligned} H(K_{i-1}, X, Y, K_i) &= H(K_{i-1}) + H(X K_{i-1}) + H(Y K_{i-1}, X) + H(K_i K_{i-1}, X, Y) \\ &= H(K_{i-1}) + H(X) + H(K_i Y) \end{aligned}$	(5.47)
--	--------

budući da je $H(X | K_{i-1}) = H(X)$, $H(Y | K_{i-1}, X) = 0$, i $H(K_i | K_{i-1}, X, Y) = H(K_i | Y)$. Ista zajednička entropija može se napisati i na drugi način:

$\begin{aligned} H(K_{i-1}, K_i, X, Y) &= H(K_{i-1}) + H(K_i K_{i-1}) + H(X K_{i-1}, K_i) + H(Y K_{i-1}, K_i, X) = \\ &= H(K_{i-1}) + H(K_i K_{i-1}) + H(X K_i) \end{aligned}$	(5.48)
--	--------

imajući u vidu da je $H(X | K_{i-1}, K_i) = H(X | K_i)$ i $H(Y | K_{i-1}, K_i, X) = 0$.

Izjednačavajući desne strane (3.47) i (3.48) dobijamo:

$H(K_i K_{i-1}) = H(X) + H(K_i Y) - H(X K_i) = H(K_i Y) + I(X; K_i).$	(5.49)
---	--------

Kako je $I(X; K_i) \geq 0$, iz (3.49) sledi:

$H(K_i K_{i-1}) \geq H(K_i Y).$	(5.50)
-------------------------------------	--------

Prema teoremi 3 [25], važi:

$H(K_i W_i) \geq K - \frac{1}{\ln 2} 2^{ K - R(W_i)}$	(5.51)
--	--------

gde je kompresiona funkcija:

$G : W_i \rightarrow \{0,1\}^{ K }$	(5.52)
-------------------------------------	--------

Univerzalna klasa heš funkcija [26], dok je $R(W_i)$ Renijeva entropija drugog reda [36]. Kako slučajne veličine Y , W_i i K_i formiraju Markovljev lanac, t.j. $Y \rightarrow W_i \rightarrow K_i$, važi:

$H(K_i Y) \geq H(K_i W_i) ,$	(5.53)
----------------------------------	--------

pa je na osnovu (5.45) - (5.47):

$H(K_i K_{i-1}) \geq H(K_i Y) \geq H(K_i W_i) \geq K - \frac{1}{\ln 2} 2^{ K - R(W_i)} .$	(5.54)
--	--------

Imajući u vidu da je $W_i \sim B(0.5)$, $H(K_i) = |K|$, $R(W_i) = H(W_i) = n_{IRO} \cdot \mu_{IR}$, konačno dobijamo:

$\begin{aligned} K - H(K_i K_{i-1}) &= H(K_i) - H(K_i K_{i-1}) = \\ &= I(K_i; K_{i-1}) \leq \frac{1}{\ln 2} 2^{-(n_{IRO} \cdot \mu_{IR} - K)} . \end{aligned}$	(5.55)
--	--------

što je i trebalo dokazati.

Primedba 5.3

Na osnovu teoreme 4 zaključujemo da su tajni ključevi generisani sistemom CR KSG maksimalne entropije i međusobno nezavisni. Ovo svojstvo potpuno opravdava izraz (3.19) za inovativnu entropiju, po kome se ona sastoji ne samo od komponente koja potiče od lokalnog generatora čiste slučajnosti već i od dodatne komponente $|K_G|$ nastale destilacijom kriptografskih ključeva u prethodnom ciklusu rada sistema.

Konkretan izgled dopustive oblasti zavisi od izbora IR protokola. U narednom poglavlju će biti detaljno analizirana dopustiva oblast $\tilde{D}$ za slučaj kada je IR zasnovan na Winnow protokolu [32].

6. OPTIMALNI SKD SISTEM ZASNOVAN NA CR KSG I WINNOW IR PROTOKOLU

Shodno teoremi 1, presudnu uticaj na izgled dopustive oblasti ima struktura pariti bita koju Alisa šalje Bobu po javnom kanalu, odnosno struktura celokupnog skupa maski $\{m_i\} = \{\{m_{i1}, m_{i2}, \dots, m_{in_i}\}\}$, $i = 1, 2, \dots, n_p$, $m_{ij} \in \{0, 1\}$. Sa $CR KSG_W$ označićemo CR KSG sistem u kome je za IR fazu SKD protokola uzet Winnow protokol. Izbor ovog IR protokola zasniva se na njegovoj efikasnosti u slučaju male početne greške p_{IRO} između Alisinog i Bobovog niza. Podsetimo se da je u CR KSG sistemu p_{IRO} , odnosno shodno parametar ε , stvar izbora dizajnera sistema.

Stoga ovaj protokol može efikasno i brzo ispravljati greške uz minimalnu komunikaciju i istovremeno sprečavanje oticanja informacija ka Evi (privacy maintenance), [33], [34], [35]. Winnow protokol započinje podelom početnih sekvenci na blokove podataka dužine N. Pitanje ove dužine je proteklih 20 tak godina bio predmet intenzivne analize, dominantno u okviru kvantne distribucije ključa (QKD) algoritama. U [33] je pokazano da je Winnow protokol sa manjim dužinama N, posebno za N=8, efikasniji u ispravljanju grešaka od većih dužina N. Stoga ćemo u daljem izlaganju usvojiti ovu vrednost kao fiksni parametar $CR KSG_W$ sistema.

Detaljan opis koraka Winnow protokola je sledeći:

1. Permutacija i podela nizova:

Alisa i Bob najpre permutuju svoje početne nizove bita na osnovu unapred dogovorenog pravila. Zatim te permutovane nizove dele na blokove dužine $N = 2^r$ gde je $r \geq 3$.

2. Izračunavanje pariteta blokova:

Obe strane (Alisa i Bob) izračunavaju paritet svakog bloka od N bita, tj. da li je broj jedinica u bloku paran ili neparan.

3. Upoređivanje pariteta i korekcija grešaka:

Ako se pariteti poklapaju, pretpostavlja se da u bloku nema grešaka. Međutim, prvi bit iz tog bloka se ipak odbacuje iz razloga očuvanja privatnosti.

Ako su pariteti različiti, to ukazuje na neparan broj grešaka u bloku. I tada se prvi bit odbacuje, a na preostalih $N-1$ bita primenjuje se Hamingov algoritam za ispravljanje grešaka.

4. Iteracije:

Koraci 1–3 se ponavljaju više puta (onoliko koliko je definisano unapred), kako bi se postigla bolja usklađenost nizova.

Hamingova korekcija grešaka se obavlja na sledeći način:

a. Računanje sindroma:

Neka su I_a i I_b nizovi od $N-1$ bita koje poseduju Alisa i Bob, respektivno. Svako od njih izračunava svoj sindrom (kontrolni kod), korišćenjem Hamingove kontrolne matrice H :

$$S_a = I_a H^T, \quad S_b = I_b H^T$$

b. Otkrivanje i ispravljanje grešaka:

Alisa šalje svoj sindrom S_a Bobu preko javnog kanala. Bob zatim računa razliku sindroma:

$$S_d = S_a \oplus S_b$$

Ako je $S_d \neq 0$, to znači da je došlo do greške, pa Bob koristi dobijeni sindrom za ispravku svoje verzije bloka.

c. Očuvanje privatnosti:

Da bi se sprečilo curenje informacija ka Evi (koja prisluškuje javni kanal), poslednjih r bita svakog bloka se uklanja nakon korekcije. Time se neutralizuje eventualni uticaj javno prenetog sindroma na bezbednost.

Naredna teorema daje eksplicitne izraze za gornja i donja granica dopustive oblasti CR_{KSG_w} , čime se otvara mogućnost optimalne sinteze odgovarajućeg SKD sistema.

Teorema 5 [5]

Gornja i donja granica oblasti $\tilde{D}^W$ koja se odnosi na CR KSG sa Winnow IR protokolom je data sa gornjom:

$\Psi_U^{Win}(p_{IRO}, \mu_{IR}^{Win}) = \min \left\{ h_b \left(\frac{1}{2} (1 - \sqrt{1 - 2 p_{IRO}}) \right), \mu_{IR}^{Win}(p_{IRO}) - \tilde{\epsilon} \right\},$	(6.1)
--	-------

i donjom granicom:

$\begin{aligned} \Psi_L^{Win}(p_{IRO}, \mu_{IR}^{Win}) \\ = 1 - \mu_{IR}^{Win}(p_{IRO}) \\ - \frac{1}{n_{IRO}} \left[2 n_b h_b \left(\frac{1}{2} (1 - (1 - 2 p_{IRO})^4) \right) + n_H h_b \left(\frac{1}{2} (1 - (1 - 2 p_{IRO})^2) \right) \right] \end{aligned}$	(6.2)
--	-------

gde μ_{IR}^{Win} je efikasnost preostalih podataka kod Winnow protokola, a p_{IRO} početni BER između Alisinog i Bobovog niza. Sa n_b je označen broj Alisinih poslatih parnosti blokova dužine $N=8$, a sa n_H broj njenih poslatih sindroma Hamingovog koda za korekciju grešaka (7.4).

Dokaz

U toku izvršavanja Winnow protokola po javnom kanalu se šalju dve klase pariti bita:

$S_b = [Y_1, Y_2, \dots, Y_8] \cdot [1, 1, \dots, 1]^T$	(6.3)
---	-------

$S_H = \begin{bmatrix} S_{H1} \\ S_{H2} \\ S_{H3} \end{bmatrix} = H_3 \cdot [Y_2, Y_3, \dots, Y_8]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot [Y_2, Y_3, \dots, Y_8]^T$	(6.4)
--	-------

Klasa S_b se računa za svaki blok i razmenjuje sa drugom stranom. U terminima teoreme 1, sve maske koje se odnose na ovu klasu su konstantne dužine 8 sa 8 jedinica, odnosno:

$m_b = [m_{b1}, m_{b2}, \dots, m_{b8}] = [1, 1, \dots, 1], \sum_{j=1}^8 m_{bj} = 8.$	(6.5)
--	-------

Klasa S_H se računa za svaki blok za koji je Alisin i Bobov pariti S_b različit. Matrica H_3 je matrica Hamingovog (7,4) korekcionog koda, tako da je S_H trobitni sindrom ovog koda [38]. Uvidom u strukturu matrice H_3 zaključujemo da u svakom redu imamo tačno 4 jedinice, što znači da za maske iz ove klase važi:

$$m_{Hi} = [m_{Hi1}, m_{Hi2}, \dots, m_{Hi7}], \quad \sum_{j=1}^7 m_{Hij} = 4, \quad i = 1, 2, 3. \quad (6.6)$$

Stoga se suma u izrazu za donju granicu (5.30) u teoremi 2 može razbiti na dva sabirka, jedan koji se odnosi na pariti bite iz klase S_b i drugi koji se odnosi na pariti bite iz klase S_H . Na osnovu (4.5), važi $\frac{1}{2} \sum_{j=1}^{N_i} m_{ij} = 8$, i $\frac{1}{2} \sum_{j=1}^{N_i} m_{ij} = 4$ za klasu S_b , odnosno S_H respektivno. Budući da je $N_i = 8$, za $\forall i$, konačno dobijamo:

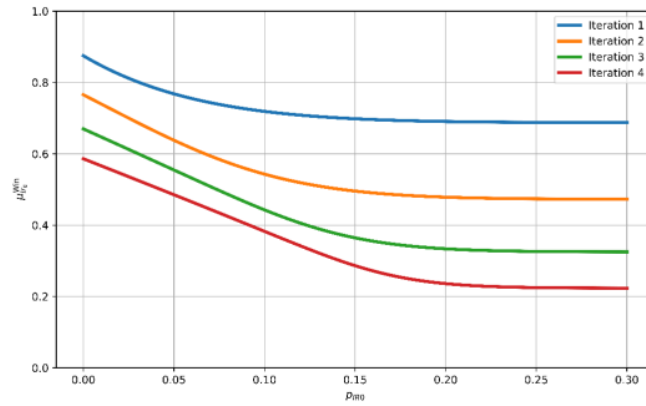
$$\sum_{i=1}^{n_p} h_b \left(\frac{1}{2} \left(1 - (1 - 2 p_{IRO})^{\frac{1}{2} \sum_{j=1}^{N_i} m_{ij}} \right) \right) = \quad (6.7)$$

$$2 n_b h_b \left(\frac{1}{2} (1 - (1 - 2 p_{IRO})^4) \right) + n_H h_b \left(\frac{1}{2} (1 - (1 - 2 p_{IRO})^2) \right)$$

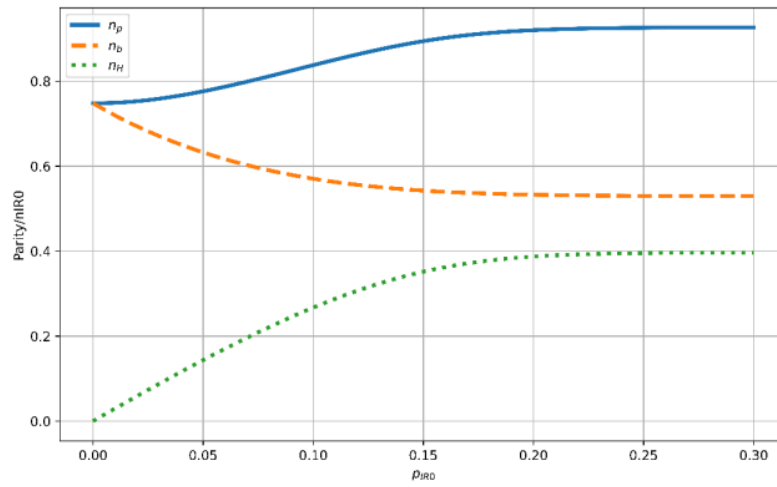
Pri čemu faktor 2 za prvi sabirak potiče iz činjenice da pored Alice i Bob šalje svoje pariti bite iz klase S_b . Zamenom (6.7) u (5.30), dobijamo tvrdnju (6.2) za donju granicu. Gornja granica (6.1) direktno sledi iz (5.29) uz zamenu izraza za opštu efikasnost $\mu_{IR}(p_{IRO})$ sa $\mu_{IR}^{Win}(p_{IRO})$, koja se odnosi na Winnow protokol. Ovim je dokaz teoreme završen.

U radu [19] prezentovan je kompletan algoritam za izračunavanje $\mu_{IR}^{Win}(p_{IRO})$, n_b , n_H , n_p i p_{IR_end} , gde je sa p_{IR_end} označen BER između Alisinog i Bobovog niza na kraju protokola. ⁸ Slika 6-1, Slika 6-2 i Slika 6-3 prikazuju promene ovih veličina u funkciji p_{IRO} , pri čemu je izvršena normalizacija broja pariti bita u odnosu na početnu dužinu n_{IRO} :

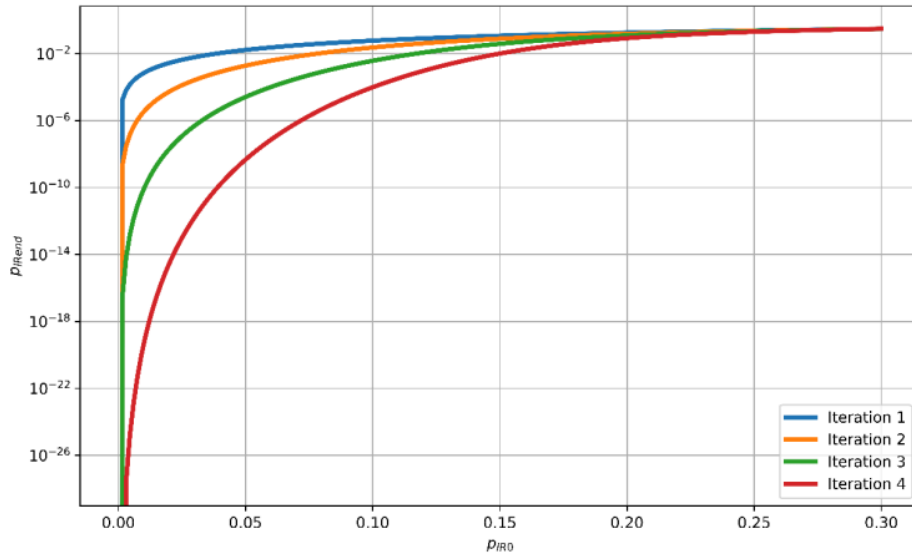
$$\tilde{n}_p = \frac{n_p}{n_{IRO}}, \quad \tilde{n}_b = \frac{n_b}{n_{IRO}}, \quad \tilde{n}_H = \frac{n_H}{n_{IRO}}. \quad (6.8)$$



Slika 6-1 Promena $\mu_{IR}^{Win}(p_{IR0})$ kroz 4 iteracije Winnow protokola



Slika 6-2 Promena normalizovanih vrednosti $\tilde{n}_p = \frac{n_p}{n_{IR0}}$, $\tilde{n}_b = \frac{n_b}{n_{IR0}}$ i $\tilde{n}_H = \frac{n_H}{n_{IR0}}$, u funkciji p_{IR0} nakon 4. iteracije Winnow protokola.



Slika 6-3 Promena konačnog BER p_{IR_end} između Alisinog i Bobovog niza na kraju prve 4 iteracije Winnow protokola.

Primedba 6.1

Winnow protokol iterativno primenjuje osnovne operacije podele nizova na blokove, razmene pariti bita blokova, računanja i slanja sindroma Hemmingovog koda (7,4), korekcije grešaka i odbacivanja odgovarajućeg broja bita u cilju održavanja nivoa privatnosti. Sa povećanjem broja iteracija, kao što vidimo sa slike 6.1 opada $\mu_{IR}^{Win}(p_{IRO})$ za svako p_{IRO} , a samim tim se smanjuje brzina destilacije ključa $CR KSG_W$ sistema. S druge strane, saglasno slici 4.3 manji broj iteracija povećava p_{IR_end} za svako p_{IRO} , efektivno smanjujući brzinu destilacije. Stoga je izbor broja iteracija kompromis između ove dve suprotnosti, koji se po pravilu bira u procesu eksperimentalne evaluacije sistema. Naš izbor od $max_iter=4$ iteracije, praktično je potvrđen kao najbolji mogući izbor.

Slika 4-4 b), prikazuje dopustivu oblast za $CR KSG_W$ sistem, sa parametrima Winnowog protokola $N=8$ i $max_iter=4$ i gornjom granicom KDR $\delta \leq 10^{-4}$.

Slika 6-4 a) prikazuje odnos između parametra $p_{IRfinal} = \delta = 10^{-4}$ i $p_{IRO}(\delta) = 0.0995$, čime je određena gornja granica dopustive oblasti $\tilde{D}^W$ po koordinati p_{IRO} , imajući u vidu relaciju (6.7), odgovarajući parametar $\varepsilon(\delta) = 0.0525$.

Na osnovu teoreme 3, sledi da se maksimalno $|\tilde{K}_S|_{max}$ bez obzira na izbor $\tilde{\Delta}_{K_Gmax}$ postiže nalaženjem maksimuma funkcije:

$f(p_{IRO}) = \Psi_U(p_{IRO}, \mu_{IR}) - \Psi_L(p_{IRO}, \mu_{IR}), \quad p_{IRO} \in \tilde{D}^W,$	(6.9)
--	-------

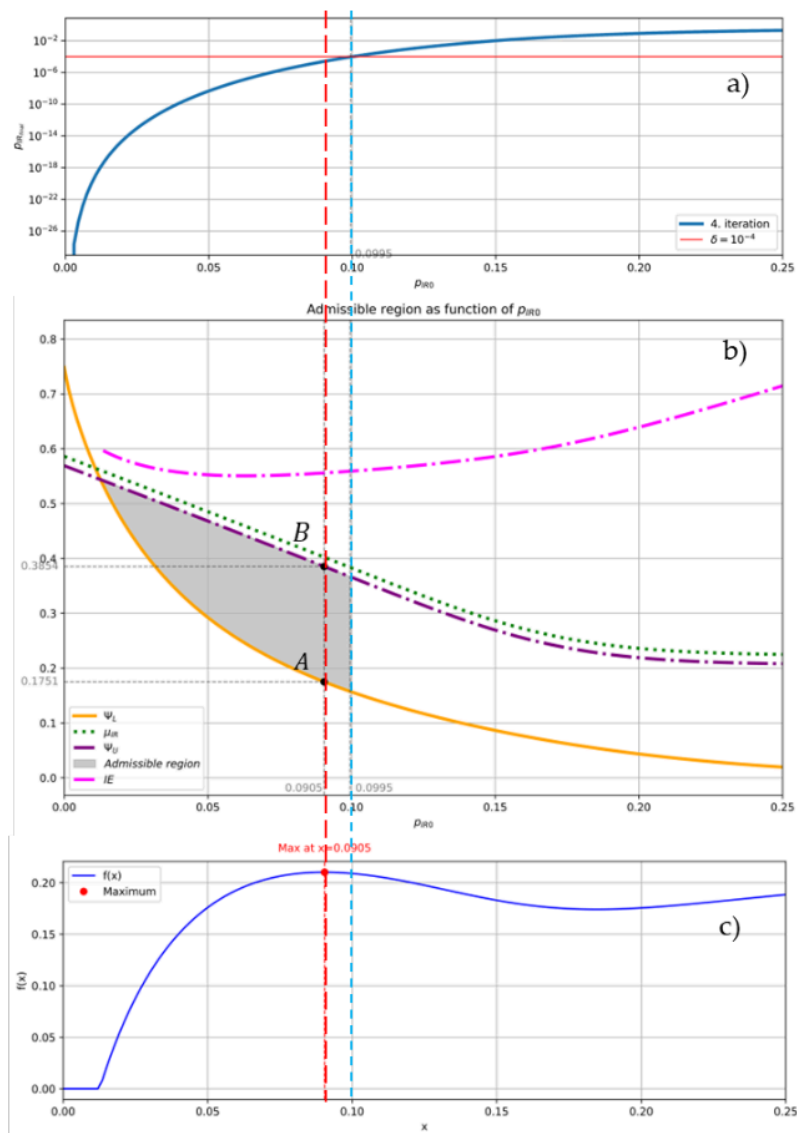
Usled vrlo kompleksnog analitičkog izraza za $\Psi_U(p_{IRO}, \mu_{IR})$ i $\Psi_L(p_{IRO}, \mu_{IR})$ ovaj maksimum se može dobiti numerički. Slika c) prikazuje funkcija $f(p_{IRO})$ i njen maksimum $f(p_{IRO_max})$ koji se postiže za $p_{IRO_max} = 0.0905$, odnosno korespondentno $\varepsilon_{max} = 0.0525$. Slika 6-4 .b) prikazuje tačke A i B na Ψ_L i Ψ_U za vrednost p_{IRO_max} . Koordinate ovih tačaka su:

$A(0.0905, C_1), \quad B(0.0905, C_2 - \tilde{\varepsilon}),$	(6.10)
---	--------

gde su C_1, C_2 :

$C_1 = \Psi_L(p_{IRO_max}, \mu_{IR}) = 0.1751, \quad C_2 = \mu_{IR}(p_{IRO_max}) = 0.4023.$	(6.11)
---	--------

Vrednost $p_{IRfinal}(0.0905) = 2.5822 \cdot 10^{-5}$, što ukazuje na ekstremno nisku verovatnoću za KDR.



Slika 6-4 Odnos između parametra $p_{IRfinal} = \delta = 10^{-4}$ i $p_{IR0}(\delta) = 0.0995$. b) Dopustiva oblast za $CR KSG_W$ sistem, sa parametrima Winnowog protokola $N=8$, $max iter = 4$ i gornjom granicom KDR $\delta \leq 10^{-4}$. c) Funkcija $f(p_{IR0})$ i njen maksimum $f(p_{IR0_max})$, koji se postiže za $p_{IR0_max} = 0.0905$, odnosno korespondentno $\varepsilon_{max} = 0.0525$.

Primedba 6.2

Na osnovu (5.42) i definicije normiranih vrednosti (5.32), dobijamo:

$ \tilde{K}_s = C_2 - \frac{t}{n_{IR0}} - \frac{C_1}{1-r},$	(6.12)
--	--------

a na osnovu (3.40), i (3.32):

$n_{IR0} = \frac{K_G - \Delta K_G}{C_1} = K_G \frac{1-r}{C_1},$	(6.13)
---	--------

$r = \frac{\Delta K_G}{K_G} = \frac{\tilde{\Delta K_G}}{\tilde{K}_G}, \tilde{\Delta K_G} < C_2 - C_1,$	(6.14)
--	--------

gde su konstante C_1 i C_2 date u (6.11). Asimptotski efektivni kapacitet tajnosti za dovoljno velike početne vrednosti n_{IR0} i dovoljno male vrednosti parametra r , iz izraza (6.12) sledi da je granična (asimptotska) vrednost maksimalnog efektivnog kapaciteta tajnosti jednaka:

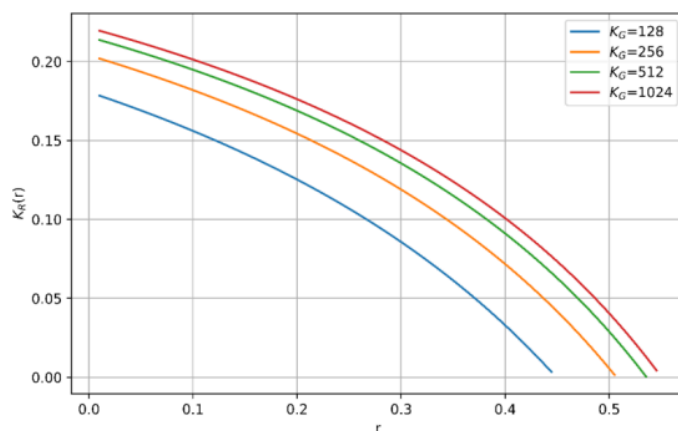
$$|\tilde{K}_s|_{max} = C_2 - C_1 = 0,2272$$

odnosno 22,72%. To znači da se, pod ovim uslovima, može efikasno izdvojiti tajni ključ koji čini približno 22,72% ukupno dostupne informacije u sistemu.

Efektivni kapacitet tajnosti (6.12) se može izraziti i preko K_G , zamenom (6.13) u (6.12), čime se dobija:

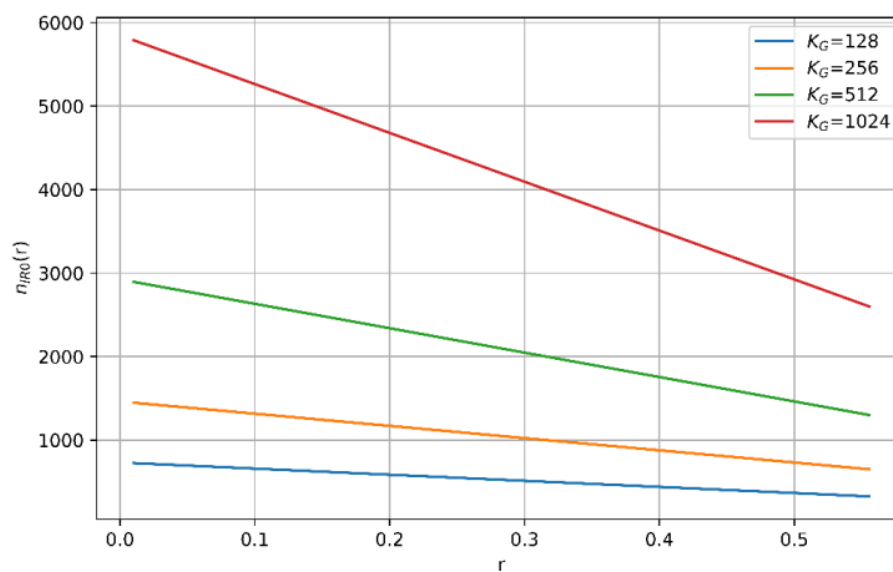
$ \tilde{K}_s = C_2 - \frac{C_1}{1-r} \left(1 + \frac{t}{K_G} \right).$	(6.15)
---	--------

Postupak sinteze optimalnog $CR KSG_W$ sistema započinje izborom parametra r , i K_G koji prema (6.15) jednoznačno određuje kapacitet tajnosti $|\tilde{K}_s|$, (Slika 6-5).



Slika 6-5 Zavisnost efektivnog kapaciteta tajnosti $|\tilde{K}_s|$ od parametra r datog sa (4.14), za različite vrednosti K_G . Za parametar kompresije t je uzeta vrednost $t = 34$.

Izbor dužine tajnog ključa K_G može biti izvršen na osnovu različitih praktičnih okolnosti. Npr. ukoliko se raspolaze nekim standardnim KSG, koji po pravilu ima predefinisane dužine za K_G , [6], tada se bira jedna od ponuđenih opcija.



Slika 6-6 Zavisnost osnovne dužine bloka podataka n_{IR0} od parametra r za različite vrednosti K_G .

Ova vrednost jednoznačno određuje dužinu osnovnog bloka podataka n_{IRO} , shodno (6.13). Na Slika 6-6 prikazane su zavisnosti $n_{IRO}(r)$, za različite tipične vrednosti $|K_G|$.

Primer 4.1

Ako smo izabrali $r = 0.3$ i $|K_G| = 512$ b rezultujuća efektivna brzina tajnosti $|\tilde{K}_s| = 0.1355$ a postiže se izborom dužine osnovnog bloka $n_{IRO} = 2047$ b. Pri tome je vrednost donje granice ekvivokacije $\Delta_{K_G} = r K_G = 0.3 \cdot 512 = 154$ b. Stepen kompresije t je kao i do sada, fiksiran na vrednost $t = 34$, što obezbeđuje nivo oticanja informacija rate manji od 10^{-10} . U Tabela 6-1 dat je pregled vrednosti za $|\tilde{K}_s|_{max}$ i n_{IRO} za tipične vrednosti $|K_G|$, zadržavajući donju granicu ekvivokacije Δ_{K_G} na konstantnoj vrednosti 128 b.

Tabela 6-1 Maksimalna efektivna brzina generisanja kriptografskih ključeva $|\tilde{K}_s|_{max}$ i odgovarajuća dužina bloka n_{IRO} , za tipične vrednosti dužine ključa $|K_G|$ i stepen kompresije $t = 34$.

$ K_G $	r	Δ_{K_G}	$ \tilde{K}_s _{max}$	n_{IRO}
256	0.500	128	0.0056	732
512	0.250	128	0.1533	2194
1024	0.125	128	0.1955	5118
4096	0.031	128	0.2005	20469

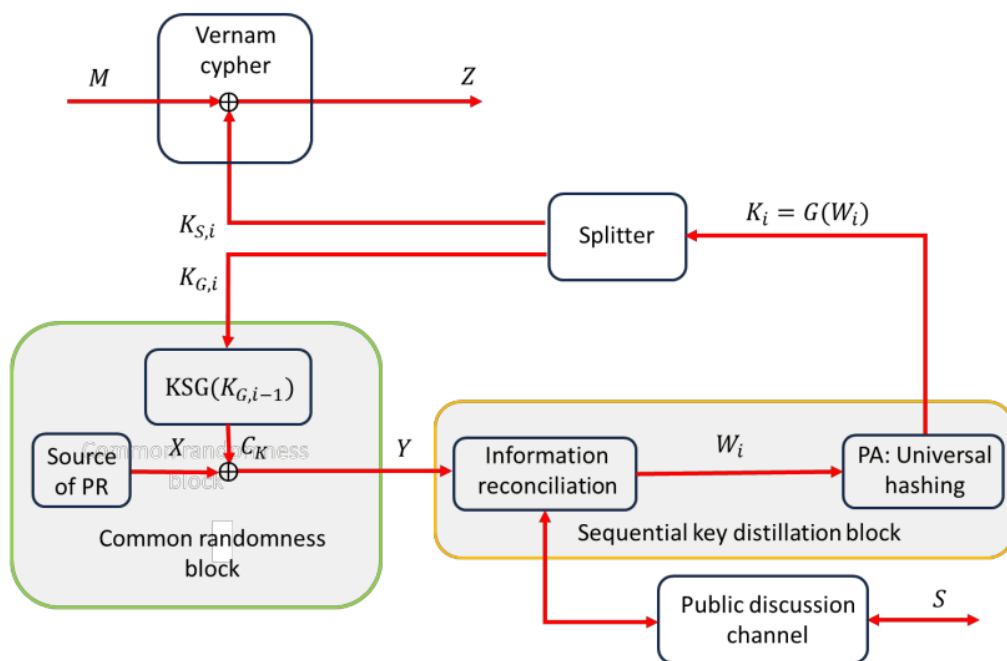
6.1 Od idealne do perfektne bezbednosti korišćenjem SKD zasnovanog na CR KSG i Winnow IR protokola

Bezbednost predloženog SKD-a zasnovanog na CR KSG-u zasniva se na idealnosti KSG-a u Šenonovom smislu [1]. U Šenonovoj definiciji idealnog sistema, važno je da se ekvivokacija ključa ne svodi na nulu sa neograničenim povećanjem dostupnog šifrovanog teksta [1]. U [37] je uvedeno proširenje osnovnog Šenonovog koncepta na pojam tzv. Autonomna i robusna šema šifrovanja sa idealnom tajnošću (Ideally Secret Autonomous Robust Cipherring-ISAR) sistem. Prema Definiciji 3, u [37], ISAR sistem za šifrovanje je onaj koji može da održi minimalnu ekvivokaciju ključa na unapred definisanoj vrednosti D_K , nezavisno od raspodele verovatnoće poruke i bez dodatnog sistema distribucije tajnog ključa [5] .

Primedba 6.3

Shodno teoremi 1, zajednička slučajnost blokova predloženog SKD-a zasnovanog na CR KSG-u je ISAR sistem šifrovanja u kome je šifrat skup svih pariti bita poslatih po javnom kanalu.

Stoga se napad na sistem usmeren ka rekonstrukciji ključa K_G suočava sa neodređenošću reda $2^{\Delta K_G}$. Drugim rečima, kriptanalitičar ima na raspolaganju $2^{\Delta K_G}$ jednako verovatnih hipoteza za ključ K_G .



Slika 6-7 Sistem perfektne bezbednosti zasnovan na destilaciji tajnog ključa (SKD) korišćenjem izvora zajedničke slučajnosti realizovanog putem determinističkog generatora (KSG) i IR protokola tipa Winnow

Slika 6-7 prikazuje proširenje osnovnog SKD CR sistema, slika 4-1, na sistem čija je krajnja namena generisanje kriptografskih ključeva za Vernamovu šifru, kojom se šifruje neki nezavisni izvor poruka M . Intrigantno je pitanje da li i pod kojim uslovima ovaj sistem može biti perfektno tajn. Da bi smo odgovorili na ovo pitanje, neophodno je da dokažemo sledeću teoremu [5] .

Teorema 6

Za CR SKD sistem važi:

$H(W_i S) = H(W_i),$	(6.16)
$R(W_i S = s) = W_i .$	(6.17)

Dokaz

Informacije sa javnog kanala $S = \{S_i\}$ dostupne Evi su uvek pariti biti oblika:

$$S_i = \sum_{j=1}^N Y_j \cdot m_{ij}, \quad m_{ij} \in \{0,1\} \quad (6.18)$$

gde su $m_{ij} \in \{0,1\}$ biti vektora maske pridruženog S_i , kao što je ukazano u teoremi 1, formule (6.1)-(6.2). Nakon slanja bita S_i , Alisa odbacuje jedan bit sa poznate pozicije j^* u tekućem bloku dužine N , usled čega se jednačina (6.16) transformiše u jednačinu

$$\bar{S}_i = \sum_{j=1, j \neq j^*}^N Y_j \cdot m_{ij} \quad (6.19)$$

Jednačina (5.4) se može napisati i u sledećoj ekvivalentnoj formi:

$$\bar{S}_i = S_i \oplus Y_{j^*} \quad (6.20)$$

Kako je $P(Y_{j^*} = 1) = P(Y_{j^*} = 0) = 0.5$, poznavanje pariti bita S_i ne daje nikakvu informaciju o paritiju $\bar{S}_i$ preostalih bita. Nakon završetka IR protokola, niz W_i je sačinjen samo od bita preostalih nakon isključivanja bita sa pozicija j^* . O njihovim vrednostima Eva ne zna ništa dodatno iako su joj dostupni svi paritiji $S = \{S_i\}$ sa javnog kanala, odnosno $H(W_i|S) = H(W_i)$, što je upravo prva tvrdnja ove teoreme.

Za dokaz tvrdnje (6.16), podsetimo se da za uslovnu Renijevu entropiju drugog reda i odgovarajuću Šenonovu entropije važi nejednakost:

$$H(W_i|S = s) \geq R(W_i|S = s), \quad (6.21)$$

pri čemu se jednakost dostiže samo u slučaju kada je $H(W_i) = |W_i|$, odnosno kada je niz W_i maksimalne entropije. Imajući u vidu da je svaki bit u nizu W_i oblika $W = X \oplus C_K$, $C_K \sim B(0.5)$, zaključujemo da je $H(W_i) = |W_i|$, odnosno da na osnovu (5.6) važi:

$$R(W_i|S = s) = H(W_i|S = s) = H(W_i) = |W_i|, \quad (6.22)$$

čime je dokaz teoreme završen. ■

Primedba 6.4

Na osnovu posledice 5 teoreme 4 i teoreme 6, sledi:

$I(K_s; G, S) \leq \frac{1}{\ln 2} 2^{-t}$	(6.23)
--	--------

gde je t stepen kompresije primenjene univerzalne heš funkcije G . Drugim rečima Evina informacija o K_s na osnovu G i S se može učiniti proizvoljno malom.

Teorema 7 [5]

Sistem sa slike 4.1 je perfektno tajan, ako je:

$ \tilde{K}_s = \tilde{\Delta}_{K_G},$	(6.24)
---	--------

sa greškom manjom od $\frac{1}{\ln 2} 2^{-t}$, gde je t stepen kompresije primenjene univerzalne heš funkcije G .

Maksimalna efektivna brzina tajnosti, $|\tilde{K}_s|$ data je sa:

$ \tilde{K}_s _{max} = \frac{1}{2} \left(\Psi_U(p_{IRO_max}, \mu_{IR}) - \Psi_L(p_{IRO_max}, \mu_{IR}) \right), \quad p_{IRO_max} = 0.0905.$	(6.25)
--	--------

Dokaz

Za perfektну tajnost je potreban i dovoljan uslov da opservacije prisluškivača ne menjaju njegovu neodređenost u pogledu primenjenih kriptografskih ključeva , odnosno da važi:

$H(K_s Z, S) = H(K_s) = K_s .$	(6.26)
---------------------------------	--------

Primetimo da uslov perfektne tajnosti (6.26) obuhvata potpun skup $\{Z, S\}$ opservacija dostupnih napadaču, dakle ne samo šifrat Z , već i sve informacije $\{S\}$ sa javnog kanala u toku realizacije pratećeg SKD protokola.

Veza između M, Z i K_s data je Vernamovom šifrom:

$Z = M \oplus K_s$	(6.27)
--------------------	--------

gde je $K_s \sim B(0.5)$ i nezavisno od M . Odavde sledi da je Z nezavisno od K_s , odnosno:

$H(K_s Z, S) = H(K_s S).$	(6.28)
---------------------------	--------

Na osnovu (5.8) iz (5.12) važi:

$H(K_s Z, S) = H(K_s S) \geq K_s - \frac{1}{\ln 2} 2^{-t}$	(6.29)
--	--------

što znači da je Evina entropija o tajnom ključu K_s blizu maksimalne, ili drugim rečima:

$H(K_s Z, S) = H(K_s S) = H(K_s)$	(6.30)
-----------------------------------	--------

sa tačnošću od $\frac{1}{\ln 2} 2^{-t}$. Ovim je dokazano da važi uslov perfektne tajnosti (5.10) u odnosu na tajni ključ K_s .

S druge strane, budući da je CR blok ISAR šifarski sistem, važi:

$H(K_G Z, S) = H(K_G S) \geq \Delta_{K_G}.$	(6.31)
---	--------

Iz (6.30) i (6.31) sledi da u slučaju kada važi:

$ K_s = \Delta_{K_G},$	(6.32)
-------------------------	--------

Napadač na sistem nema nikakav dobitak u rekonstrukciji K_G , u odnosu na rekonstrukciju K_s , jer se, zbog (6.31) i (6.32), susreće sa skupom iste kardinalnosti $2^{|K_s|}$ jednako verovatnih alternativa, odnosno da istovremeno važi

$H(K_G Z, S) = H(K_s), H(K_s Z, S) = H(K_s)$	(6.33)
--	--------

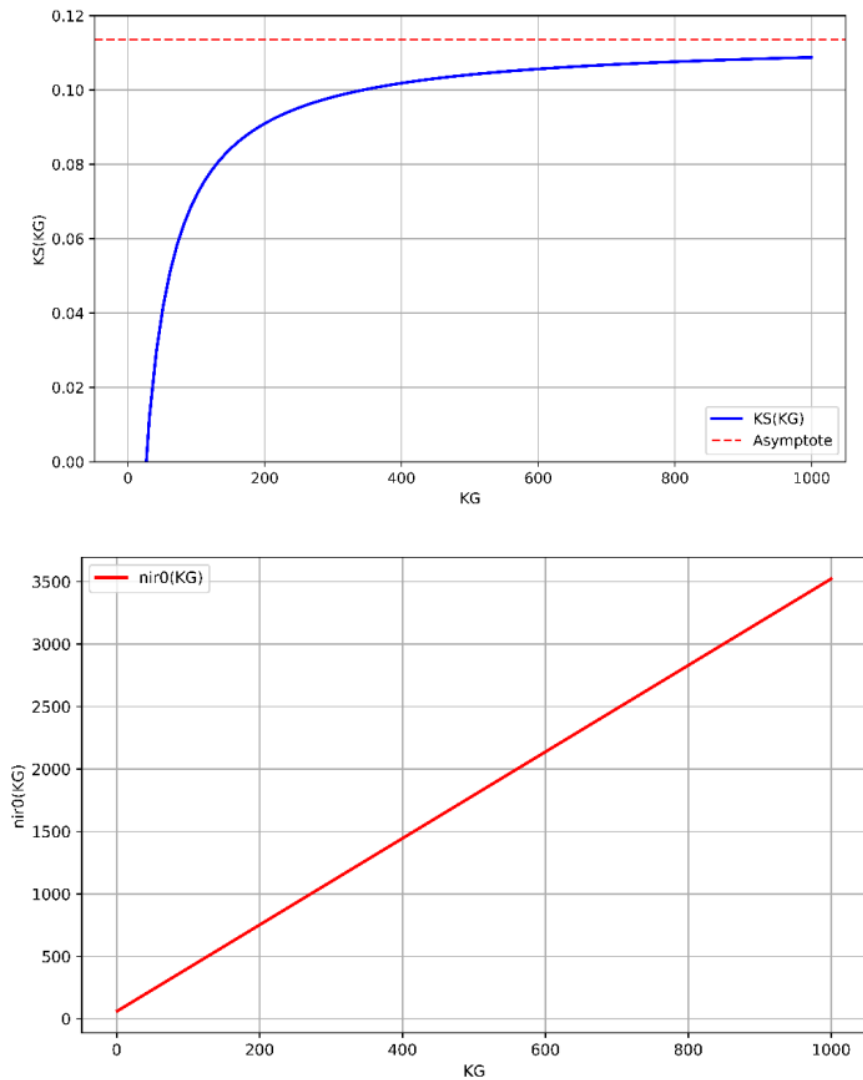
sa tačnošću od $\frac{1}{\ln 2} 2^{-t}$. Ovim je dokaz teoreme završen. ■

Primedba 6.5

Polazeći od (4.12) i (4.13), možemo doći do izraza koji povezuju $|\tilde{K}_s|_{max}$ i dužinu osnovnog bloka n_{IR0} sa $|K_G|$ i stepenom kompresije t

$ \tilde{K}_s _{max} = \frac{1}{2} \left(c_2 - c_1 - t \cdot \frac{c_2 + c_1}{2 K_G + t} \right)$	(6.34)
$n_{IR0} = \frac{2 K_G + t}{c_2 + c_1}$	(6.35)

gde su konstante c_1 i c_2 date sa (4.11), videti Slika 6-8.



Slika 6-8 Zavisnost maksimalnog efektivnog kapaciteta tajnosti $|\tilde{K}_s|_{max}$ od dužine tajnog ključa $|K_G|$ (gornja slika). Na istoj slici prikazana je njena asimptotska vrednost

$0.5 \cdot (C2 - C1) = 0.5 \cdot 0.1136$. Zavisnost neophodne dužine osnovnog bloka podataka n_{IRO} od iste veličine (donja slika). Stepen kompresije heš funkcije G je standardno $t = 34$.

6.2 Postupak sinteze

Postupak sinteze je jednostavan i sastoji se prvo u izboru $|K_G|$ i t , koji zatim jednoznačno određuju n_{IRO} . Primetimo sa slike.6.2, da već nakon $|K_G| > 400$ b ulazimo u predeo zasićenja, gde se $|\tilde{K}_s|_{max}$ ne povećava za više od 10 %. Tabela 6-2 Maksimalna brzina generisanja kriptografskih ključeva $|\tilde{K}_s|_{max}$ i odgovarajuća dužina bloka n_{IRO} , za tipične vrednosti dužine ključa $|K_G|$ i stepen kompresije $t=34$ dat je pregled ovih veličina za standardne vrednosti $|K_G|$ [5] .

Tabela 6-2 Maksimalna efektivna brzina generisanja kriptografskih ključeva $|\tilde{K}_s|_{max}$ i odgovarajuća dužina bloka n_{IRO} , za tipične vrednosti dužine ključa $|K_G|$ i stepen kompresije $t = 34$.

$ K_G $	$ \tilde{K}_s _{max}$	n_{IRO}
128	0.0797	502
256	0.0956	946
512	0.1043	1833
1024	0.1088	3606
4096	0.1124	14244

Izbor operativnog režima sistema u osnovi zavisi od karakteristika operativnog okruženja i prioriteta koji se dodeljuju bezbednosnim zahtevima. Kada se proceni da potencijalni napadač ne raspolaže računski moćnim sredstvima koja bi omogućila efektivnu analizu svih mogućih hipoteza o primenjenom tajnom ključu u okviru vremenskog okvira u kojem informacije zadržavaju svoju vrednost, tada se idealni režim bezbednosti nameće kao racionalan izbor. U ovom kontekstu, prihvatljiv vremenski okvir za analizu definiše se kao period tokom kojeg zaštićene informacije ostaju relevantne za protivnika, npr. u realnim sistemima, to je često ograničeno trajanjem operacije ili važnosti podataka (npr. vojna, finansijska, politička informacija).

Nasuprot tome, u slučajevima kada je zahtevana jača forma bezbednosti, kao što je prospektivna otpornost (forward secrecy) i otpornost na kvantne napade, odnosno situacije u kojima se želi osigurati da dešifrovanje ostane nemoguće čak i ukoliko protivnik raspolaže neograničenim računskim resursima, uključujući kvantne kompjutere, tada je režim perfektne tajnosti jedina adekvatna opcija. Međutim, ovaj režim nosi sa sobom određene kompromise, pre svega u vidu smanjene brzine destilacije tajnog ključa, što može uticati na ukupnu efikasnost sistema, naročito u aplikacijama sa ograničenim resursima ili zahtevima za visokom propusnošću.

U okviru Primera 6.1, predstavljene su praktične situacije u kojima se različiti režimi operativnog rada pokazuju kao optimalni izbor, u zavisnosti od konteksta primene i ciljanog nivoa bezbednosti.

Primer 6.1

Izborom optimalnog $\varepsilon_{max} = 0.0525$, $t = 34$, $|K_G| = 512$, $n_{IRO} = 1833$, sintetisali smo perfektno tajan autonoman šifarski sistem, koji može da štiti informacioni izvor brzine do $|\tilde{K}_s|_{max} = 0.1043$, čiji je $KDR < 2.5822 \cdot 10^{-5}$, i brzine curenja ključa $I(K_s, K_G; Z, S) < 10^{-10}$.

Radi jasnoće, u nastavku sumiramo ključne pretpostavke koje su uzete u obzir pri projektovanju autonomnog sistema sa perfektnom tajnošću. Pored osnovnih pretpostavki koje su već izložene za sistem sa Slike 6.1 (videti Pod poglavlje 23.1), dodatno se podrazumevaju sledeće:

1. Statistička nezavisnost poruke i ključa: Tajni ključ koji je izlaz SKD (sistema za destilaciju tajnog ključa), koristi se za šifrovanje nezavisnog izvora poruka M pomoću Vernamove šifre. Ovo zahteva da između ključa i poruke postoji statistička nezavisnost, kako bi se sačuvala sigurnost na nivou jednokratne upotrebe (one-time pad).
2. Uniformna raspodela i dužina ključa u skladu sa marginom tajnosti: Pretpostavlja se da je destilovani ključ uniformno raspodeljen, što osigurava maksimalnu entropiju. Takođe, dužina ključa je dimenzionirana tako da odgovara marginu tajnosti, čime se obezbeđuje efektivna tajnost prilikom šifrovanja.
3. Informaciona rekonsilijacija pomoću Winnow protokola sa probijanjem (puncturing):
U sistemu se koristi Winnow protokol za informacionu rekonsilijaciju uz primenu probijanja, čime se obezbeđuje da otkrivanje paritetnih bita putem javnog kanala S smanjuje entropiju usaglašene sekvence.
4. Postizanje perfektne tajnosti uz zanemarljivu grešku: Sistem koristi dovoljno velike blokove i odgovarajuću stopu kompresije, kako bi ušao u regiju perfektne tajnosti sa zanemarljivom verovatnoćom greške.
5. Očuvanje margine tajnosti pri neograničenoj izloženosti šifrovanom tekstu: CR SKD blok (destilacija zajedničke slučajnosti) se tretira kao ISAR kriptosistem, što podrazumeva da sistem zadržava marginu tajnosti čak i ako napadač ima neograničen pristup šifrovanim porukama.
6. Integritet autentifikovanog javnog kanala. U skladu sa pretpostavkama iz sistema sa slike 4.1, javni komunikacioni kanal se smatra autentifikovanim, tj. otvoren za prisluškivanje, ali zaštićen od umetanja ili izmene poruka od strane napadača.

Ove dodatne pretpostavke, uzete zajedno, omogućavaju sistemu da proširi koncept idealne tajnosti i ostvari praktičnu savršenu tajnost u Šenonovom smislu, čime se omogućava efikasna i autonomna generacija sigurnih ključeva za Vernamovo šifrovanje u realnim uslovima rada.

7. ANALIZA BEZBEDNOSTI I PRAKTIČNI ASPEKTI PRIMENE

Generički napadi na SKD sisteme se zasnivaju na optimalnim strategijama estimacije niza W_i . Na osnovu teoreme 6, zaključujemo da je predloženi sistem otporan na ove strategiju napada. Međutim strategije rekonstrukcije tajnog ključa K_G su najkritičnija za ovu klasu sistema. Ako Eva može da rekonstruiše K_G , tada ima isti ključ C_K kao i Alisa i Bob. U tom slučaju, optimalna Evina strategija se sastoji u generisanju sopstvenog lokalnog binarnog šuma $X_E \sim B(\epsilon)$ i praćenja svih koraka IR i PA protokola koje sprovode Alisa i Bob, [6]. Na osnovu (6.15) dobijamo da je kapacitet tajnosti [5]:

$$C_S = \min\{I(X_A; X_B), I(X_A; X_B | X_E)\} = I(X_A; X_B | X_E) = h_b(P_{AB}) - h_b(P_{AE}) = 0 \quad (7.1)$$

budući da je:

$$P_{AB} = P_{AE} = 2\epsilon(1 - \epsilon), \quad (7.2)$$

kao i da se ne primenjuje AD protokol, koji bi mogao da preokrene situaciju u Alisinu i Bobovu prednost u odnosu na Evu. Ovaj tip napada je u CR KSG sistemu sprečen kontinuiranim održavanjem ekvivokacije $H(K_G | S)$ većom od unapred odabranog praga Δ_{K_G} . Praktično to znači da je u svakom ciklusu rada sistema napadač suočen sa $2^{\Delta_{K_G}}$ jednako verovatnih hipoteza o ključu K_G , čineći ovaj sistem idealno sigurnim u Šenonovskom smislu.

U Primedba 4.2. je pokazano kako se u ovom režimu rada sistema, koga možemo nazvati *režimom idealne sigurnosti*, mogu birati relevantni parametri kojim se obezbeđuje željeni između brzine destilovanja kriptografskih ključeva i donje granice ekvivokacije ključa K_G .

U teoremi 7, pokazano je kako CR KSG prelazi u režim *perfektnje tajnosti*, izjednačavanjem ekvivokacija destilovanih ključeva i tajnog ključa KSG. Ako se ovaj

režim uporedi sa režimom idealne sigurnosti, vidimo da je cena koja se plaća smanjenje efektivne brzine destilovanja kriptografskih ključeva .

Predloženi autonomni SKD sistem je praktično uvek moguće primeniti ukoliko je stranama koje učestvuju u protokolu na raspolaganju javni autentifikovani kanal dovoljnog kapaciteta. Da bi smo dobili predstavu o ovom zahtevu, uvešćemo meru opterećenja javnog kanala po jednom bitu destilovanog ključa K_S :

$$E_{BC} = \frac{|\tilde{K}_s|_{max}}{\tilde{n}_p} = \frac{1}{\tilde{n}_p} \left(C_2 - \frac{t}{n_{IRO}} - \frac{C_1}{1-r} \right) \quad (7.3)$$

Uzimajući u obzir (4.12), ili ekvivalentno:

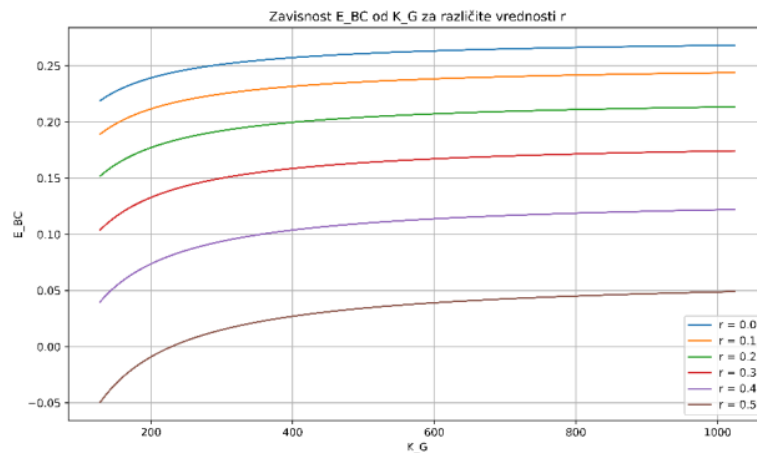
$$E_{BC} = \frac{1}{\tilde{n}_p} \left(C_2 - \frac{C_1}{1-r} \cdot \left(1 + \frac{t}{K_G} \right) \right). \quad (7.4)$$

ako se oslonimo na (4.15). Na Slika 7-1 prikazana je zavisnost (6.4) za različito r , kada sistem radi u modu perfektne tajnosti.

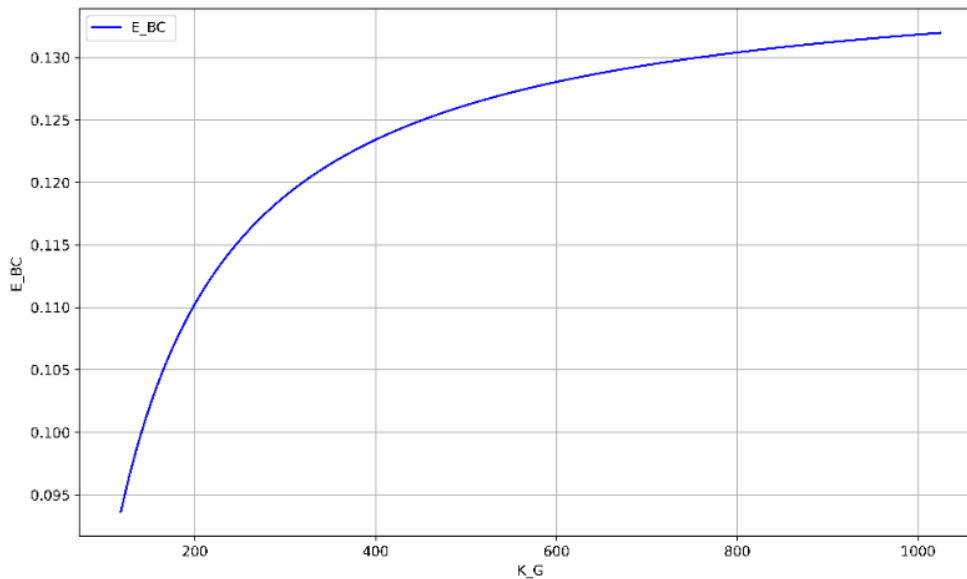
U slučaju perfektne tajnosti, na osnovu (5.18) dobijamo zavisnost:

$$E_{BC} = \frac{|\tilde{K}_s|_{max}}{\tilde{n}_p} = \frac{1}{\tilde{n}_p} \left(C_2 - C_1 - \frac{t}{n_{IRO}} \cdot \frac{C_2 + C_1}{2K_G + t} \right). \quad (7.5)$$

koja je prikazana na Slika 7-2 .



Slika 7-1 Zavisnost mere opterećenosti javnog kanala E_{BC} u režimu rada idealne sigurnosti



Slika 7-2 Zavisnost mere opterećenosti javnog kanala E_{BC} u režimu perfektne sigurnosti.

Na osnovu ovih zavisnosti, možemo zaključiti da u režimu perfektne tajnosti, za $K_G = 512$, ovaj odnos nije manji od $1/8$. Drugim rečima za on line rad autonomnog perfektno tajnog CR KSG sistema, javni kanal mora dopuštati brzine prenosa oko 8 puta veće od brzine informacionog izvora koji se štiti. Sa slike 7-1 možemo zapaziti da je za iste vrednosti K_G , i ekvivokaciju tajnog ključa K_S reda 128 b ($r = 0.2$) ovaj zahtev značajno manji i iznosi oko 5 puta. U eri savremenih telekomunikacija i interneta, ovaj zahtev ne predstavlja ozbiljno ograničenje. U off line režimu rada, ograničenost brzine prenosa po javnom kanalu utiče samo na vreme destilovanja potrebne količine kriptografskih ključeva [5] .

Praktična primena autonomnih CR KSG sistema obuhvata široki spektar scenarija, od komercijalnih do strateških od značaja za bezbednost kritične infrastrukture, diplomatije do vojnih primena. Budući da na strateškim nivoima se po pravilu razvijaju specijalizovani kompleksni sistemi generisanja i distribucije kriptografskih ključeva, autonomni CR KSG sistemi su idealni kao rezervni sistemi,

koji u slučaju prekida rada osnovnih sistema ili njihove kompromitacije ili uništenja, mogu preuzeti njihovu funkciju.

U vojnim primenama, ovi sistemi postaju posebno atraktivni usled sve prisutnog mobilnog interneta, kao što je npr. Starlink. U slučaju prekida standardnih zaštićenih veza, koje su ključne za uspešno obavljanje vojnih ili specijalnih operacija, autonomni CR KSG sistemi mogu preuzeti ulogu generisanja i distribucije kriptografskih ključeva.

Rat u Ukrajini je pokazao da sveprisutnost Starlink sistema potencijalno omogućava perfektno tajnu komunikaciju sa centralnim ili regionalnim komandama i u uslovima potpuno odsečenih ili opkoljenih vojnih jedinica iako im prethodno nisu distribuirani kriptografski ključevi ili su potpuno utrošeni.

Predloženi autonomni sistem za destilaciju tajnog ključa (SKD), zasnovan na sintetičkom izvoru zajedničke slučajnosti (CR) koji koristi generator ključa sa deljenim ključem i lokalnu čistu slučajnost, ostvaruje ograničenu i predvidivu računarsku složenost i komunikaciono opterećenje po ciklusu. Ova svojstva su od suštinske važnosti za implementaciju u ugrađenim sistemima i okruženjima sa ograničenim resursima.

7.1 Faza generisanja zajedničke slučajnosti (CR)

Blok za generisanje CR vrši bit-po-bit mod-2 sabiranje) između lokalno generisane Bernulijeve sekvence X i ključa C_K dobijenog iz generatora $KSG(K_G)$. Ova operacija zahteva ukupno n XOR operacija za blok podataka dužine n . Generisanje sekvence X podrazumeva n poziva lokalnom generatoru pseudoslučajnih nizova (RNG), dok $KSG(K_G)$ koji ispunjava kriterijum lavinske osobine, uobičajeno zahteva fiksni i mali broj operacija po bitu, u zavisnosti od konkretne implementacije generatora.

Tabela 7-1 prikazuje strukturirano poređenje široko korišćenih generatora ključa koji se mogu primeniti unutar SKD sistema, sa fokusom na njihovu operativnu složenost, memorijske zahteve i propusnost u realnim uslovima.

Tabela 7-1 Mogući generatori ključa za SDK sisteme

¹ KSG	Block size	Ops per Bit (SW)	¹ Ops per Bit (HW/AES-NI)	RAM Footprint	Throughput (MB/s, SW)	Remarks
AES (CTR/OFB)	128 bits	~10–15 ops/bit	~1 op/bit	~2–4 KB (tables)	~30–100 MB/s	High security margin, mature
³ [44,45,46] Grain v1 [47,48]	1 bit	³ ~1–3 ops/bit	~1 op/bit	~80 bytes	~50–150 MB/s	Lightweight, low area
Trivium [48,49]	1 bit	~1–3 ops/bit	~1 op/bit	~36 bytes	~50–200 MB/s	Lightweight, low area
ChaCha20 [50,51]	512 bits	~3–4 ops/bit	~1–2 ops/bit	~128 bytes	~100–400 MB/s	High performance, strong security
HC-128 [48,52]	128 bits	¹ ~4–6 ops/bit	~2 ops/bit	~4 KB	~70–200 MB/s	Balanced security and speed

Tabela uključuje sledeće pristupe:- AES u CTR/OFB režimu predstavlja sigurni KSG baziran na blok šifri, sa većom složenosti po bitu u softverskoj implementaciji, ali izuzetno efikasan u okruženjima sa odgovarajućom hardverskom podrškom [5].

7.2 Poređenje operativne složenosti po bitu tajnog ključa u SKD sistemima

Nasuprot blok šiframa, generatori šifara u obliku niza u odlikuju se izuzetno niskom složenosti po bitu i minimalnim memorijskim zahtevima, što ih čini pogodnim za SKD implementacije u mikro kontrolerima sa ograničenom RAM memorijom i niskom potrošnjom energije. ChaCha20 i HC-128 pružaju visoku propusnost i izbalansiranu bezbednost u opštim softverskim SKD rešenjima.

Na osnovu ovoga, zaključujemo:

- AES ostaje prikladan kada je dostupna hardverska podrška putem AES-NI, omogućavajući malo kašnjenje i sigurno generisanje ključa.
- Grain i Trivium su poželjni u SKD čvorovima zasnovanim na mikro kontrolerima, zbog izuzetno male računarske složenosti i male potrošnje energije.

Pri poređenju SKD arhitektura, najvažniji kriterijum za praktičnu primenljivost jeste operativna složenost po destilovanom bitu tajnog ključa, uz ekvivalentne bezbednosne garancije. Radi pravičnog poređenja, razmatramo sledeće:

- Sistem A: Klasičan SKD sistem zasnovan na prirodnim izvorima zajedničke slučajnosti (npr. bežično slabljenje, biometrijski signali), koji zahteva fazu destilacije prednosti (AD) radi smanjenja korelacije sa Evom i povećanja korelacije između Alise i Boba.

- Sistem B(Predloženi): Autonomni SKD sistem koji koristi sintetički izvor zajedničke slučajnosti, formiran kombinovanjem lokalne Bernulijeve slučajnosti i ključa dobijenog iz generatora sa deljenim ključem, $KSG(K_G)$. Ova arhitektura u potpunosti eliminiše potrebu za fazom AD, funkcionišući uz maksimalnu unutrašnju korelaciju i maksimalnu Renijevu entropiju drugog reda.

Faza destilacije prednosti (AD) u Sistem A zahteva eksponencijalno više početnih sirovih podataka da bi se postigla ista krajnja dužina bloka na kraju faze informacionog usaglašavanja (IR), naročito u uslovima visoke početne korelacije između Eve i Alise, [5]. Dobijena sekvenca ima smanjenu Renijevu entropiju drugog reda, što zahteva jaču kompresiju u fazi privatne ekstrakcije (PA) radi ispunjenja bezbednosnih parametara. U Sistemu A usled preostale korelacije sa Evom dolazi do značajno manjeg prinosa destilovanih tajnih bita po ciklusu.

Nasuprot tome, Sistem B obezbeđuje da je Renijeva entropija drugog reda jednaka maksimalnoj Šenonovoj entropiji za usaglašenu sekvencu. Ovo omogućava da faza PA funkcioniše uz minimalnu kompresiju, a fiksna bezbednosna margina nezavisna je od dužine bloka podataka n .

Kao rezultat, za dovoljno veliku vrednost n_{IR_end} , konačna dužina destilovanog tajnog ključa u Sistemu B je približno jednaka n_{IR_end} dok u Sistemu A može biti znatno manja. S obzirom da oba sistema imaju sličnu složenost u fazama IR efektivna složenost po destilovanom bitu za Sistem A postaje znatno veća zbog potrebe za fazom AD i smanjenog izlaznog kapaciteta nakon PA.

S druge strane, Sistem B zahteva samo dodatni utrošak generisanja ključa pomoću $KSG(K_G)$, što se može efikasno implementirati uz ~1–15 operacija po generisanom bitu ključa, u zavisnosti od izabranog KSG (AES, Grain, Trivium itd.), i sa minimalnim dodatnim zahtevima za RAM i potrošnju energije, vidi Tabelu 7.1.

Štaviše, ova prednost sistema B dodatno raste kako raste početna korelacija Eva-Alisa u Sistemu A, što dodatno smanjuje efikasnost Sistema A. Dakle, predložena arhitektura ne samo da pojednostavljuje protokol eliminacijom faze AD, već i maksimizuje efektivnu brzinu generisanja ključa, dok istovremeno minimizuje operativna i komunikaciona opterećenja, čime postiže superiornu efikasnost za bezbednu autonomnu destilaciju tajnog ključa (SKD) u praktičnim implementacijama.

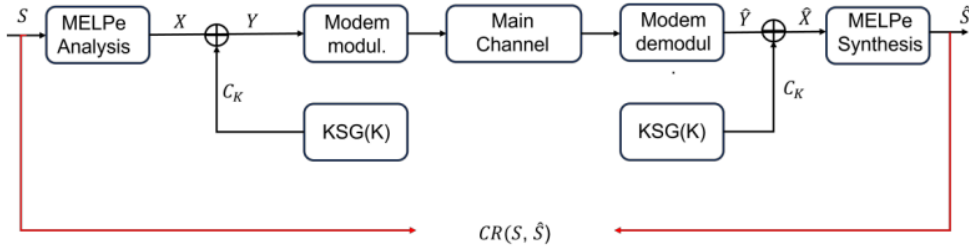
7.3 Eksperimentalna verifikacija

Eksperimentalna verifikacija predloženog sistema izvršena je na ⁵ **Vlatacom Personal Crypto Platform for Voice encryption (vPCP-V)**. Empirijska merenja pokazuju da se uz adekvatan izbor sistemskih parametara za prenos glasa od 1,2 kb/s može postići brzina tajnog ključa (KR) do 8,8 kb/s, uz zanemarljivu brzinu curenja (LR). Koliko nam je poznato, ovo je prvi autonomni, perfektno tajni sistem za glasovnu komunikaciju sa niskom brzinom prenosa koji ne zahteva eksplicitno prethodno generisanje i distribuciju kriptografskih ključeva [4].

Generički tajni sistem sa niskom brzinom prenosa govora sa niskom brzinom prenosa prikazan je na slici 1. Izabrali smo standardni MELPe vokoder sa niskom brzinom prenosa i brzinom prenosa od 1,2 kb/s [38], [39]. Treba napomenuti da se MELPe vokoder može zameniti bilo kojim drugim standardnim vokoderom sa sličnim performansama. Ulazni govorni signal S se sempluje na 8 kHz, diskretizuje se sa 16 bita po semplu i deli na frejmove trajanja 67,5 ms (540 semplova). U MELPe analizatoru, za svaki ulazni frejm se generiše 81 bit, od kojih 80 bita kodira 10 LSP parametara LP modela produkcije govora, dok je 81. bit sinhronizacije. Ovaj tok bita se šifruje dodavanjem modula 2 binarnom pseudoslučajnom nizu C_K generisanom generatorom toka ključeva $KSG(K)$, sa tajnim ključem K , koji mora biti podeljen između legitimnih strana pre nego što komunikacija počne. Šifrovani tekst Y se prenosi preko glavnog kanala nakon odgovarajuće modulacije.

Na strani prijemnika, nakon demodulacije, vrši se dešifrovanje. Dešifrovanje se vrši dodavanjem modula 2 sinhrono generisanom binarnom nizu C_K na strani prijemnika. Kao rezultat toga, dobijaju se identični LSP parametri, koji proizvode rekonstruisani govorni signal $\hat{S}$ u MELPe bloku sintetizatora. Sa $CR(S, \hat{S})$ označavamo našeg prvog kandidata za zajednički izvor koincidencije, formiran od

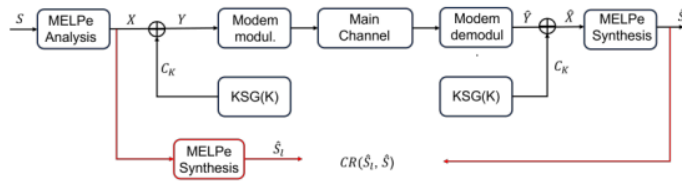
ulaznog govornog signala S na strani predajnika i govornog signala $\hat{S}$ sintetizovanog na strani prijemnika, videti Slika 7-3



Slika 7-3 Generička šema bezbedne komunikacije sa niskom brzinom prenosa podataka korišćenjem MELPe koda.

Kriptografski deo sistema sastoji se od KSG(K) generatora binarnog pseudoslučajnog niza C_K , koji se sabira po modulu 2 sa binarnim nizom koji dolazi iz analizatora. Sa $CR(S, \hat{S})$ je označen izvor zajedničke slučajnosti, formiran od ulaznog govornog signala S na strani predajnika i govornog signala $\hat{S}$ sintetizovanog na strani prijemnika.

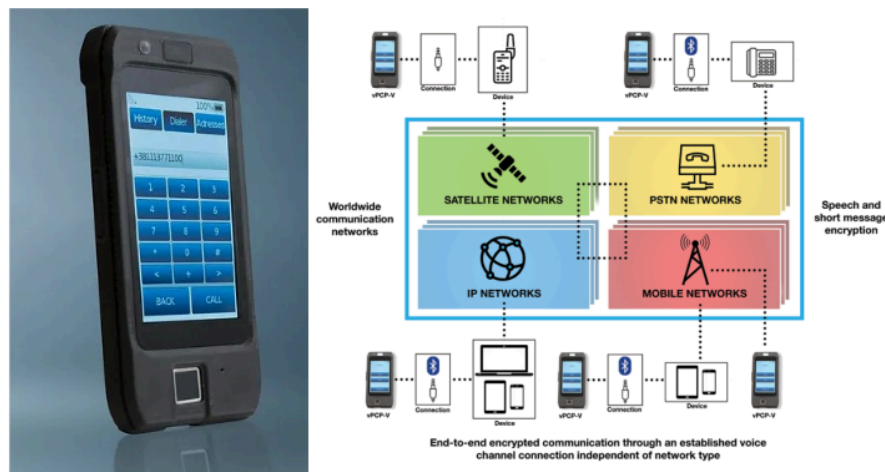
Slika 7-4 prikazuje proširenje generičke šeme sa slike 1 sa lokalnom MELPe sintezom na strani predajnika. Sa $CR(\hat{S}_i, \hat{S})$ je označen naš drugi kandidat za izvor zajedničke slučajnosti, formiran od lokalno sintetizovanog govornog signala $\hat{S}_i$ na strani predajnika i govornog signala $\hat{S}$ sintetizovanog na strani prijemnika. Ako nema grešaka u prenosu, filteri sinteze na strani prijema i predajnika su jednaki, a razlike u sintetizovanim signalima dolaze iz različitih lokalnih izvora slučajnosti, koji se koriste za formiranje kompleksnog pobuđivanja MELPe vokodera sintetizatora [4].



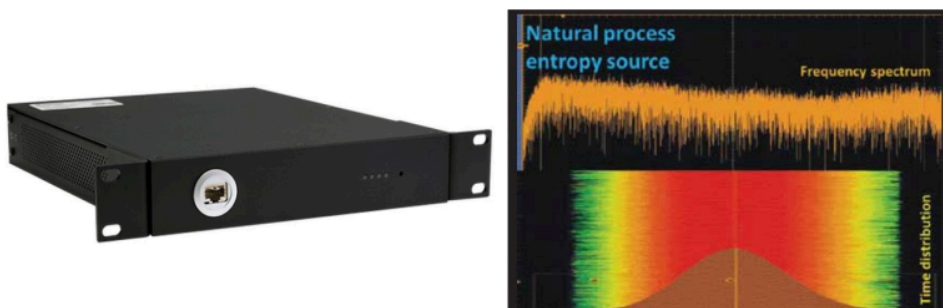
Slika 7-4 Proširenje generičke šeme prikazane sa lokalnom MELPe sintezom na strani predajnika. Sa $CR(\hat{S}_i, \hat{S})$ je označen izvor zajedničke slučajnosti, formiran od lokalno sintetizovanog govornog signala $\hat{S}_i$ na strani predajnika i govornog signala $\hat{S}$.

Prethodna analiza pokazuje da su u fazi otvorenog govora dostupna dva izvora zajedničke slučajnosti, $CR(S, \hat{S})$ i $CR(\hat{S}, \hat{S})$. Da bismo procenili koji je od ovih izvora pogodniji, sprovedi smo eksperimentalnu evaluaciju u realnim uslovima komunikacije sa vPCP-V Vlatacom lična krypto platforma za šifrovanje glasa dizajnirana za upotrebu u bilo kom dostupnom komunikacionom sistemu (glas preko internet protokola (VoIP), javni, fiksni, mobilni ili satelitski, Slika 7-5.

Generator slučajnih nizova Vlatacoma zasnovan na izvoru entropije prirodnog procesa sa ugrađenom proverom slučajnosti prikazan je na Slika 7-6.



Slika 7-5 Vlatacom lična krypto platforma za šifrovanje govora dizajnirana za upotrebu u bilo kom dostupnom komunikacionom sistemu



Slika 7-6 Generator slučajnih nizova Vlatacoma zasnovan na izvoru entropije prirodnog procesa sa ugrađenom proverom slučajnosti.

Cena koja se plaća za savršenu tajnost APS-VCS sistema je uspostavljanje i održavanje javnog kanala tokom bezbednog razgovora. Međutim, glavni i javni kanal

rade u asinhronom režimu, što značajno pojednostavljuje praktičnu implementaciju. Jedini uslov koji mora biti ispunjen jeste održavanje konstantne brzine čitanja FIFO memorije od 1,2 kb/s za Vernamovu šifru.

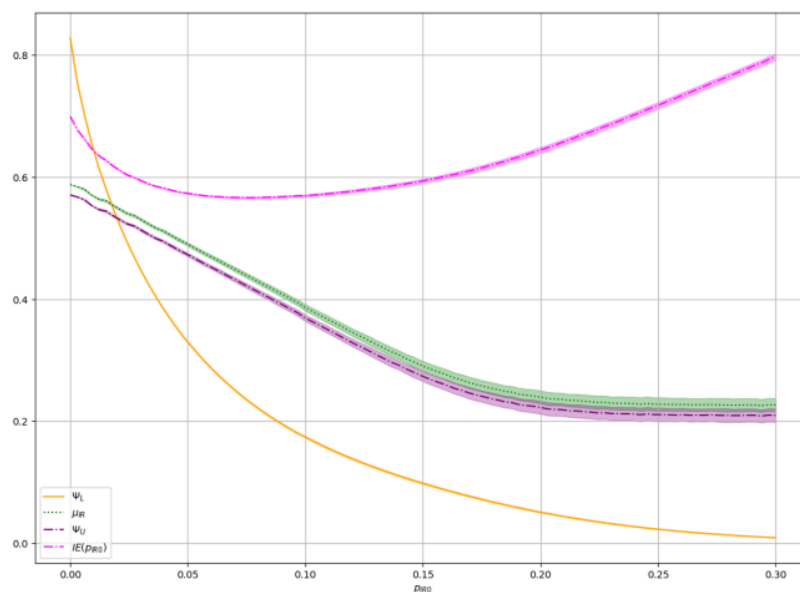
Perfektno tajni sistem govorne komunikacije zasniva se na MELPe vokoderu od 1,2 kb/s i Vernamovoj šifri. Osnova za generisanje i distribuciju kriptografskih ključeva su dva izvora deljene slučajnosti i SKD protokol, koji zahteva upotrebu dodatnog autentifikovanog kanala. Glavni izvor CR je specijalno dizajnirani LP sintisajzer, koji obezbeđuje potrebnu količinu inovativne entropije zasnovane na lokalnom izvoru slučajnosti. Izborom parametara sigurnosne margine i sintisajzera, kao što su brzina uzrokovanja i odnos signal-šum (SNR), projektant sistema može da obezbedi željenu brzinu tajnog ključa od 1,2 kb/s kako bi se održala savršena tajnost primenjene Vernamove šifre. Maksimalna vrednost parametra bezbednosti je oko 460 bita, što obezbeđuje zanemarljivo curenje generisanih kriptografskih ključeva.

Potreba za dodatnim pouzdanim autentifikovanim javnim kanalom može se smatrati cenom koja se plaća za savršenu tajnost. Međutim, asinhroni rad glasovnog kodera i sistema za šifrovanje u glavnom kanalu u sprezi sa delom sistema koji koristi javni kanal značajno prevazilazi tehničke teškoće u implementaciji sistema i čini ga praktično upotrebljivim. Eksperimentalna evaluacija vPCP-V sistema potvrđuje ovu tvrdnju.

U daljem razvoju ove klase sistema, razmatra se mogućnost integracije glavnog i javnog kanala odgovarajućim procedurama multipleksiranja, što bi omogućilo dalje pojednostavljenje operativne upotrebe APS-VCS i njegovu širu upotrebu u praksi.

Ovim je dokazano da je predloženi sistem praktično uvek moguće primeniti ukoliko je stranama koje učestvuju u protokolu na raspolaganju javni autentifikovani kanal dovoljnog kapaciteta.

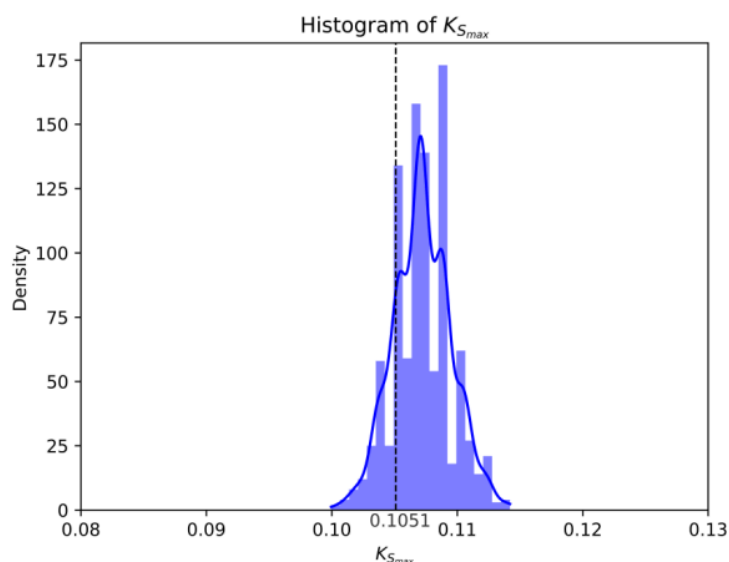
Slika 7-7 prikazuje empirijsko rasprostriranje četiri merene krive sistemskih parametara (žuta, ljubičasta, crvena, zelena), uz prikaz intervala poverenja od jedne standardne devijacije (jedan sigma) oko svake krive. Rezultati pokazuju izuzetno slaganje između simulacionih i teorijskih predviđanja iz Slike 8, potvrđujući tačnost analitičkog modela pod uslovima perfektne tajnosti.



Slika 7-7 Empirijsko rasprostranje za jednu σ standardne devijacije za merene stope generisanja tajnog ključa u režimu perfektne tajnosti, tokom 1000 simulacionih ciklusa predloženog SKD sistema zasnovanog na zajedničkoj slučajnosti (CR), sa početnom vrednošću $n_{IR0} = 2000$ bita.

Žute linije predstavljaju donju granicu ekvivokacije za Evu (napadača). Zelene linije označavaju efikasnost preostalog korisnog podatka nakon IR protokola. Gornja granica, umanjena za bezbednosnu marginu $\tilde{\epsilon}$, prikazana je ljubičastim linijama. Ulazna inovativna entropija IE predstavljena je purpurnim linijama.

Slika 7-8 prikazuje histogram dužina generisanih perfektno tajnih ključeva kroz sve simulacije (puna linija), dok isprekidana vertikalna linija označava teorijski očekivanu vrednost. Zbog niske varijanse u simulacijama, zaključuje se da se eksperimentalni i teorijski rezultati za stopu perfektne tajnosti odlično poklapaju.



Slika 7-8 Histogram generisanih perfektno tajnih dužina ključeva tokom 1000 simulacija (puna linija). Vertikalna isprekidana linija označava teoretski očekivanu vrednost brzine tajnog ključa $|\tilde{K}_s|_{max} = 0.1051$. Mala varijansa pokazuje izuzetno slaganje između eksperimentalnih i teorijskih rezultata..

Očekivana teorijska vrednost stope destilovanih tajnih ključeva potvrđuje sposobnost sistema da konzistentno generiše tajne ključeve pri predviđenoj stopi, uz očuvanje perfektne tajnosti.

Krive u žutoj, purpurnoj, crvenoj i zelenoj boji predstavljaju različite konfiguracije sistemskih parametara. Izuzetno poklapanje sa teorijskim predviđanjima dodatno potvrđuje validnost analitičkog modela.

8. ZAKLJUČAK I PRAVCI BUDUĆIH STRAŽIVANJA

Novi metod generisanja izvora zajedničke slučajnosti (IZS) kroz upotrebu determinističkog generatora ključeva zasnovanog na prethodno podeljenom tajnom ključu, što u osnovi čini osnovu za kreiranje sigurnih kanala komunikacije između dve legitimne strane – Alise i Boba je osnovni doprinos ove disertacije. Umesto oslanjanja na fizički sloj ili fizičke izvore entropije, ovde se koristi funkcionalno projektovan ključni generator KSG(K), koji na osnovu poznatog zajedničkog ključa K proizvodi nizove koji predstavljaju zajednički entropijski resurs.

Jedinstvena i nova karakteristika ovog pristupa jeste njegovo proširivanje preko superpozicije lokalno generisanih, nezavisnih nizova čiste slučajnosti, čime se dodatno maskiraju determinističke komponente i postiže robusnost sistema. Time se funkcionalno simulira Maurer-ov satelitski scenario, ali bez potrebe za složenom fizičkom infrastrukturu. Prednost ovakve arhitekture je u tome što omogućava zatvorene, analitički izvodljive izraze za ključne parametre kao što su stopa zajedničke entropije, količina informacija dostupnih prisluškivaču i uslovi za sigurnu ekstrakciju tajnog ključa.

Naravno, tajnost početnog ključa K mora biti zagarantovana. Ako napadač, označen kao Eva, poseduje delimičnu ili statističku informaciju o ovom ključu, moguće je da izvede napad koji kompromituje celu arhitekturu. Stoga se bezbednost sistema kvantifikuje pomoću mere ekvivokacije – koncepta koji je još Klod Šenon uveo kao temeljnu metriku sigurnosti kod sistema sa simetričnim ključevima.

Uvedena je klasa determinističkih IZS sistema za koje se može formalno pokazati donja granica na Šenonovu ekvivokaciju tajnog ključa K. Time se stvara osnova za bezbednu destilaciju ključeva i u nepovoljnim uslovima – uključujući prisustvo šuma, ograničenja u komunikacionim resursima, i postojanje delimično informisanog napadača.

Uvođenjem strukturiranog pristupa koji povezuje determinističke generatore sa lokalnim izvorima čistog šuma, stvara se fleksibilan okvir koji može da se primeni u raznovrsnim komunikacionim uslovima – od ograničenih IoT okruženja do zahtevnih vojno-bezbednosnih aplikacija. Teorijska analiza je potkrepljena konkretnim

proračunima, a sistem se može implementirati uz upotrebu postojećih digitalnih resursa i algoritama.

Predstavljena je nova SKD paradigma koristeći osvežavanje sintetičkog ključa i autonomno osvežavanje ključa. Dizajn je validiran teoretski i praktično, nudeći:

- Parametarski kontrolisanu ekvivokaciju,
- Visoko efikasno pomirenje zasnovano na Winnow-u,
- Bezbedan rad bez destilacije koristi.

Glavni doprinosi rada su:

1. Novi matematički okvir za sintezu zajedničke slučajnosti iz determinističkog kriptografskog generatora.

2. Teorijsko izvođenje donjih granica za ekvivokaciju zajedničkih ključeva, čime se obezbeđuje ograničeno curenje informacija. Definisano je dokazano sedam novih teorema čime je dokazan kvalitet novog modela.

3. Potpuno autonomna arhitektura SKD protokola koja integriše generisanje IZS, usklađivanje i ponovnu upotrebu ključeva.

4. Eksperimentalna evaluacija visoke efikasnosti i minimalne komunikacione složenosti Winnow protokola.

5. Praktični uvidi u konfiguraciju sistema u cilju maksimizacije stope tajnosti i održavanja ekvivokacije.

U režimu perfektne tajnosti, za $K_G = 512$ za on line rad novog autonomnog perfektnog tajnog CR KSG sistema, javni kanal mora dopuštati brzine prenosa oko 8 puta veće od brzine informacionog izvora koji se štiti.

Takođe smo dobili da je za iste vrednosti K_G , i ekvivokaciju tajnog ključa K_S reda $128\text{ b } (r = 0.2)$. U eri savremenih telekomunikacija i interneta, ovaj zahtev ne predstavlja ozbiljan izazov. U off line režimu rada, ograničenost brzine prenosa po javnom kanalu utiče samo na vreme destilovanja potrebne količine kriptografskih ključeva.

Integracijom i optimizacijom Winnow protokol za kratke blokove ($N = 8$), postiže se visoka efikasnost i niska stopa grešaka u rekonsilijaciji. Analizom su identifikovana

dva režima rada sistema: idealna i savršena tajnost, sa pripadajućim stopama generisanja ključa do 22%, uz istovremeno ispunjenje uslova $KDR < 10^{-5}$ i $LR < 10^{-10}$.

Mogući pravci budućeg istraživanja i daljeg razvoja ove oblasti obuhvataju sledeće tematske celine:

- Implementacija razvijenog sistema u realnim uslovima rada. Jedan od najvažnijih narednih koraka jeste praktična realizacija predloženog modela u kontrolisanom, ali dinamičnom okruženju, kako bi se testirala robusnost algoritama, otpornost na smetnje i kompatibilnost sa postojećom infrastrukturom. Ova faza omogućila bi evaluaciju performansi pod stvarnim opterećenjem i identifikaciju potencijalnih inženjerskih ograničenja.
- Integracija sistema u operativne bezbednosne protokole. Dalje istraživanje može biti usmereno ka uključivanju predloženog modela u realne bezbednosne arhitekture, kao što su sistemi za zaštitu komunikacije u vojnim, diplomatskim ili industrijskim aplikacijama. U tom kontekstu, potrebno je prilagoditi model standardima interoperabilnosti, kao i obezbediti formalnu verifikaciju njegovih bezbednosnih karakteristika.
- Uvođenje adaptivnih SKD sisteme koji dinamički podešavaju parametre generisanja ključeva kao odgovor na sistemske uslove u realnom vremenu, kao što su različite verovatnoće grešaka i dostupnost entropije.
- Eksploracija potencijala velikih jezičkih modela (LLM) kao determinističkih izvora zajedničke slučajnosti. Novi pravac istraživanja mogao bi uključiti upotrebu semantički stabilnih odgovora LLM-ova kao osnove za generisanje entropije koja je zajednička dvema ili više strana. Ovaj pristup otvara mogućnosti za razvoj teorije sinteze kriptografskih ključeva (SKD) koja se ne oslanja na fizičke izvore slučajnosti, već na semantičko poravnanje deterministički generisanih odgovora.
- Razrada kvantne verzije modela. Istraživanje potencijalne primene predloženog sistema u kontekstu kvantne bezbednosti predstavlja izazovan, ali značajan pravac. To podrazumeva analizu mogućnosti adaptacije arhitekture i algoritama za scenarije u kojima se komunikacija odvija u kvantnom domenu, uz poštovanje principa kvantne mehanike, kao što su

superpozicija, kvantna neodređenost i nemogućnost kloniranja kvantnih stanja. Takva proširenja mogla bi doprineti razvoju hibridnih kvantno-klasičnih sistema bezbednosti.

9. LITERATURA

- [1] C. E. Shannon, "Communication Theory of Secrecy Systems*," *Bell System Technical Journal*, vol. 28, p. 656–715, October 1949.
- [2] NIST, *Data Encryption Standard*, 1999.
- [3] J. Daemen and V. Rijmen, *The Design of Rijndael: The Advanced Encryption Standard (AES)*, Springer Berlin Heidelberg, 2020.
- [4] J. Radomirović, M. Milosavljević, S. Čubrilović, Z. Kuzmanović, M. Perić, Z. Banjac and D. Perić, "A Class of Perfectly Secret Autonomous Low-Bit-Rate Voice Communication Systems," *Symmetry*, vol. 17, p. 365, February 2025.
- [5] D. Cizelj, M. Milosavljević, J. Radomirović, N. Latinović, T. Unkašević and M. Vučetić, "Synthesis of Sources of Common Randomness Based on Keystream Generators with Shared Secret Keys," *Mathematics*, vol. 13, p. 2443, July 2025.
- [6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, p. 733–742, May 1993.
- [7] G. S. Vernam, *Secret Signaling System*. U. S. Patent 1310719A, 1919.
- [8] T. Lugin, "One-Time Pad," in *Trends in Data Protection and Encryption Technologies*, V. Mulder, A. Mermoud, V. Lenders and B. Tellenbach, Eds., Cham, Springer Nature Switzerland, 2023, p. 3–6.
- [9] A. V. McCree, "Low-Bit-Rate Speech Coding," in *Springer Handbook of Speech Processing*, J. Benesty, M. M. Sondhi and Y. A. Huang, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, p. 331–350.
- [10] MELPe TSVCIS Available online: <https://melpe.com/melpe-tsvcis/> (accessed on 15 November 2024)., 2024.
- [11] Nato Standardization Office. Available online: <https://nso.nato.int/nso/nsdd/main/standards> (accessed on 15 November 2024)., 2024.
- [12] Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S. X.; Hanzo, L. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials* 2022, 24, 839-894.

- [13] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, pp. 1121-1132, 1993.
- [14] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, pp. 3047-3061, 2004.
- [15] J. Zhang, T. Q. Duong, A. Marshall and R. Woods, "Key Generation From Wireless Channels: A Review," *IEEE Access*, vol. 4, pp. 614-626, 2016.
- [16] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao and A. Hu, "Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities," *Entropy*, vol. 21, 2019.
- [17] J. Zhang, T. Q. Duong, R. Woods and A. Marshall, "Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview," *Entropy*, vol. 19, 2017.
- [18] J. Radomirović, M. Milosavljević, Z. Banjac and M. Jovanović, "Secret Key Distillation with Speech Input and Deep Neural Network-Controlled Privacy Amplification," *Mathematics*, vol. 11, 2023.
- [19] M. Galis, M. Milosavljević, A. Jevremović, Z. Banjac, A. Makarov and J. Radomirović, "Secret-Key Agreement by Asynchronous EEG over Authenticated Public Channels," *Entropy*, vol. 23, 2021.
- [20] J. Pourbemany, Y. Zhu and R. Bettati, "A Survey of Wearable Devices Pairing Based on Biometric Signals," 24 July 2021.
- [21] G. Li, Z. Zhang, J. Zhang and A. Hu, "Encrypting Wireless Communications on the Fly Using One-Time Pad and Key Generation," *IEEE Internet of Things Journal*, vol. 8, pp. 357-369, 2021.
- [22] A. V. McCree and T. P. Barnwell, "A mixed excitation LPC vocoder model for low bit rate speech coding," *IEEE Transactions on Speech and Audio Processing*, vol. 3, pp. 242-250, 1995.
- [23] *Vlatacom Institute—Encryption and Authentication*, 2024.
- [24] F. Itakura, "Line spectrum representation of linear predictor coefficients of speech signals," *The Journal of the Acoustical Society of America*, vol. 57, p. S35–S35, April 1975.
- [25] S. Goldwasser, G. N. Rothblum and P. Vasudevan, *Language Models as Knowledge Bases for Factoid Question Answering*, 2023.

- [26] Y. Yarom and R. Oppenheim, "LM-Key Exchange: Enabling Secret Key Agreement via Language Models.," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2024.
- [27] E. B. Barker and J. M. Kelsey, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, 2015.
- [28] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, p. 3–28, January 1992.
- [29] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Advances in Cryptology — EUROCRYPT '93*, Springer Berlin Heidelberg, p. 410–423.
- [30] A. Rényi, "On Measures of Entropy and Information," 1961.
- [31] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, p. 143–154, April 1979.
- [32] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, p. 1915–1923, 1995.
- [33] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A*, vol. 67, p. 052303, 19 May 2002.
- [34] Q. Wang, X. Wang, Q. Lv, X. Ye, Y. Luo and L. You, "Analysis of the information theoretically secret key agreement by public discussion," *Security and Communication Networks*, vol. 8, p. 2507–2523, January 2015.
- [35] Y. Luo, X. Cheng, H.-K. Mao and Q. Li, "An Overview of Postprocessing in Quantum Key Distribution," *Mathematics*, vol. 12, p. 2243, July 2024.
- [36] A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, Handbook of applied cryptography, Rev. repr. with updates, [5. print.] ed., Boca Raton, Fla. [u.a.]: CRC Press, 2001.
- [37] M. Milosavljević, J. Radomirović, T. Unkašević and B. Božilović, "One Class of Ideally Secret Autonomous Symmetric Cipherng Systems Based on Wiretap Polar Codes," *Mathematics*, vol. 12, p. 3724, November 2024.

- [38] K. Kumar, K. R. Ramkumar and A. Kaur, "A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, p. 3878–3885, June 2022.
- [39] M. Kara, H. R. J. Merzeh, M. A. Aydın and H. H. Balık, "VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain," *Computer Communications*, vol. 198, p. 247–261, January 2023.

Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva

ORIGINALITY REPORT

3%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.mdpi.com Internet	194 words — 1%
2	nardus.mpn.gov.rs Internet	105 words — 1%
3	Dejan Cizelj, Milan Milosavljević, Jelica Radomirović, Nikola Latinović, Tomislav Unkašević, Miljan Vučetić. "Synthesis of Sources of Common Randomness Based on Keystream Generators with Shared Secret Keys", Mathematics, 2025 Crossref	91 words — 1%
4	singipedia.singidunum.ac.rs Internet	29 words — < 1%
5	www.vlatacominstitute.com Internet	27 words — < 1%
6	www.fonforum.org Internet	21 words — < 1%
7	eteze.bg.ac.rs Internet	12 words — < 1%
8	repozitorij.fsb.unizg.hr Internet	10 words — < 1%

9	danicar.info Internet	9 words — < 1 %
10	discovery.researcher.life Internet	9 words — < 1 %
11	micro.co.rs Internet	9 words — < 1 %
12	patents.google.com Internet	9 words — < 1 %
13	www.cek.ef.uni-lj.si Internet	9 words — < 1 %
14	Jelica Radomirović, Milan Milosavljević, Sara Čubrilović, Zvezdana Kuzmanović et al. "A Class of Perfectly Secret Autonomous Low-Bit-Rate Voice Communication Systems", Symmetry, 2025 Crossref	8 words — < 1 %
15	repositorio.upct.es Internet	8 words — < 1 %
16	www.vladimirbozovic.net Internet	8 words — < 1 %
17	Information Security and Cryptography, 2015. Crossref	7 words — < 1 %
18	Remi A. Chou, Matthieu R. Bloch, Emmanuel Abbe. "Polar Coding for Secret-Key Generation", IEEE Transactions on Information Theory, 2015 Crossref	7 words — < 1 %

EXCLUDE QUOTES ON

EXCLUDE BIBLIOGRAPHY ON

EXCLUDE SOURCES OFF

EXCLUDE MATCHES OFF