Primjena staničnih automata u razvoju kritopisnih sustava

Liović, Aleksandar

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:179749

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-09-02**

Sveučilište u Zagrebu
Filozofski fakultet
University of Zagreb
Faculty of Humanities
and Social Sciences

Repository / Repozitorij:

ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2023./2024.

Aleksandar Liović

Primjena staničnih automata u razvoju kritopisnih sustava

Završni rad

Mentor: dr. sc. Vjera Lopina

Zagreb, svibanj 2024.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

1. Uvod

Stanični automati su posebna vrsta automata karakterizirana svojim svojstvom simuliranja složenih ponašanja prema jednostavno definiranim pravilima. Pronašli su primjenu u raznim znanstvenim područjima, uključujući i kriptografiju. Međutim, stanični automati se u praksi kriptografije primjenjuju isključivo u modernim, računalnim sustavima koji se bave digitalnim podatcima. Ovaj rad proučava primjenu staničnih automata u kriptografiji na način da se princip rada staničnog automata, jednostavno primjenjivanje pravila koje vodi nepredvidljivim rezultatima, ilustrira kroz razvoj kritopisnih sustava koji koriste klasične metode zamjene, premještanja te kombinacije oba.

U ovu svrhu, ovaj rad najprije nudi teoretski pregled staničnih automata pri čemu se izdvajaju blokovski stanični automati, kao i teoretski pregled kriptografije s fokusom na kritopisne sustave. Ova teorija zatim se primjenjuje u razvoju algoritama kritopisnih sustava inspiriranih blokovskim staničnim automatima koji su izabrani zbog svojeg svojstva reverzibilnosti, što omogućuje postupak raskrivanja ključan za kritopisne sustave. Razvijen je i definiran stanični automat koji može služiti toj namjeni, a prema njemu su uspostavljenja pravila zamjene i premještanja kojima se realiziraju pravila osmišljenog staničnog automata. Prikazan je i postupak zakrivanja ovim kritopisnim sustavima te su isti evaluirani u svojoj sigurnosti.

Ovaj rad nastoji spojiti područja teorije automata i kriptologije, konkretnije staničnih automata i kritopisnih sustava, na dosad neviđen način. Namjera je kroz razvoj kritopisnih sustava približiti koncept staničnih automata koji su u današnje vrijeme privlačni području kriptografije kao modeli složenosti.

2. Stanični automati

U staroj Grčkoj, svijet su pokretali bogovi – vukli su sunce preko neba, donosili kiše, čak su i kontrolirali ljudsku sudbinu. U modernijim shvaćanjima, naš svijet može se promatrati kao automat – sam se pokreće koristeći složeni unutarnji mehanizam. Toffoli i Margolus (1987) predstavljaju stanične automate kao svojevrsne sintetičke svjetove koje pokreću jednostavna pravila nalik onima kakva se mogu pronaći u uputstvima za neku društvenu igru. Ovi svjetovi imaju vlastite vrste materije koje se mijenjaju kroz vrijeme i prostor svemira u kojem se nalaze, a bilo tko može preuzeti ulogu stvaratelja i definirati pravila u skladu kojih će se materija svijeta ponašati.

Stanični automati su diskretni, apstraktni računalni sustavi koji su se pokazali korisnima kao opći modeli složenosti, ali i kao specifični modeli u raznim znanstvenim područjima. Stanični automati su prostorno i vremenski diskretni: diskretno vrijeme označava vrijeme koje se razmatra u odvojenim vremenskim koracima, a diskretan prostor označava prostor koji se razmatra kao da je sastavljen od odvojenih točka, u ovom kontekstu stanica. U svakoj vremenskoj instanci, stanice poprimaju jedno od konačnog skupa stanja. One evoluiraju paralelno u diskretnim vremenskim koracima, slijedeći funkcije ažuriranja stanja, odnosno dinamička pravila prijelaza stanja, pri čemu ažuriranje stanja stanice uzima u obzir stanja stanica u njenoj lokalnoj okolini. Nadalje, stanični automati su apstraktni – ne ovise o specifičnim vrijednostima ili fizičkim interpretacijama, što znači da vremenski i prostorno mogu biti potencijalno beskonačni. Treće svojstvo sustava staničnih automata jest da su računalni, što znači da su sposobni obavljati računanje ili izvoditi algoritme i logičke operacije, kao i automatizirati svoje zadatke bez ljudske intervencije. Unatoč tome što funkcioniraju drugačije od ostalih računalnih sustava nalik Turingovim strojevima, stanični automati s odgovarajućim pravilima mogu emulirati univerzalni Turingov stroj i stoga, prema Turingovoj teoriji, takvi stanični automati mogu izvršiti bilo koji računalni algoritam (Berto i Tagliabue, 2023).

Morita (2018) definira stanični automat kao sustav koji se sastoji od velikog, teoretski beskonačnog broja polja povezanih u mrežnom prostoru. Svako polje u ovoj mreži naziva se stanica, a čini ju jedan konačni stroj. Svaka stanica ima svoje tekuće stanje koje mijenja ovisno o vlastitom stanju i stanju stanica u svojoj lokalnoj okolini, odnosno susjedstvu. Skup svih stanja stanica u susjedstvu o kojima ovisi prijelaz stanja naziva

se konfiguracija susjedstva, a sam prijelaz stanja stanice određen je lokalnom funkcijom. Primjenom te lokalne funkcije na sve stanice u mrežnom prostoru u jednom vremenskom koraku ostvaruje se prijelaz cjelokupnog staničnog prostora. Takva prijelazna funkcija naziva se globalna funkcija i ona opisuje prijelaz staničnog automata iz jedne generacije, skupa svih stanica automata u određenom vremenskom koraku, u sljedeću.

Stanični automati opisuju se kroz četiri glavne osobine: stanični prostor, susjedstvo stanice, konačan skup stanja stanice te lokalna funkcija (Hadeler i Müller, 2018). Zbog slobode u određivanju ovih parametra postoje raznoliki oblici staničnih automata. Proizvoljno se definira izgled mreže stanica, što čini susjedstvo jedne stanice, kakva sve stanja stanica može poprimiti te prema kojim se pravilima mijenja stanje pojedine stanice.

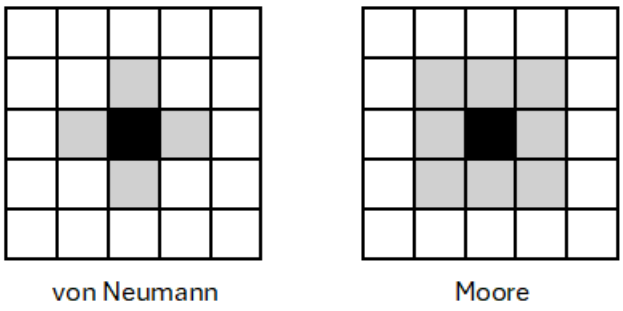
Stanični prostor je osobina staničnog automata koja definira raspored stanica u diskretnom prostoru. Glavni prostorni parametar koji najviše utječe na rad automata je dimenzija automata. Ovisno o dimenziji, stanični automat može biti jednodimenzionalan, dvodimenzionalan, trodimenzionalan i tako dalje do proizvoljno n-dimenzionalnog staničnog automata (Berto i Tagliabue, 2023).

Najjednostavniji stanični automati su elementarni stanični automati. Elementarni stanični automati su jednodimenzionalni, što znači da su njihove stanice smještene u jednu liniju. Svaka stanica ima samo dva moguća stanja, 1 ili 0, koja poprima ovisno o svojem susjedstvu koje čine dvije stanice: jedna slijeva i druga zdesna. Postoji osam mogućih konfiguracija u kojem se jedna stanica može pronaći, pošto se uzima u obzir tekuće stanje dotične stanice, kao i tekuća stanja njenih dvaju susjeda; svaka od triju stanica može poprimiti jedno od dva stanja, što znači da postoji $2^3 = 8$ mogućih permutacija. Nad svaku stanicu se primjenjuje pravilo ovisno o aktualnoj konfiguraciji koje određuje stanje stanice u sljedećem vremenskom koraku, odnosno u sljedećoj generaciji automata. Kako postoji osam mogućih konfiguracija za kojih pravilo određuje hoće li stanica biti 1 ili 0 u sljedećoj generaciji, postoji $2^8 = 256$ mogućih permutacija pravila. Ovih 256 skupova pravila čine ujedno i 256 mogućih elementarnih staničnih automata koje imenujemo prateći Wolframov kod, shemu za imenovanje elementarnih staničnih automata strukture riječi „Pravilo“ koju prati broj između 0 i 255 koji specificira skup pravila aktualan za pojedini automat. Tako na primjer imamo Pravilo 110, elementarni stanični automat koji je pokazao svojstvo simuliranja

univerzalnog Turingovog stroja, što znači da se teoretski bilo koji računalni algoritam može izvršiti koristeći Pravilo 110 (Wolfram, 2002).

Dvodimenzionalni stanični automati uključuju dodatnu dimenziju koja metaforično i doslovno produbljuje rad automata. U jednodimenzionalnim staničnim automatima se gledao samo redoslijed stanica koje su smještene jedne do druge. Oblik stanica nije bio relevantan za takav poredak, za razliku od dvodimenzionalnih staničnih automata kod kojih oblik stanice utječe na oblik čitave mreže. Najčešće se stanice raspoređuju u beskonačnom nizu kvadrata, ali koriste se i trokuti i heksagoni kao oblici stanica, a mogu se koristiti čak i nedosljedni oblici povezani u nepravilnu mrežu (Hadeler i Müller, 2018).

Ova dodatna dimenzija predstavlja i dodatan problem definiranja susjedstva. Određivanje koje stanice čine susjedstvo pojedine stanice ima velik utjecaj na rad cjelokupnog automata. Kod dvodimenzionalnih staničnih automata, dvije najčešće sheme susjedstva koje se koriste su von Neumannovo susjedstvo i Mooreovo susjedstvo.



Slika 1. Von Neumannovo i Mooreovo susjedstvo, izvor: rad autora

Kao što je prikazano na slici 1, von Neumannovo susjedstvo uključuje stanicu koju se promatra i njene ortogonalne susjede. S druge strane Mooreovo, susjedstvo uključuje ortogonalne susjede prisutne u von Neumannovom susjedstvu, ali također uključuje i četiri dijagonalna susjeda. Von Neumannovo susjedstvo čini pet stanica, a Mooreovo susjedstvo čini devet stanica. Stoga se primjenjuju ovisno o namjeni staničnog automata; ako su poželjni jednostavniji uzorci ponašanja, primjenjuje se von Neumannovo susjedstvo koje ima $2^5 = 32$ moguće konfiguracije u najjednostavnijem slučaju kad stanice mogu poprimiti dva moguća stanja. Suprotno tome, ako su poželjni složeniji uzorci ponašanja, primjenjuje se Mooreovo susjedstvo koje ima $2^9 = 512$ mogućih konfiguracija u istom slučaju (Bhattacharjee, 2019).

Berto i Tagliabue (2023) koriste sljedeću shemu za opisivanje staničnih automata prema njihovim parametrima:

a. Diskretan n-dimenzionalan stanični prostor, koji specificira izgled mreže stanica. Prema ovom parametru, stanični automat može biti jednodimenzionalan, dvodimenzionalan, heksagonski, itd.
b. Diskretna stanja, koja označavaju sva moguća stanja koja pojedina stanica može poprimiti, a predstavlja se u obliku konačnog skupa stanja koji označavamo velikim grčkim slovom sigma. Najosnovniji slučaj je onaj kada postoje dva moguća stanja koje stanica može poprimiti, što se označava kao: $\Sigma = \{0, 1\}$.
c. Lokalne interakcije, koje određuju koje susjedstvo automat koristi, odnosno topologiju automata.
d. Diskretne dinamike, koje ovise o lokalnim funkcijama koje se primjenjuju nad pojedinim stanicama prateći unaprijed definirana pravila. Koje pravilo, odnosno koja lokalna funkcija će se primijeniti nad tekućom stanicom ovisi o konfiguraciji njenog susjedstva.

Princip rada dvodimenzionalnih staničnih automata može se objasniti na primjeru koji je ujedno i najpoznatiji stanični automat: Conwayeva Igra života. Igra života je dvodimenzionalni stanični automat osmišljen kao simulacija umjetnog života, postavljen tako da stanični prostor predstavlja svijet u kojem se nalazi hipotetska populacija. Jedinke koje čine ovu populaciju predstavljene su preko stanica automata te mogu biti ili žive ili mrtve (Toffoli i Margolus, 1987).

Koristeći shemu koju su osmislili Berto i Tagliabue (2023), Igra života definira se kao:

a. Dvodimenzionalna mreža ortogonalno povezanih kvadrata.
b. $\Sigma = \{0, 1\}$, u sklopu čega je stanica sa stanjem 1 živa, a stanica sa stanjem 0 mrtva.
c. Koristi se Mooreovo susjedstvo.
d. Pravila prijelaza primjenjuju se prema tri moguća tipa konfiguracije:
    1. Ako je stanica mrtva, postaje živa ako ima točno tri živa susjeda;
    2. Ako je stanica živa, ostaje živa ako ima dva ili tri živa susjeda;
    3. Ako je stanica živa, postaje mrtva ako ima manje od dva ili više od tri živa susjeda.

Prateći biološki motiv, ova pravila se nazivaju rađanje, preživljavanje i umiranje. Stanica se rađa ako su prisutna tri živa susjeda koji se smatraju njenim roditeljima, umire od samoće ili prenaseljenosti, a preživljava u idealnim uvjetima. Conwayjeva igra života izvrstan je primjer staničnog automata jer slikovito dočarava glavnu misao staničnih automata: iz jednostavnih pravila proizlaze nevjerojatno složena ponašanja. Igra života uistinu je zasebno područje izučavanja, a imala je i velik utjecaj na različita područja, uključujući matematiku, računalnu znanost i filozofiju (Toffoli i Margolus, 1987). Navrh svega, igra života smatra se univerzalnim staničnim automatom jer je pokazala svojstvo emuliranja Turingovog stroja, kao i bilo kojeg sustava koji je izračunljiv Turingovom stroju, uključujući i brojne ostale stanične automate (Weisstein, 2024).

2.1 Blokovski stanični automati

Reverzibilni stanični automati su posebna vrsta staničnih automata čija je globalna funkcija bijektivna, a pritom i inverzna, što omogućuje da svaka konfiguracija automata ima točno jednu moguću prethodnu konfiguraciju. To svojstvo čini ovaj tip staničnog automata unazad determinističkim (Morita, 2018). Globalna funkcija odnosi na prijelaz stanja čitave generacije automata, a taj prijelaz se postiže primjenom lokalnih funkcija na svaku pojedinu stanicu, što znači da lokalne funkcije prijelaza moraju također biti bijektivne. Iz ovoga proizlazi kako je stanični automat globalno reverzibilan ako i samo ako je lokalno reverzibilan – za svaku konfiguraciju svakog susjedstva mora biti poznata prethodna konfiguracija tog susjedstva. Stoga se zaključuje kako pravila prijelaza moraju biti deterministička (Morita, 2018).

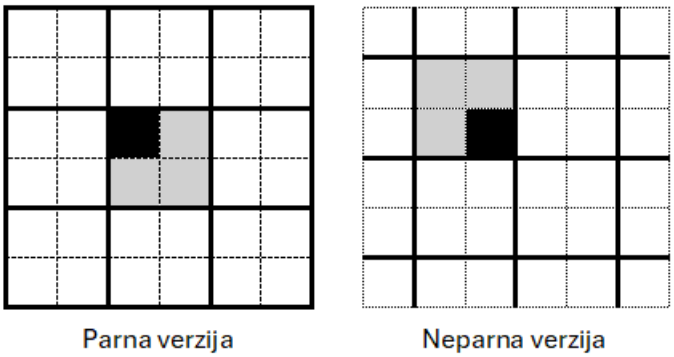
Problem uspostavljanja determinističkih pravila javlja se u tome što svaki mogući prijelaz stanja mora biti definiran bez mogućnosti izbora ili nasumičnosti. Na primjer, ako se koristi Mooreovo susjedstvo za osmišljavanje reverzibilnog staničnog automata, potrebno je odrediti sljedeću konfiguraciju za svaku moguću konfiguraciju susjedstva, što čini $2^9 = 512$ pravila prijelaza. Von Neumannovo susjedstvo bi sa svojih $2^5 = 32$ pravila prijelaza bilo jednostavnije, ali također nepraktično implementirati. Iz ovog razloga, osmišljeni su načini odjeljenja staničnog prostora koji omogućavaju manji broj permutacija susjedstva, ali bez žrtvovanja složenosti ponašanja samog automata.

Jedno od najčešćih rješenja ovog problema su blokovski ili odjeljivi stanični automati, čije ime proizlazi iz načina na koji se stanični prostor odjeljuje na zasebne blokove. Toffoli i Margolus (1987) opisuju jedan od najpoznatijih blokovskih staničnih automata:

1. Stanice u mrežnom prostoru odijeljene su skup konačnih, razdvojenih i uredno poredanih grupa koje se nazivaju blokovi. Za razliku od običnih susjedstva, jedan blok nema središnju stanicu.
2. Primjenjuje se blokovsko pravilo prijelaza koje uzima u obzir sadržaj jednog bloka i ažurira čitav blok odjednom, za razliku od pravila prijelaza u običnom staničnom automatu koja ažuriraju samo jednu stanicu.
3. Odjeljenje stanica se mijenja iz jednog vremenskog koraka u drugi kako bi se postiglo preklapanje blokova koje je vremenski razdvojeno.

Treća točka ovog automata je posebno važna: ako se koristi samo jedno odjeljenje za svaki korak staničnog automata, rezultat bi bio stanični automat koji se sastoji od manjih, međusobno neovisnih podsustava.

Najjednostavnija shema za odjeljivanje staničnog prostora je na blokove koji se sastoje od četiri stanice. Ovakva vrsta odjeljivanja naziva se Margolusovo susjedstvo i ima samo $2^4 = 16$ mogućih konfiguracija, što ujedno znači da se mora osmisliti samo 16 pravila prijelaza. Ova shema postiže vremenski razdvojeno preklapanje tako da koristi dvije verzije odjeljenja: parno i neparno odjeljenje. U parnom odjeljenju, granice između susjedstva se nalaze na parnim crtama staničnog prostora, dok se u neparnom odjeljenju granice nalaze na neparnim crtama staničnog prostora (Toffoli i Margolus, 1987).



Slika 2. Margolusovo susjedstvo, izvor: rad autora

Na slici 2 se vidi implementacija ovog susjedstva. Istaknuta stanica će se u parnim koracima nalaziti u jednoj verziji odjeljenja, a u neparnim koracima će se nalaziti u drugoj verziji odjeljenja. Ovime se izbjegava stvaranje neovisnih podsustava koji se ponavljaju svakih par koraka, pošto bi se neovisan blok koji nema vanjski utjecaj nalazio u jednoj mogućoj konfiguraciji iz koje bi prešao u sljedeću, jedinstvenu konfiguraciju iz koje bi se opet nakon određenih broja koraka vratio na početnu konfiguraciju zbog toga što blokovska pravila prijelaza moraju biti lokalno inverzna (Toffoli i Margolus, 1987).

2.2 Primjena staničnih automata

Stanični automati su izuzetno svestrani zbog svoje jednostavnosti, skalabilnosti i sposobnosti generiranja složenih ponašanja iz jednostavnih pravila. Njihova inherentna svojstva omogućuju modeliranje širokog spektra različitih sustava i fenomena, što ih čini vrijednim alatima u raznovrsnim područjima poput fizike, biologije, računalne znanosti te čak i umjetnosti. Sve ovo moguće je upravo zbog prilagodljivosti i fleksibilnosti pri osmišljavanju staničnih automata i njihove mogućnosti prilagođavanja konkretnom zadatku. Iz ovih razloga stanični automati služe kao lako razumljiv ispitni alat za složenije modele i često rješavaju problem u pitanju s dovoljnom preciznošću.

U prirodnim znanostima, stanični automati se koriste za simulaciju fizikalnih sustava kao što su na primjer dinamike tekućina, rast kristala i fazni prijelazi. U biologiji, stanični automati se koriste za modeliranje formiranja uzoraka u biološkim sustavima, poput razvoja pruga i točaka na životinjskim kožama ili obrazaca grananja kod biljaka. Također pomažu u razumijevanju dinamike populacija time da ilustriraju kako se populacije vrsta mijenjaju i međusobno djeluju tijekom vremena. U ekologiji, stanični automati modeliraju okolišne procese poput požara u šumama i erozije, što pomaže istraživačima da razumiju i ublaže učinke prirodnih katastrofa. Nadalje, stanični automati su ključni u modeliranju širenja bolesti, u sklopu čega pomažu epidemiolozima predvidjeti i kontrolirati izbijanja bolesti. Njihova sposobnost repliciranja složenih ponašanja fizičkih sustava čini ih neprocjenjivima za istraživače koji proučavaju ove fenomene (Chopard i Droz, 1998). Urbanističko planiranje je područje u kojem stanični automati imaju posebno velik utjecaj. Stanični automati se

koriste za simuliranje protoka prometa, što pomaže pri dizajniranju učinkovitije mreže prijevoza. Stanični automati se također koriste za modeliranje urbanističkog razvoja, što omogućava predviđanje kako će gradovi rasti i mijenjati se tijekom vremena te donošenje informiranih odluka o infrastrukturi i alokaciji resursa (Hadeler i Müller, 2018).

Stanični automati primjenjuju se i u raznim područjima informacijskih znanosti. Na primjer, Shao i sur. (2024) opisuju korištenje staničnih automata u kontekstu diseminacije informacija kako bi se modeliralo širenje informacija kroz mrežu povezanih stanica. Svaka stanica predstavlja pojedinca ili entitet unutar mreže i simuliranjem interakcije i dinamike između stanica pružaju se uvidi u proces diseminacije informacija, interpretacije poruka, utjecaj komunikacije na računalne mreže i predviđanje trendova u dinamici javnog mišljenja.

Stanični automati se također primjenjuju u obradi digitalnih slika, u sklopu čega se digitalna slika promatra kao stanični prostor automata, s pojedinim pikselima slike kao zasebne stanice automata. Jedan od načina koji primjenjuje ovakav pristup opisuju Yin i Hadjiloucas (2023). Oni predstavljaju tehniku uklanjanja šuma u digitalnim slikama koristeći stanične automate, uz održavanje važnih detalja poput rubova i tekstura slike. Njihova metoda sastoji se od dva koraka: prvo se identificiraju oštećeni pikseli putem procesa koji procjenjuje najmanju vrijednost među središnjim pikselima i srednju vrijednost susjednih piksela u Mooreovom susjedstvu; drugo se potvrđuje neoštećeni pikseli provjerom jesu li ostali netaknuti. U ovom koraku se mjere ekstremne vrijednosti aritmetičke sredine susjednih piksela kako bi se otkrio šum, s fokusom na područja gdje dolazi do značajnih promjena u intenzitetu. Osnovni princip algoritma temelji se na otkrivanju povećanih razlika između piksela kako bi se učinkovito identificirala prisutnost šuma.

3. Kriptografija

Etimologija naziva znanstvene discipline često ukazuje na njenu srž. Riječ kriptografija dolazi od grčkih riječi *kryptos*, što znači tajan ili skriven te *graphein*, što znači pisati. Prije doba tehnologije, kriptografija se uistinu i bavila tajnim pisanjem izučavajući postupke i načine na koje se informacije mogu zakriti koristeći neki dogovoreni sustav za zakrivanje. Međutim, s razvojem kanala kroz koje se informacije šalju i medija u kojima se pohranjuju, načini zaštite informacija pomoću zakrivanja morali su se prilagoditi računalnoj moći obrade podataka koja je presudila postojećim sustavima za zakrivanje i ubrzo ih učinila arhaičnim. Stoga je djelokrug kriptografije postao cjelokupno područje zakrivanja informacija u oblike koji su neovlaštenim osobama nemogući ili računalno neizvedivi za udvostručiti, poništiti ili raskriti (Simmons, 2023). S time je otežan posao definiranja kriptografije kao discipline te Banoth i Regar (2023) ističu tri moguće definicije. Prvo kriptografiju promatraju kao praksu korištenja matematičkih tehnika u svrhu zaštite podataka i ulijevanja povjerenja u elektroničke sustave. Kriptografiju također definiraju kao znanost ili umjetnost koja se bavi konceptima, tehnikama i postupcima za zakrivanje običnog teksta i raskrivanje zakrivenog teksta. Konačno, definiraju kriptografiju kao disciplinu koja obuhvaća principe, sredstva i metode za preoblikovanje podataka kako bi se zakrio njihov semantički sadržaj, spriječila njihova neovlaštena upotreba te spriječila njihova neprimjetna izmjena.

Osnovni principi kriptografije mogu se objasniti na teoretskom primjeru u kojem dvije osobe, pošiljatelj i primatelj, žele komunicirati preko komunikacijskog kanala koji je nesiguran te u kojem postoji mogućnost prisutnosti neke treća osobe koja ima pristup porukama koje se izmjenjuju kroz komunikacijski kanal. Stinson i Paterson (2018) ukupnu sekvencu izmijenjenih poruka između pošiljatelja i primatelja nazivaju protokolom. Sesija jednog takvog protokola između pošiljatelja i primatelj sastoji se od jednog ili više tokova, u sklopu čega tok podrazumijeva slanje poruke od samog izvora kroz komunikacijski kanal do njenog odredišta. Zbog nesigurnosti komunikacijskog kanala i opasnosti od prisluškivača, poruke koje se izmjenjuju moraju se zaštiti. Jedan od mogućih pristupa zaštiti je kriptografski. U takvom pristupu, pošiljatelj svoju poruku zaštićuje koristeći kritopisni sustav u kojem se unaprijed dogovoreni ključ primjenjuje nad kriptografskom algoritmu koji otvoreni tekst pretvara u zakriveni oblik. Pritom, ako se mogući prisluškivač komunikacijskog kanala domogne poruka koje se razmjenjuju,

imat će njihov zakriveni oblik iz kojeg ne može odrediti otvoreni tekst. Međutim, primatelj kojem je poruka namijenjena zna ključ kojem se poruka zakrila, što mu omogućuje raskrivanje zakrivenog teksta u njegov otvoreni oblik (Dujella i Maretić, 2007).

U samom procesu zakrivanja i raskrivanja u jednom takvom sustavu koristi se kriptografski ili zakrivni algoritam koji uključuje dvije matematičke funkcije – jednu za zakrivanje i drugu za raskrivanje. Ove funkcije određuju postupak iz kojeg se otvoreni tekst zakriva, odnosno zakriveni tekst raskriva (Dujella i Maretić, 2007).

Banoth i Regar (2023) detaljnije definiraju elemente sustava za zakrivanje, odnosno kritopisnog sustava:

- Jasnopis (engl. plaintext) još se naziva i otvoreni tekst, a označuje semantički smislenu poruku u izvornom obliku koju pošiljatelj šalje primaocu.
- Zakritak (engl. ciphertext) još se naziva i šifrat ili kriptogram, a označuje rezultat primjene zakrivnih algoritama nad jasnopisom. Odnosno, radi se o promijenjenom obliku jasnopisa koji je semantički nepojmljiv.
- Zakrivanje (engl. encryption) još se naziva i šifriranje, a označuje postupak kojim se jasnopis pretvara u zakritak.
- Raskrivanje (engl. decryption) još se naziva i dešifriranje, a označuje postupak kojim se iz zakritka uspostavlja jasnopis.
- Ključ (engl. key) je proizvoljan dio kritopisnog sustava koji se primjenjuje nad zakrivnim algoritmom. Ova proizvoljnost ostvaruje raznolikost kritopisnog sustava i utvrđuje njegovu sigurnost time čak u situacijama gdje je zakrivni algoritam poznat, pošto sam ključ određuje kako će se poruka zakriti.

Prema Dujella i Maretić (2007), kritopisni sustav se formalno definira kao uređena petorka (P, C, K, E, D) za koju vrijede sljedeća svojstva:

1. P je konačan skup svih mogućih osnovnih elemenata jasnopisa;
2. C je konačan skup svih mogućih osnovnih elemenata zakritka;
3. K je prostor ključeva, konačan skup svih mogućih ključeva;
4. Za svaki $K \in K$ postoji funkcija šifriranja $eK \in E$ i odgovarajuća funkcija dešifriranja $dK \in D$. Pritom su $eK : P \rightarrow C$ i $dK : C \rightarrow P$ funkcije sa svojstvom da je $dK(eK(x)) = x$ za svaki jasnopis $x \in P$.

Najvažnije svojstvo u ovoj formalnoj definiciji jest četvrto svojstvo. Iz njega se zaključuje da ako se jasnopis zakrije koristeći funkciju zakrivanja i dobiveni zakritak raskrije koristeći funkciju raskrivanja, ponovno će se dobiti izvorni jasnopis. Iz ovoga slijedi da su sve funkcije zakrivanja bijektivne funkcije, pošto se u suprotnom postupak raskrivanja ne može obaviti na nedvosmislen način (Stinson i Paterson, 2018).

Dujella i Maretić (2007) klasificiraju kritopisne sustave prema sljedećim kriterijima:

- Tip operacija koje se koriste pri zakrivanju, prema kojem se razlikuju zamjenski i premještajni kritopisni sustavi te složeni kritopisni sustavi koji kombiniraju oba.
- Način na koji se obrađuje jasnopis, prema kojem se razlikuju blokovski i protočni kritopisni sustavi.
- Tajnost i javnost ključeva, prema kojem se razlikuju simetrični kritopisni sustavi i kritopisni sustavi s javnim ključem.

Zamjenski kritopisni sustavi još se nazivaju i supstitucijski sustavi a karakterizira ih svojstvo da se svako slovo abecede zamjenjuje s nekim drugim slovom ili u sofisticiranijim sustavima s nekim drugim znakom, brojem, simbolom, kombinacijom znakova, riječima i tako dalje. Najpoznatiji i jedan od najjednostavnijih kritopisnih sustava je Cezarov kritopisni sustav, zamjenski sustav koji svako slovo jasnopisa zamjenjuje odgovarajućim slovom zakritne abecede čija su slova pomaknuta za dogovoreni broj mjesta. Na primjer, ako se radi o pomaku za tri mjesta, slovo A će se zamijeniti slovom Č, slovo B sa slovom Ć i tako dalje. Ovakvi jednostavniji zamjenski sustavi koji se služe jednom zakritnom abecedom nazivaju se monoalfabetski sustavi, za razliku od složenijih polialfabetskih sustava koji koriste više zakritnih abeceda, odnosno slovoreda. Jedan takav primjer je Vigenereov kritopisni sustav koji koristi onoliko zakritnih slovoreda koliko je slova u abecedi, a svaki zakritni slovored nastao je pomakom kao i u Cezarovom sustavu (Klima i Sigmon, 2018).

Premještajni kritopisni sustavi razlikuju se od zamjenskih time da se slova jasnopisa ne zakrivaju zamjenom drugim slovima, već se zakrivaju razmjenom poretka slova prema dogovorenim pravilima. Primjer takvog sustava jest stupačni kritopisni sustav u sklopu kojeg se jasnopis dijeli po stupcima koji se ispisuju određeno po dogovorenom ključu. Rezultat je zakritak koji se sastoji od slova jasnopisa čiji je redoslijed slova promijenjen dovoljno da poruka bude nejasna (Klima i Sigmon, 2018).

Zamjenski i premještajni kritopisni sustavi nisu međusobno isključivi, već se primjenom oba ostvaruje dodatan sloj zaštite u kritopisnim sustavu, a takvi sustavi koji se sastoje i od zamjene i od premještanja elemenata jasnopisa nazivaju se složeni kritopisni sustavi (Klima i Sigmon, 2018).

Protočni kritopisni sustavi zakrivaju elemente jasnopisa jedan po jedan. Tehnički su svi monoalfabetski i polialfabetski zamjenski sustavi ujedno i protočni kritopisni sustavi, ali izraz protočni kritopisni sustavi uglavnom se koristi za kritopisne sustave u kojima su elementi jasnopisa izraženi u bitovima koji se zakrivaju jedan po jedan koristeći također binaran ključ koristeći najčešće operaciju zbrajanja bez prijenosa, odnosno isključivo ili (Klima i Sigmon, 2018).

Za razliku od protočnih, blokovski kritopisni sustavi zakrivaju elemente jasnopisa u blokovima ili grupama, a ne jedan po jedan element. Jednostavan primjer toga su stupačni kritopisni sustavi, pošto se u njima elementi jasnopisa obrađuju u grupama, odnosno stupac po stupac. Međutim, takvi jednostavni kritopisni sustavi često se ne podrazumijevaju kada se spominju blokovski kritopisni sustavi. Blokovski kritopisni sustavi najčešće se vežu uz moderne, naprednije kritopisne sustave koji poput protočnih sustava također izražavaju elemente jasnopisa u bitovima i čiji blokovi čine definiran broj bitova. Primjer toga su jedni od najpoznatijih modernih standarda za zakrivanje, DES i njegova unaprijeđena zamjena AES, odnosno *Data Encryption Standard* i *Advanced Encryption Standard* (Klima i Sigmon, 2018).

Konačno, prema tajnosti i javnosti ključa imamo simetrične kritopisne sustave. Kod simetričnih kritopisnih sustava, ključ za zakrivanje je najčešće identičan ključu za raskrivanje, to jest koristi se jedan te isti ključ. Sigurnost ovakvog kritopisnog sustava leži u tajnosti ključa, što je ujedno i najveći nedostatak ovakvih sustava. Naime, pošiljatelj i primatelj moraju unaprijed dogovoriti ključ koji će koristiti, što stvara dodatnu razinu opasnosti od potencijalnog prisluškivača. Jedini način kojim bi se pouzdano osigurala sigurnost simetričnog sustava bi bio razmjenom ključa preko sigurnog komunikacijskog kanala. Međutim, sama dostupnost osiguranog komunikacijskog kanala čini samo zakrivanje poruka bespotrebnim (Dujella i Maretić, 2007).

Kako bi se izbjegao problem razmjene ključa, osmišljen je kritopisni sustav s javnim ključem. Kritopisni sustav s javnim ključem još se naziva i asimetričnim kritopisnim

sustavom jer primjenjuje dva različita ključa, jedan za zakrivanje i drugi za raskrivanje. U ovakvom sustavu, pošiljatelj koristi javno dostupan ključ primaoca za zakrivanje jasnopisa te zatim primatelj primjenjuje svoj tajni ključ za raskrivanje nad dobivenim zakritkom. U ovom slučaju funkcija zakrivanja smatra se jednosmjernom pošto ju je lako izračunati, dok je njenu inverziju teško izračunati (Dujella i Maretić, 2007).

3.1 Primjena staničnih automata u kriptografiji

Prema Dujella i Maretić (2007), kriptografija se u današnjoj praksi javlja u obliku razvoja jednosmjernih funkcija zakrivanja, generiranju nasumičnih brojeva, uspostavljanju digitalnih potpisa, utvrđivanju identiteta i slično. Zbog svoje nepredvidljivosti i složenog ponašanja unatoč jednostavne implementacije, nije iznenađujuće kako su stanični automati značajan alat u području kriptografije. Stanični automati pronašli su se u svim aspektima procesa zakrivanja – od samih zakrivnih funkcija, kroz čitave kritopisne sustave, do generiranja sigurnih ključeva. Osobine staničnih automata koje su posebno poželjne kriptografima su baratanje lokalnim informacijama, decentralizirano upravljanje i mogućnost univerzalne izračunljivosti (Stănică i Anghelescu, 2023).

Stanični automati mogu se koristiti pri izradi funkcija za zakrivanje, prilikom čega se prema jednostavnim pravilima podaci zakrivaju na nepredvidiv i teško obrazloživ način. Ovime se stvara funkcija koju je lako izračunati za svaki unos, ali teško ili nemoguće izračunati njenu inverziju, odnosno funkciju za raskrivanje. Ovakav tip funkcije naziva se jednosmjerna funkcija, koje su često primijenjene u skladištenju podataka za poslove kao što je primjerice provjera lozinka korisnika pri prijavi u neki sustav, pri čemu su lozinke spremljene u zakrivnom obliku koristeći jednosmjernu funkciju, a prilikom prijave u sustav unesena se lozinka zakriva koristeći istu jednosmjernu funkciju i podudaranjem zakritka potvrđuje se točnost lozinke (Wu i Chang, 2023).

Moderna kriptografija uvijek mora uzimati u obzir snagu računala i brzinu kojom se algoritmi mogu izvršiti te su stoga nasumično generirani ključevi vrlo poželjni zbog svoje nepredvidljivosti, ali pronalaženje dobrih generatora nasumičnih brojeva je težak posao pošto sve praktične metode za generiranje nasumičnih brojeva koriste deterministčke algoritme, zbog čega se brojevi generirani takvim metodama nazivaju pseudo-nasumični brojevi. Iz ovih razloga je ključan odabir kvalitetnog algoritma koji

će proći razna ispitivanja nasumičnosti, za što se znaju koristiti principi rada staničnih automata zbog svojih nepredvidivih ishoda (Levina i sur., 2022).

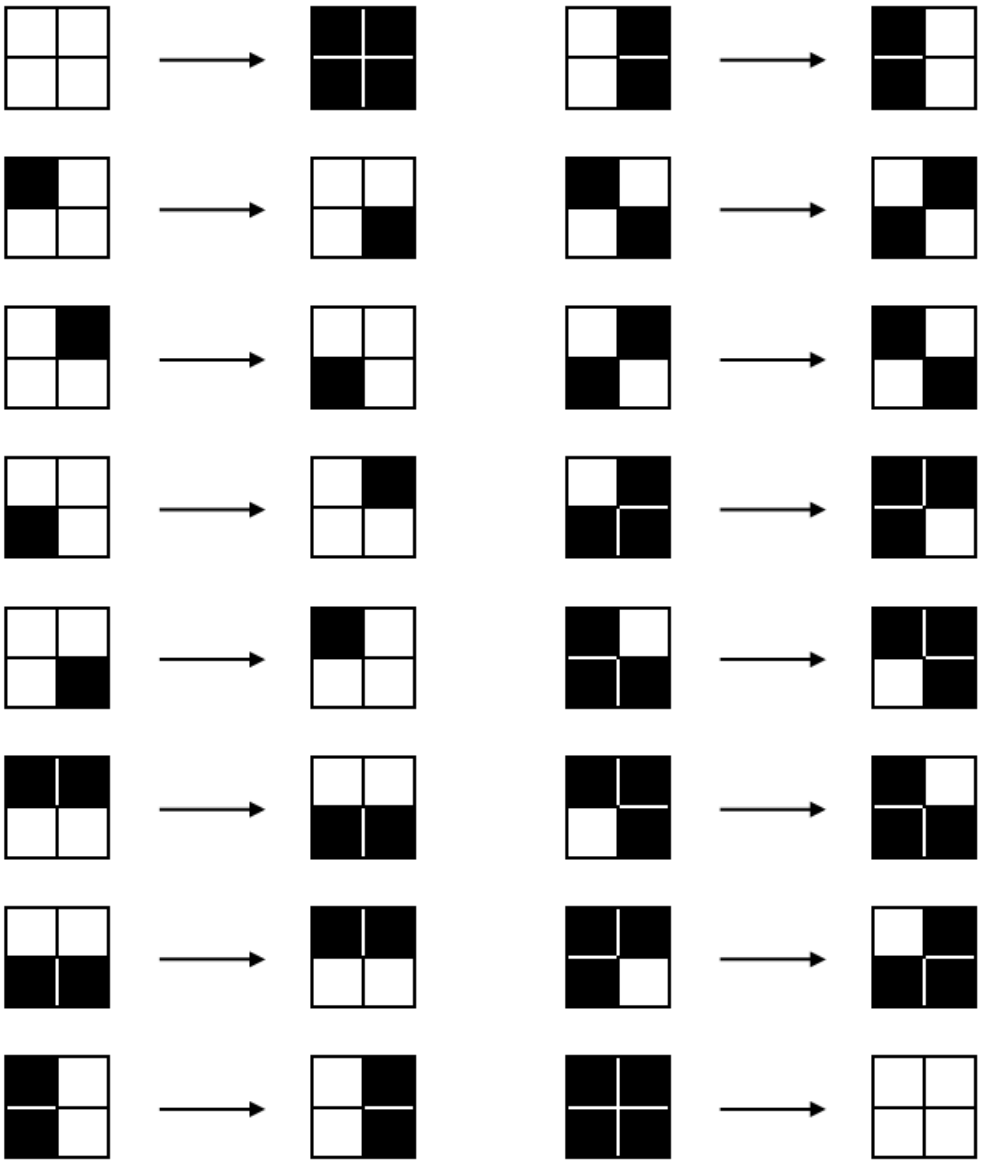
Zbog primjenjivosti u obradi digitalnih slika, stanični automati često se koriste i u kriptografiji digitalnih slika. Abusham i sur. (2023) opisuju kako se stanični automati mogu osmisliti da koriste digitalnu sliku kao stanični prostor u kojoj svaki piksel čini jednu stanicu, pri čemu se ovisno o susjednim pikselima svaki pojedini piksel zakriva koristeći razne metode. Primjeri koje navode u svom radu uključuju korištenje staničnih automata kao premetala, kao i primjena XOR logičkog operatora – operacije zbrajanja bez prijenosa, koja se još naziva i isključno ili, a primjenjuje se u kriptografiji zbog svoje karakteristike ujednačenosti – koja je uvjetovana pravilima nalik principu rada staničnih automata. Abusham i sur. (2023) koriste ove tehnike uz algoritam prepoznavanja lica kako bi zaštitili identitet osoba u sustavu za prepoznavanje lica. S druge strane, Moya-Albor i sur. (2023) osmislili su tehniku zakrivanja slika temeljenu na principu rada staničnih automata koja zakrivenu sliku čini otpornom na statističku analizu zbog tendencije premetala prema što većoj entropiji.

4. Razvoj kritopisnih sustava

Ovaj rad bavi se primjenom staničnih automata u razvoju kritopisnih sustava. Namjera rada jest prikazati principe rada staničnih automata koristeći ih kao inspiraciju za zakrivne algoritme u klasičnim kritopisnim sustavima. Poruku koja se zakriva može se posložiti u prostoru tako da svaki element poruke zauzima jedno polje u mreži, odnosno nalazi se u stanici u dvodimenzionalnom staničnom polju automata. Ta slova u stanicama predstavljaju tekuće stanje stanice koje se mijenja ovisno o proizvoljnim pravilima prijelaza stanja, a ta promjena može podrazumijevati zamjenu, premještanje ili kombinaciju oba postupka. Kako slovo predstavlja stanje stanice, teoretski bi ovakav stanični automat mogao imati trideset mogućih stanja u skladu s trideset slova hrvatske abecede, što uvodi nepotrebne komplikacije. Stoga se broj mogućih stanja svodi na dva, 1 i 0, pošto cilj rada nije osmisliti elaborativan kritopisni sustav, već dočarati mogućnost primjene staničnih automata. Binarnost mogućih stanja ostvaruje se na najjednostavniji mogući način: parna slova u abecedi su 1, a neparna slova su 0.

Važan aspekt klasične kriptografije jest mogućnost raskrivanja poruke. Klasična kriptografija bavi se zaštitom prijenosa poruka tako da pošiljatelj zakriva jasnopis na način da je ona semantički nepojmljiva. U svrhu uspješne komunikacije, podrazumijeva se da će primatelj moći raskriti zakritak kako bi došao do izvornog oblika poruke. Za poruku koja je zakrivena koristeći princip rada staničnih automata, to znači da primatelj mora imati sposobnost iz završne konfiguracije automata dobiti prethodnu konfiguraciju kako bi korak po korak došao do izvorne konfiguracije. Ova sposobnost prisutna je jedino u reverzibilnim staničnim automatima. Stoga je za svrhu zakrivanja poruka najprikladnije koristiti najpoznatiji tip reverzibilnog staničnog automata: blokovski stanični automat s Margolusovim susjedstvom.

Osim navedenog, bitno je definirati pravilo prijelaza za svaku od 16 mogućih konfiguracija jednog susjedstva, kako bi svako pravilo bilo determinističko i čime bi se postigla reverzibilnost.



Slika 3. Pravila prijelaza blokovskog staničnog automata,
izvor: rad autora

Slika 3 ilustrira pravila prijelaza koje će ovaj stanični automat primjenjivati. Stupci s lijeve strane strelice prikazuju sve moguće konfiguracije susjedstva od kojih se promatra ona koja se podudara s konfiguracijom tekućeg susjedstva. Strelica se po uzoru na pravila produkcije u teoriji automata čita kao „daje“ ili „prelazi u“ i pokazuje na konfiguraciju u koju će tekuće susjedstvo prijeći u sljedećem koraku automata. Ključno svojstvo ovih pravila je bijektivnost između funkcija skupa tekućih konfiguracija i skupa sljedećih konfiguracija, za osiguranje reverzibilnosti. Nije nužno osmisliti

pravila prijelaza kao 8 inverznih parova pravila, ali to je najjednostavniji pristup postizanju lokalne inverzije (Toffoli i Margolus, 1987). Vrijedi spomenuti kako je stavljen poseban naglasak na to da se u svakom pravilu održava omjer stanja 0 i stanja 1, izuzev prvog i zadnjeg pravila koja prelaze iz svih nula u sve jedinice i obratno.

S ovim zaključcima može se koristeći shemu koju su osmislili Berto i Tagliabue (2023) definirati stanični automat koji će se koristiti kao inspiracija za razvoj kritopisnih sustava:

a. Dvodimenzionalna mreža ortogonalno povezanih kvadrata.
b. Σ = {0, 1}, u sklopu čega stanica sa stanjem 1 sadrži parno slovo abecede, a stanica sa stanjem 0 sadrži neparno slovo abecede.
c. Koristi se Margolusovo susjedstvo.
d. Šesnaest deterministčkih pravila prijelaza konfiguracije susjedstva glase:
    1. (0, 0, 0, 0) prelazi u (1, 1, 1, 1),
    2. (1, 0, 0, 0) prelazi u (0, 0, 0, 1),
    3. (0, 1, 0, 0) prelazi u (0, 0, 1, 0),
    4. (0, 0, 1, 0) prelazi u (0, 1, 0, 0),
    5. (0, 0, 0, 1) prelazi u (1, 0, 0, 0),
    6. (1, 1, 0, 0) prelazi u (0, 0, 1, 1),
    7. (0, 0, 1, 1) prelazi u (1, 1, 0, 0),
    8. (1, 0, 1, 0) prelazi u (0, 1, 0, 1),
    9. (0, 1, 0, 1) prelazi u (1, 0, 1, 0),
    10. (1, 0, 0, 1) prelazi u (0, 1, 1, 0),
    11. (0, 1, 1, 0) prelazi u (1, 0, 0, 1),
    12. (0, 1, 1, 1) prelazi u (1, 1, 1, 0),
    13. (1, 0, 1, 1) prelazi u (1, 1, 0, 1),
    14. (1, 1, 0, 1) prelazi u (1, 0, 1, 1),
    15. (1, 1, 1, 0) prelazi u (0, 1, 1, 1),
    16. (1, 1, 1, 1) prelazi u (0, 0, 0, 0).

Kao što se može primijetiti u četvrtoj točki gornje definicije, konfiguracije susjedstva su prikazane u obliku (0, 0, 0, 0), u sklopu čega se prva znamenka odnosi na gornje-lijevu stanicu, druga na gornje-desnu stanicu, treća na donje-lijevu stanicu i četvrta na donje-desnu stanicu. U nastavku rada će se sukladno za položaj stanica u susjedstvu koristiti

nazivi prva stanica, druga stanica, treća stanica i četvrta stanica u odnosu na ovdje uspostavljen redoslijed.

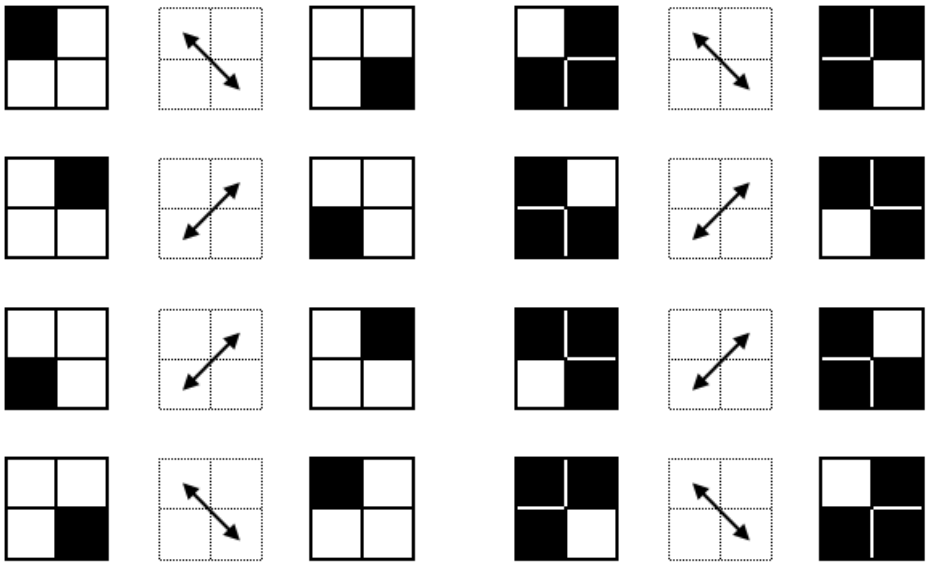
Nastavak rada bavit će se realizacijom ovih pravila putem metoda klasične kriptografije – zamjenom, premještanjem te kombinacijom obje – kako bi se osmislili zamjenski, premještajni i složeni kritopisni sustavi koji zamjenjuju i/ili premještaju elemente poruke na način nalik radu staničnog automata.

4.1 Premještajni kritopisni sustav

Većina literature koja se bavi klasičnim kritopisnim sustavima prvo predstavlja zamjenski kritopisni sustav, a zatim premještajni. Međutim, ovaj rad prvo će opisati premještajni kritopisni sustav. Razlog tome su pravila prijelaza koja su osmišljena tako da vizualno kroz vrijeme daju dojam da se stanice kreću, odnosno premještaju kroz stanični prostor. Ta osobina čini premještajni kritopisni sustav jednostavnijim za implementaciju od zamjenskog kritopisnog sustava te intuitivnijim za shvaćanje principa rada ovih kritopisnih sustava.

Klasični premještajni kritopisni sustavi uključuju premještanje jednog ili više elemenata poruke na neku drugu poziciju (Dujella i Maretić, 2007). Cilj ovog kritopisnog sustava je realizirati pravila prijelaza koristeći metodu premještanja: potrebno je premještanjem elemenata ostvariti prijelaz jednog susjedstva iz tekuće konfiguracije u sljedeću sukladno uspostavljenim pravilima. Potrebno je napomenuti kako se u stvarnom staničnom automatu ne bi doslovno premještale stanice kroz prostor, već bi se samo mijenjala njihova stanja. Međutim, kako se govori o klasičnom kritopisnim sustavu, doslovno premještanje elemenata poruke je dozvoljeno i ono se događa prema parnosti slova čitave poruke po uzoru na ponašanje definiranog staničnog automata.

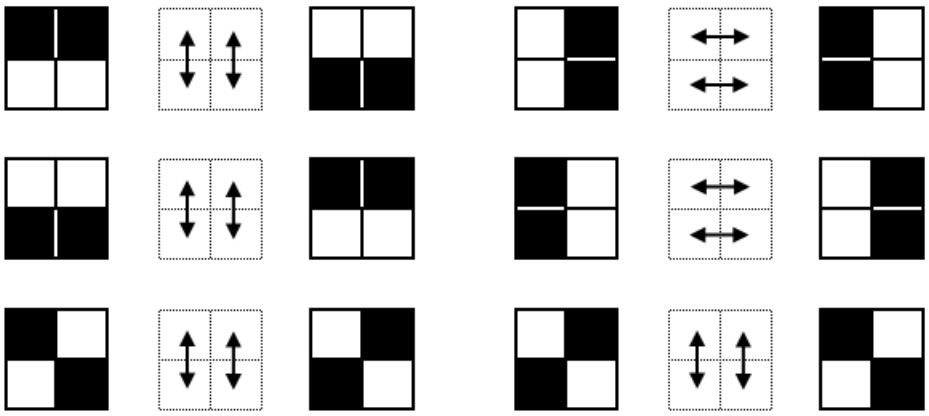
Najjednostavniji slučaj koji se može dogoditi putem premještanja je zamjena dvaju elemenata unutar susjedstva. Ovo je moguće jedino u konfiguracijama gdje je vizualno vidljiv pomak samo jedne stanice, a to su konfiguracije sa samo jednom stanicom u stanju 1 te konfiguracije sa samo jednom stanicom u stanju 0.



Slika 4. Prvi skup pravila premještanja, izvor: rad autora

Slika 4 prikazuje kako se premještanjem ostvaruju pravila prijelaza u tim konfiguracijama. Stanica koja se izdvaja premješta se na mjesto stanice u dijagonalnom odnosu, a ta dijagonalna stanica premješta se na oslobođeno mjesto. Za primjer se može uzeti susjedstvo (B, A, C, E). U tom slučaju je samo slovo B parno i zamijenit će položaje sa slovom u dijagonalnom odnosu, u ovom slučaju sa slovom E, što znači da konfiguracija (B, A, C, E) u sljedećem koraku prelazi u (E, A, C, B).

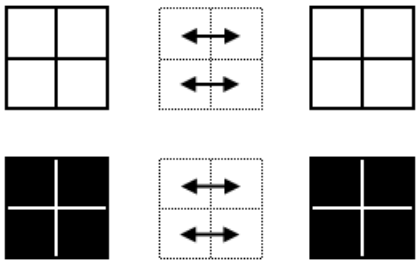
Konfiguracije u kojima je omjer stanja 0 i stanja 1 dva naprema dva uvode dodatnu razinu premještanja, pošto se treba zamijeniti mjesta dva para stanica. Drugim riječima, potrebno je premjestiti sva slova u jednom susjedstvu kako bi se ostvarili potrebni prijelazi.



Slika 5. Drugi skup pravila premještanja, izvor: rad autora

Prvih četiri slučaja su jednostavna i ostvaruju se zamjenom gornjih i donjih, odnosno lijevih i desnih „strana“ susjedstva kako je prikazano na slici 5. Međutim, zadnja dva slučaja u kojima se stanice istovrsnih stanja nalaze u dijagonalnim položajima su problematičnija, pošto se prijelaz konfiguracija može postići na dva jednakovrijedna načina. Potrebno je kao i u prvih četiri slučaja obje stanice sa stanjem 1 zamijeniti stanicama sa stanjem 0,a to je moguće ostvariti paralelnim vodoravnim ili paralelnim okomitim zamjenama tih stanica. Oba pristupa su valjana, a za ovaj sustav odabrana je paralelna okomita zamjena u kojoj se prva stanica zamjenjuje s trećom, a druga stanica se zamjenjuje s četvrtom.

Zadnje dvije moguće konfiguracije u kojima se susjedstva mogu pronaći su svi neparni brojevi i svi parni brojevi. U ovim slučajevima je premještanjem nemoguće promijeniti konfiguraciju susjedstva pošto se premještanjem ne mijenja vrijednost slova te će u svakoj permutaciji susjedstvo i dalje činiti istovrsna slova, odnosno sve stanice stanja 0 ili sve stanice stanja 1. Stoga prvo i zadnje pravilo definiranog staničnog automata ne vrijede za premještajni sustav. Međutim, kako bi se izbjegla stagnacija ovakvih susjedstva, i dalje će se članovi premještati.



Slika 6. Treći skup pravila premještanja,
izvor: rad autora

Na slici 6 se može primijetiti kako su odabrane dvije paralelne vodoravne zamjene između prve i druge te treće i četvrte stanice. Ova odluka je donesena kako bi se postigla ujednačenost svih šesnaest slučajeva. Ovime se ostvaruje ravnomjernost premještanja na svim razinama. U najvećoj razini, u polovici slučajeva prisutno je premještanje dvaju slova, a u drugoj polovici prisutno je premještanje svih četiri slova. Daljnjim promatranjem može se uočiti i kako su same polovice ujednačene. U osam slučajeva u kojima se premještaju dva slova, četiri od njih zamjenjuju mjesta prvog i četvrtog slova, a drugih četiri zamjenjuju mjesta drugog i trećeg slova. U osam slučaja

u kojima se premještaju sva četiri slova, četiri od njih zamjenjuju mjesta prvog i trećeg te drugog i četvrtog slova, a ovom odlukom preostalih četiri zamjenjuju mjesta prvog i drugog te trećeg i četvrtog slova.

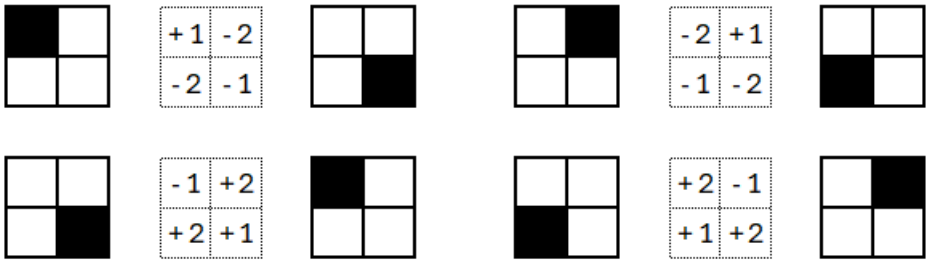
4.2 Zamjenski kritopisni sustav

Zamjena se pokazala dosta složenijom metodom pri osmišljanju kritopisnih sustava temeljenih na radu blokovskog staničnog automata. Razlog tome jest što unatoč ograničenosti bloka od samo četiri prisutnih slova, svako slovo može se zamijeniti s potencijalno bilo čime. U klasičnoj kriptografiji, jedno slovo može se zamijeniti drugim slovom, brojem, simbolom, a čak i čitavim riječima (Dujella i Maretić, 2007). Iz praktičnih razloga je kao način zamjene izabran jedan od najjednostavnijih pristupa zamjeni: Cezarov kritopisni sustav. Konkretnije, preuzeta je tehnika pomaka slova za određen broj mjesta u abecedi. Cezarov kritopisni sustav je sam po sebi dosta nesiguran, ali može se uključiti u neki složeniji kritopisni sustav kao korak pri zakrivanju, kao što je slučaj u Vigenereovom kritopisnim sustavu (Klima i Sigmon, 2018).

Koristeći pomake mjesta u abecedi kao metodu zamjene, promjena parnosti slova je izrazito laka. Ako se želi promijeniti parnost nekog slova, dovoljno ga je pomaknuti za neparan broj mjesta. Na primjer: ako se slovo A koje se nalazi na neparnom prvom mjestu hrvatske abecede pomakne za pet mjesta udesno, dobit će se slovo D na parnom šestom mjestu abecede. Suprotno tome, ako se ne želi promijeniti parnost slova ali ga se želi pomaknuti, može se pomaknuti za paran broj mjesta i parnost će ostati ista. Ovo je analogno množenju s jedan u matematici – dogodila se promjena, ali je vrijednost ostala ista – pošto pravila prijelaza gledaju samo parnost slova koja se nije promijenila. Ovaj zamjenski sustav iskorištava to svojstvo i u svakom pravilu pomiče slovo svake stanice u susjedstvu kako neka slova ne bi slučajno ostala nepomaknuta. Ključno je pritom ne poremetiti svojstvo reverzibilnosti pri definiranju pravila – pomaci u inverznim parovima pravila moraju imati inverzne vrijednosti kako bi se inverzijom postupka opet došlo do izvornog položaja slova.

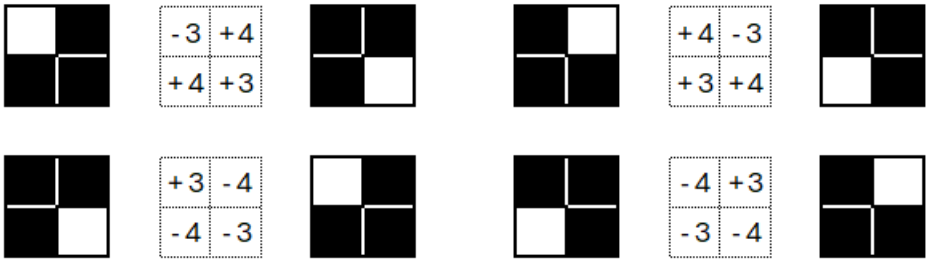
Prva iteracija ovih pravila se sastojala od najjednostavnijih mogućih opcija: ako se želi promijeniti parnost će se slovo pomaknuti za jedno mjesto, a ako se ne želi promijeniti parnost će se slovo pomaknuti za dva mjesta. Ovo se pokazalo kao loša praksa, pošto se nakon nekoliko generacija moglo primijetiti kako je većina slova pomaknuta za vrlo

mali broj mjesta, a dosta slova su čak imala svoju početnu vrijednost. Razlog tome je ujednačenost pravila: ako sva pravila imaju jednake pomake od jedan ili dva, stanica će se uvijek pomaknuti za jedno ili dva mjesta unaprijed ili unazad, a ujednačenost ovih pravila znači da se većina slova neće pomaknuti daleko od početnog položaja u abecedi. Stoga se zaključuje kako valja primijeniti različite pomake za različita pravila. Najbolja nepredvidljivost bi podrazumijevala različite vrijednosti pomaka za svaki par inverznih pravila, no to bi negativno utjecalo na praktičnost samog sustava i činilo ga nepotrebno višeslojnim i kompliciranim. Za lakše i intuitivnije razumijevanje, pravila se grupiraju u skupine.



Slika 7. Prvi skup pravila zamjene, izvor: rad autora

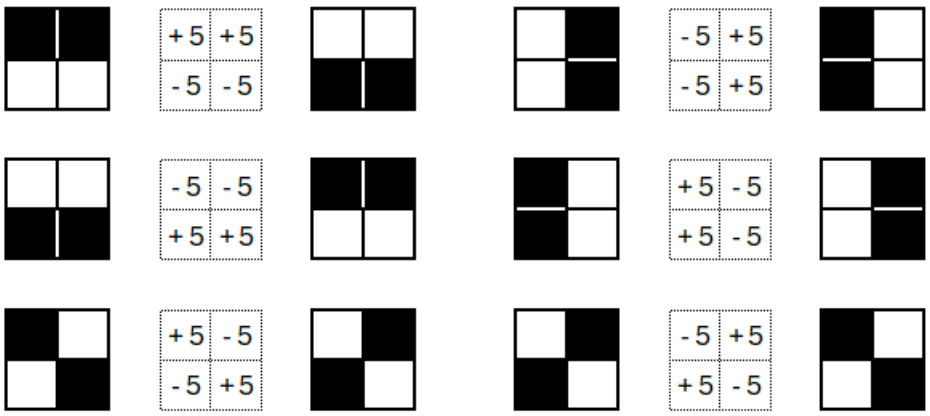
Slika 7 prikazuje konfiguracije s jednim parnim slovom. U ovom slučaju potrebno je parno slovo pomaknuti za neparan broj mjesta, a slovo u dijagonalnom odnosu također se treba pomaknuti za neparan broj mjesta, dok se preostala dva slova ortogonalna parnom slovu pomiču za paran broj mjesta. Vrijednosti koje su uzete za ovaj skup pravila su jedan za neparan pomak i dva za paran pomak, zato jer se u susjedstvu nalazi jedno parno slovo. Hoće li se slova pomaknuti unaprijed ili unazad određuje položaj parnog slova: ako se parno slovo nalazi u gornjem dijelu susjedstva, slova čija se parnost ne mijenja će se pomaknuti za dva mjesta unazad, a ako se parno slovo nalazi u donjem dijelu susjedstva, slova čija se parnost ne mijenja će se pomaknuti za dva mjesta unaprijed. Parno slovo uvijek će se pomaknuti unaprijed, a neparno slovo u dijagonalnom položaju uvijek će se pomaknuti unazad.



Slika 8. Drugi skup pravila zamjene, izvor: rad autora

Konfiguracije s jednim neparnim slovom koje prikazuje slika 8 je sličan konfiguracijama s jednim parnim slovom, pošto u oba slučaja samo jedno slovo odstupa. Stoga je primijenjen isti princip pomaka kao i u prethodnom slučaju, a za neparnu i parnu vrijednost pomaka uzeti su brojevi tri i četiri, pošto se u susjedstvu nalaze tri parna slova. Za vrijednosti pomaka slova čije se parnosti ne mijenjaju, opet se promatra položaj parnog slova koji je u dijagonalnom odnosu na neparno slovo: ako se nalazi u donjem dijelu susjedstva, „sporedna“ slova se pomiču unaprijed za četiri mjesta, a ako se nalazi u gornjem dijelu susjedstva, pomiču se unazad za četiri mjesta.

Konfiguracije koje imaju dva parna slova i dva neparna su drugačije od prethodnih, pošto se mijenja parnost svakog slova u susjedstvu. To znači da se za broj pomaka može odabrati isti neparan broj.

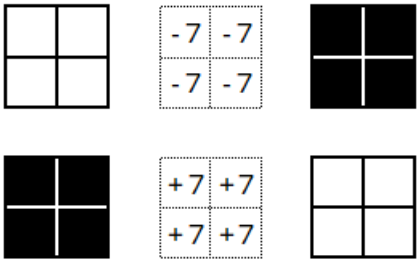


Slika 9. Treći skup pravila zamjene, izvor: rad autora

Na slici 9 vide se sve moguće konfiguracije s jednakim omjerom parnih i neparnih slova. Kao broj pomaka uzet je broj pet, pošto prethodna pravila primjenjuju pomake od jedan do četiri. Hoće li se slovo pomaknuti unaprijed ili unazad vrlo se lako određuje: ako je slovo parno, pomiče se unaprijed, a ako je slovo neparno, pomiče se unazad.

U konfiguracijama sa svim istovrsnim slovima, odnosno svim parnim ili svim neparnim slovima, dolazi se do značajnog problema. Za razliku od premještajnog sustava kojim se primjenom istog pravila dvaput bez promjene parnih odnosa u konfiguraciji dobije izvorna vrijednost slova jer se opet premještaju ista slova, zamjenom to nije moguće. Razlog tome jest što se pomak odvija za svako slovo u jednom smjeru, što znači da primjenom istog pravila dvaput bez promjene parnih odnosa u konfiguraciji označava

dvostruki pomak, a ne vraćanje na izvorne vrijednosti. Ovime bi se narušilo svojstvo reverzibilnosti i poništila mogućnost raskrivanja. Stoga prvo i zadnje pravilo definiranog staničnog automata glasi kako (0, 0, 0, 0) prelazi u (1, 1, 1, 1), a (1, 1, 1, 1) prelazi u (0, 0, 0, 0).



Slika 10. Četvrti skup pravila zamjene,
izvor: rad autora

Na slici 10 se može primijetiti taj prijelaz. Kako se mijenja parnost svih slova, potrebno je pomaknuti sva slova za neparan broj, a kao taj broj je uzet sljedeći dostupan neparan broj nakon pet: sedam. Ovim putem je ostvarena lokalna reverzibilnost, pošto će se sva parna slova pomaknuti sedam mjesta unaprijed i postati neparna, a sva neparna slova će se pomaknuti sedam mjesta unazad i postati parna.

4.3 Složeni kritopisni sustav

Složeni ili kombinirani kritopisni sustav uključuje i zamjenu i premještanje slova poruke (Dujella i Maretić, 2007). Postoji dosta slobode kako pri kombiniranju tih metoda u kritopisnim sustavu, a u ovom radu će se primijeniti na isti način kao i u prethodna dva razvijena sustava: na razini pojedinačnih susjedstva. To znači kako će se u svakom susjedstvu primijeniti i zamjena i premještanje.

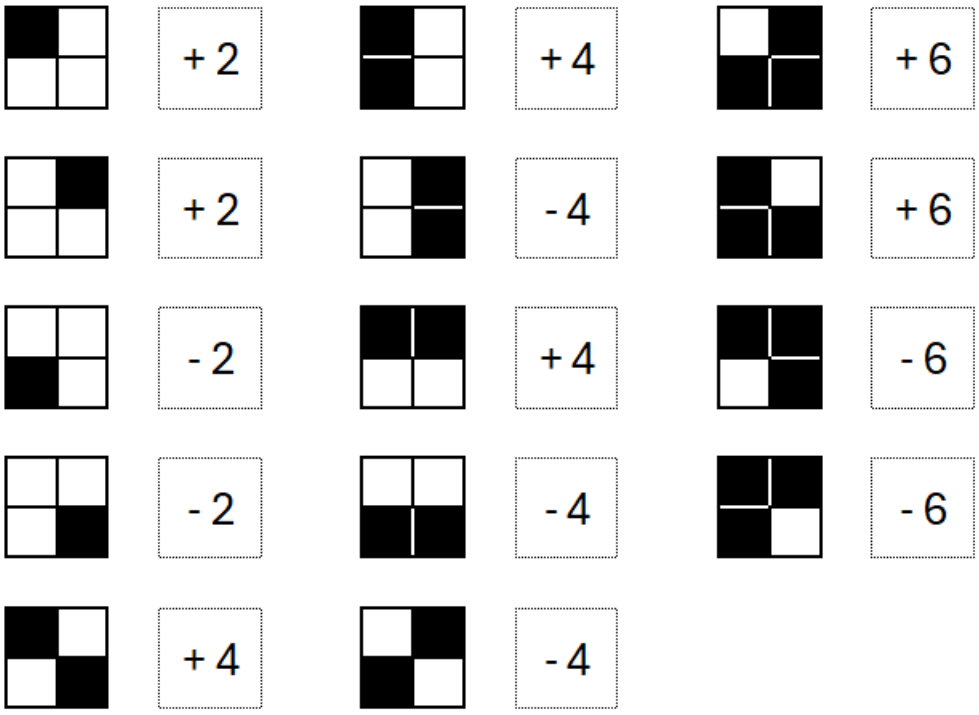
Sama primjena prethodnih dvaju kritopisnih sustava istovremeno nije valjan pristup; ako prostor u kojem je poruka raspoređena promatramo kao stanični prostor parnih i neparnih slova, odnosno stanja 1 i 0. Primjenom oba pravila istovremeno, premještanjem bi jedno susjedstvo prešlo u svoju sljedeću konfiguraciju, a zamjenom bi se iz te konfiguracije ponovo vratilo na početnu konfiguraciju. Rezultat bi bio statični stanični automat čija se stanja stanica ne mijenjaju iz generacije u generaciju, što znači da se poruka ne bi zakrivala na način nalik radu staničnog automata.

Moguć pristup koji samo kombinira prethodne sustave je korištenje jedne metode u jednom vremenskom koraku, a druge metode u drugom vremenskom koraku. Ovime automat ne bi bio statičan, ali bi se pojavio drugi problem: jedna metoda bi se uvijek

koristila u istoj verziji odjeljenja staničnog prostora. Na primjer, zamjena bi se uvijek odvijala u verziji odjeljenja koju koriste parne generacije automata, a premještanje bi se uvijek odvijalo u verziji odjeljenja koju koriste neparne generacije automata. Ovime se izgubilo svojstvo vremenski razdvojenog preklapanja koje je osnova Margolusovog susjedstva za postizanje složenog ponašanja koje vodi nepredvidljivosti. Ponovo se dolazi do istog rezultata: poruka se ne zakriva na način nalik radu staničnog automata.

Najjednostavniji način da se očuva princip rada staničnog automata korištenjem obje metode zakrivanja jest uspostavljanje da jedna metoda ne mijenja stanja stanica u susjedstvu, odnosno ne mijenja parnost slova. Kao što je obrazloženo u razvoju zamjenskog kritopisnog sustava, pomicanjem slova vrlo je lak način za promjenu vrijednosti slova bez promjene parnosti. Iz toga slijedi kako sve članove svakog susjedstva možemo pomaknuti za jednak, paran broj mjesta prije ili poslije nego ih premjestimo. Bitno je pritom naglasiti kako redoslijed primjena metoda mora biti dosljedan za svaki korak – uvijek prije ili uvijek nakon premještanja. U sklopu ovog sustava, slova će se pomicati prije premještanja.

Ovime se zaključuje da je za razvoj složenog kritopisnog sustava dovoljno primijeniti pravila premještajnog kritopisnog sustava te uključiti broj pomaka za svako susjedstvo.



Slika 11. Prvi skup pravila kombinacije, izvor: rad autora

Slika 11 prikazuje pomake za sporednu zamjenu složenog sustava koja ne utječe na stanje konfiguracije susjedstava. Za koliko mjesta će se svaki član susjedstva pomaknuti određuje broj parnih slova u susjedstvu: susjedstva s jednim parnim slovom će se pomaknuti za dva mjesta, susjedstva s dva parna slova će se pomaknuti za četiri mjesta, a susjedstva s tri parna slova će se pomaknuti za šest mjesta. Hoće li taj pomak biti unaprijed ili unazad po abecedi određuje se po slovu koje se izdvaja u osam konfiguracija gdje je jedno slovo parno, odnosno jedno slovo neparno: ako je slovo koje se izdvaja u gornjem dijelu susjedstva, pomak je udesno, a ako je u donjem dijelu susjedstva, pomak je ulijevo. Za preostalih šest konfiguracija, smjer pomicanja se određuje po prvom, gornje-lijevom slovu u susjedstvu: ako je prvo slovo parno, svi članovi se pomiču unaprijed, a ako je prvo slovo neparno, svi članovi se pomiču unazad.

Ova pravila održavaju reverzibilnost čitavog sustava zato jer pravila premještajnog kritopisnog sustava već samostalno mijenjaju stanja, što znači da su u kombinaciji s premještanjem i dalje u svojim inverznim parovima unatoč tome što ne mijenjaju stanje konfiguracije. Iznimka tome je slučaj s nula ili četiri parnih slova.

Slika 12. Drugi skup pravila kombinacije,
izvor: rad autora

Slika 12 prikazuje kako konfiguracije s nula ili četiri parnih slova odstupaju od ostalih i označavaju neparan pomak od 1. Ova odluka uvjetovana je činjenicom da samim premještanjem slova u susjedstvu nije moguće promijeniti njihovu parnost i stoga u premještajnim kritopisnim sustavu konfiguracije susjedstva sa svim neparnim i susjedstva sa svim parnim slovima nisu povezana inverznim pravilima prijelaza. Kako je već obrazloženo u razvoju zamjenskog sustava, povezanost ovih konfiguracija preko inverznih pravila je ključna za metodu zamjene, pošto je to jedini način da se održi lokalna reverzibilnost tih konfiguracija. S obzirom na to da su pravila premještanja u obje konfiguracije jednaka, promjena parnosti svih članova susjedstva u tim dvaju konfiguracijama ne utječe na pravila premještanja. Drugim riječima, u ovim dva slučaja je za razliku od ostalih zamjena glavna operacija pošto utječe na stanje konfiguracije, dok je premještanje sporedna operacija koja ne utječe na stanje konfiguracije.

4.4 Razvoj ključa

Dosad su razvijeni kriptografski algoritmi za sve tri vrste kritopisnih sustava. Definirana su pravila prema kojima će se poruke zakrivati, ali preostaju određene nedoumice u cjelokupnim sustavima koje je potrebno razriješiti kako bi se upotpunio proces zakrivanja. Nužno je uspostaviti koja će se verzija odjeljenja koristiti za prvu, odnosno svaku neparnu iteraciju, dok će se druga verzija koristiti za svaku parnu iteraciju. Također je nužno uspostaviti koliko će se iteracija primjenjivati pri zakrivanju. Ovo su promjenjivi dijelovi kritopisnog sustava i stoga se mogu definirati pomoću ključa. Shodno tome, informacije koje ključ mora nositi su: početno odjeljenje i broj iteracija. Ovo se može ostvariti na brojne načine, ali po uzoru na postojeće kritopisne sustave, koristit će se ključne riječi i/ili izrazi kao ključ.

Postoji dva moguća odjeljenja blokovskog staničnog automata s Margolusovim susjedstvom, parno i neparno, a ključ mora definirati u kojem se započinje proces zakrivanja. S obzirom na korištenje riječi i/ili izraza kao ključa, odlučeno je kako je prikladno da prvo slovo ključa nosi informaciju o prvoj iteraciji zakrivanja. Iz toga logično slijedi da parno prvo slovo označava početak u parnom odjeljenju, a neparno prvo slovo označava početak u neparnom odjeljenju.

Određivanje broja iteracija predstavlja dodatnu dvojbu pošto klasična kriptografija podrazumijeva ručno zakrivanje korak po korak. To znači da broj generacija treba biti broj za koji je realistično ispisivanje svih iteracija, pogotovo s obzirom na veličinu staničnog prostora. Stoga se predlažu dvije verzije ključa za zakrivanje: kraća verzija koja omogućava ručno zakrivanje poruke te duža verzija koja ostvaruje nepredvidljivije ponašanje po uzoru na ponašanje staničnih automata koji uglavnom podrazumijevaju velik broj generacija.

Kraća verzija ključa određuje broj iteracija na vrlo jednostavan način: broj slova u ključu označuje broj iteracija. Ovo omogućava svjesno biranje broja iteracija koje će se ručno ispisivati. Na primjer, ključ „Mama“ označava četiri iteracije pri zakrivanju.

S druge strane, duža verzija ključa određuje broj iteracija time da se svako slovo pretvara u broj prema svojem mjestu u abecedi te se ti brojevi zbrajaju u konačan rezultat koji čini broj iteracija. Ako se ponovno uzme „Mama“ kao ključ, to znači da će zakrivanje imati 18 + 1 + 18 + 1 = 40 iteracija, pošto je *M* osamnaesto slovo abecede, a *A* prvo slovo abecede.

5. Zakrivanje razvijenim kritopisnim sustavima

Stanični automat je teoretski beskonačna mreža stanica bez granica. Za razne simulacije nekih sustava to je vrlo korisno svojstvo pošto materija takvog sintetičkog svijeta nikada neće biti prostorno ograničena, niti će biti vremensko ograničena pošto se automat može proizvoljno dugo pustiti da djeluje. Problem se javlja kada je namjera koristiti stanični prostor u konkretnom zadatku za koji nije poželjan neograničen svijet, kao što je slučaj u ovome radu. Svrha ovih sustava je zamjena i premještanje elemenata poruka po uzoru na rad staničnog automata, što znači da „svijet“ koji stanični prostor čini se mora sastojati samo od elemenata poruka. Za svrhe ovog rada, potrebno je prikladno ograničiti stanični prostor.

Toffoli i Margolus (1987) ograničavaju stanični prostor tako da ga omotavaju oko sebe na način da spajaju lijevu i desnu stranu mreže, kao i gornju i donju stranu mreže. Nadalje opisuju dobiven oblik kao američku krafnu, ali prikladnije je koristiti stručan geometrijski izraz torus, koji se već od prije koristi u matematici na sličan način kako bi svako polje matrice imalo isti broj susjednih polja (Becher i Carton, 2023). Isti princip se primjenjuje iz istog razloga nad staničnim prostorom; ovime se omogućuje da u ograničenom prostoru svaka stanica ima jednak broj susjeda. Ovo svojstvo pogotovo je bitno za Margolusovo susjedstvo, konkretnije za neparnu verziju odjeljenja čija bi rubna susjedstva bila prerezana ako se strane prostora ne spajaju.

Stanični prostor potrebno je dalje ograničiti kako bi bio prikladan za blokovski stanični automat koji koristi Margolusovo susjedstvo. Naime, kako je jedno susjedstvo kvadrat veličine dva puta dva, potrebno je ustanoviti kako stanični prostor ne smije imati neparan broj redaka ili stupaca, pošto bi to rezultiralo nepravilnom mrežom susjedstava. Dimenzije staničnog prostora koje će ovi kritopisni sustavi koristiti standardizirat će se primjenom isključivo kvadratnih staničnih prostora. To znači da su valjane dimenzije staničnog prostora: četiri puta četiri, šest puta šest, osam puta osam i tako dalje. Koju dimenziju će se koristiti određuje se prebrojavanjem slova u poruci koja se zakriva i uzimanjem najmanje mogućih dimenzija.

Kako se stanični prostor ne bi sastojao od praznih polja, preostala mjesta se nadopunjuju nasumično izabranim slovima. Na primjer, ako se poruka sastoji od trideset slova, potrebno ju je nadopuniti sa šest nasumičnih slova kako bi stanični prostor veličine šest puta šest bio upotpunjen.

5.1 Zakrivanje premještajnim kritopisnim sustavom

Postupak zakrivanja će se prikazati demonstracijskim primjerom na kratkoj poruci. Kao ključ će se uzeti riječ „prst“ koja u kraćoj verziji ključa označava četiri iteracije, a u dužoj verziji ključa devedeset i pet iteracija. Jasnopis koja će se zakrivati glasi „Stanični automati“ i sastoji se od šesnaest slova, točan broj za stanični prostor veličine četiri puta četiri.

S	T	A	N
I	Č	N	I
A	U	T	O
M	A	T	I

Slika 13. Izvorno stanje demonstracijskog primjera, izvor: rad autora

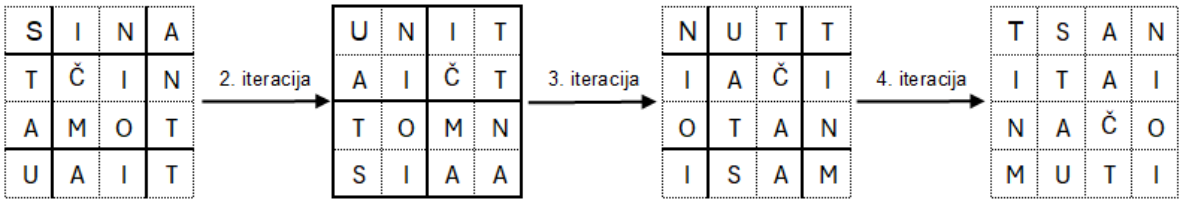
Slika 13 prikazuje poruku „stanični automati“ preslikanu u odgovarajući prostor i odijeljenu u parnu verziju odjeljenja sukladno ključu „prst“ koji počinje parnim slovom abecede. Susjedstva koja čine prostor poruke su (S, T, I, Č), (A, N, N, I), (A, U, M, A) i (T, O, T, I). Za svako susjedstvo određuje se konfiguracija gledajući parnosti slova. Kao pomoć pri primjeni pravila, koristi se prilog 1 koji nudi prikaz svih pravila. Iz priloga 1 se zaključuje:

- Susjedstvo (S, T, I, Č) konfiguracije (1, 1, 0, 1) premještanjem drugog i trećeg člana prelazi u (S, I, T, Č);
- Susjedstvo (A, N, N, I) konfiguracije (0, 0, 0, 0) premještanjem prvog i drugog te trećeg i četvrtog člana prelazi u (N, A, I, N);
- Susjedstvo (A, U, M, A) konfiguracije (0, 0, 1, 0) premještanjem drugog i trećeg člana prelazi u (A, M, U, A);
- Susjedstvo (T, O, T, I) konfiguracije (1, 0, 1, 0) premještanjem prvog i drugog te trećeg i četvrtog člana prelazi u (O, T, I, T).

S	I	N	A
T	Č	I	N
A	M	O	T
U	A	I	T

Slika 14. Rezultat prve iteracije premještanja demonstracijskog primjera, izvor: rad autora

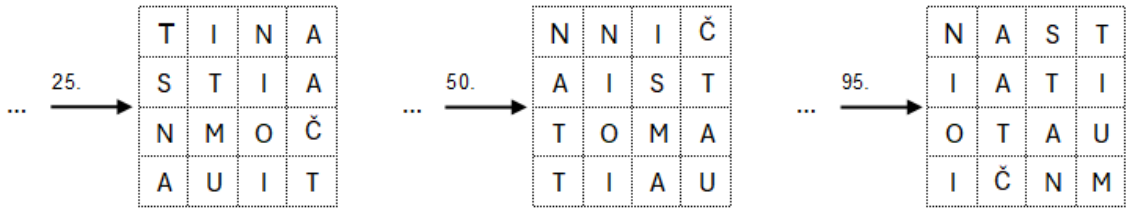
Slika 14 prikazuje rezultat ovih premještanja, odnosno prve iteracije poruke. Prateći princip rada Margolusovog susjedstva, prostor poruke se odjeljuje neparnom verzijom odjeljenja. Stoga su susjedstva ovog prostora (Č, I, M, O), (A, I, I, N), (N, T, T, A) i (T, U, A, S), s obzirom na to kako se strane mrežnog prostora spajaju slijeva i zdesna, kao i odozgo i odozdo. Isti postupak se primjenjuje nad ovim susjedstvima.



Slika 15. Preostale iteracije premještanja kraće verzije demonstracijskog primjera, izvor: rad autora

Na slici 15 su prikazane ostale iteracije ovih poruka, u kojima se mogu primijetiti tekuća susjedstva i odjeljenja prostora. Rezultat četvrte i konačne iteracije kraće verzije ključa prikazuje dobiveni zakritak „TSANI TAINA ČOMUT I“ koji se ispisuje u skupinama od pet kako bi se lakše prebrajala slova.

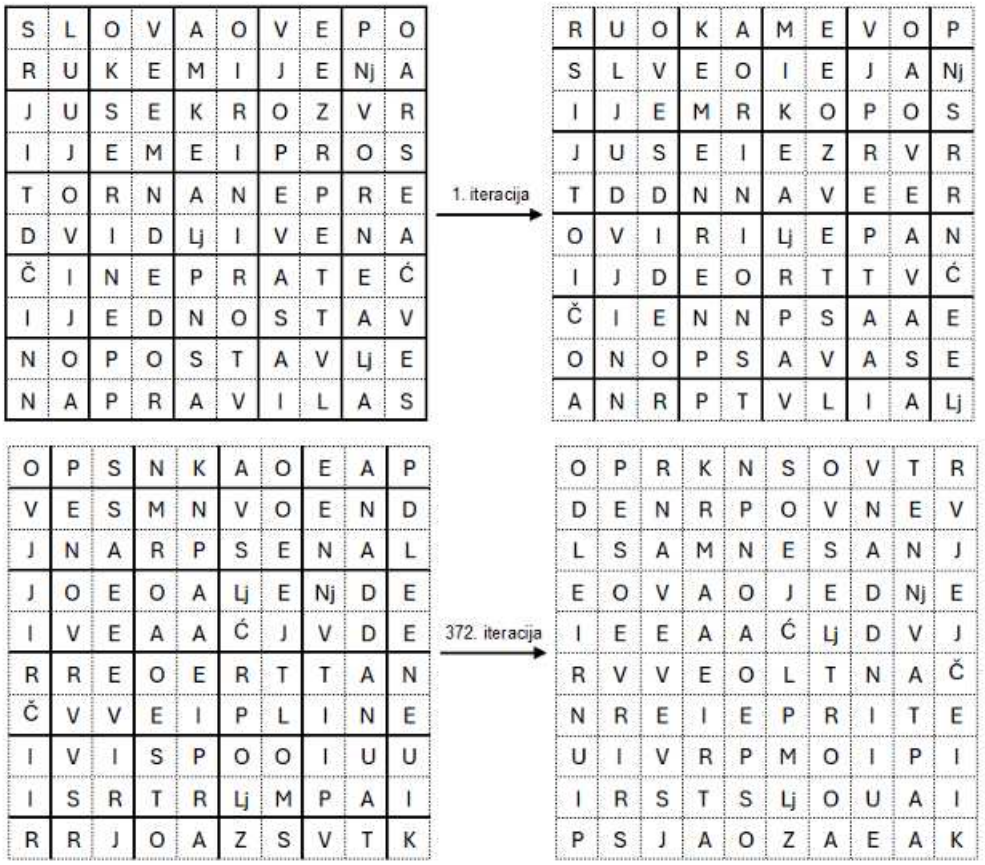
Postupak zakrivanja se nastavlja do devedeset i pete iteracije u slučaju duže verzije ključa.



Slika 16. Rezultati nekih iteracija premještanja duže verzije demonstracijskog primjera, izvor: rad autora

Na slici 16 su prikazani rezultati 25., 50. te konačne 95. iteracije čiji zakritak glasi „NASTI ATIOT AUIČN M.“

Kao jedan složeniji primjer, zakrit će se jasnopis „Slova ove poruke mijenjaju se kroz vrijeme i prostor na nepredvidljive načine prateći jednostavno postavljena pravila“ koristeći ključ „Tko rano rani dvije sreće grabi.“ Ova se poruka sastoji od 99 slova, što znači da se organizira u prostor veličine deset puta deset za koji nedostaje jedno slovo. Nasumično je odabrano slovo S kako bi se prostor upotpunio.



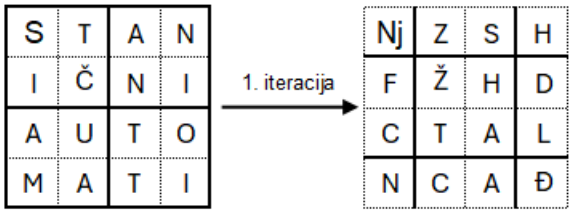
Slika 17. Složeniji primjer premještanja, izvor: rad autora

Odabrani ključ u dužoj verziji označava 372 iteracije, a slika 17 prikazuje prvu i konačnu iteraciju koja izlaže zakritak: „OPRKN SOVTR DENRP OVNEV LSAMN ESANJ EOVAO JEDNjE IEEAA ĆLjDVJ RVVEO LTNAČ NREIE PRITE UIVRP MOIPI IRSTS LjOUAI PSJAO ZAEAK.“

Što se tiče raskrivanja, postupak je identičan zakrivanju. Izvorno stanje je dobiveni zakritak, a početno odjeljenje koje se koristi određuje se pomoću ključa: prvo se odredi početno odjeljenje korišteno u zakrivanju te se odredi broj iteracija kroz koji je poruka prošla; ako je poruka prošla kroz parni broj iteracija, početno odjeljenje je suprotno onom koje se koristilo u zakrivanju, a ako je poruka prošla kroz neparan broj iteracija, početno odjeljenje je isto kao u zakrivanju.

5.2 Zakrivanje zamjenskim kritopisnim sustavom

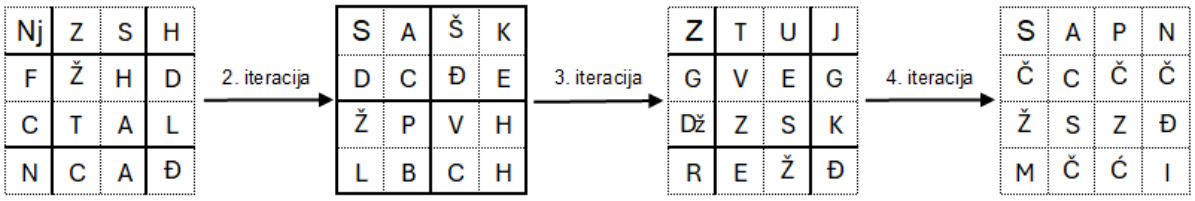
Zamjenski kritopisni sustav djeluje na isti princip te će se kao demonstracijski primjer ponovo koristiti jasnopis „stanični automat“ s ključem „prst.“



Slika 18. Prva iteracija zamjena demonstracijskog primjera, izvor: rad autora

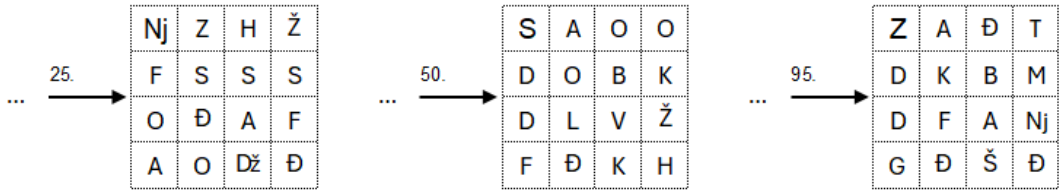
Na slici 18 se može primijetiti kako se u prvoj iteraciji radi o istim susjedstvima kao u premještajnim sustavu, pošto su jasnopis i ključ identični. Međutim, već će u prvoj iteraciji doći do promjene u konačnom skupu parnosti svih slova poruke, pošto jedno susjedstvo ima konfiguraciju (0, 0, 0, 0) koja u zamjenskom sustavu prelazi u (1, 1, 1, 1). Ponovno se koristi prilog 1 kao pomoć pri primjenjivanju pravila te se zaključuje:

- Susjedstvo (S, T, I, Č) konfiguracije (1, 1, 0, 1) pomiče se za (-4, +3, -3, -4), čime prelazi u (Nj, Z, F, Ž);
- Susjedstvo (A, N, N, I) konfiguracije (0, 0, 0, 0) pomiče se za (-7, -7, -7, -7), čime prelazi u (S, H, H, D);
- Susjedstvo (A, U, M, A) konfiguracije (0, 0, 1, 0) pomiče se za (+2, -1, +1, +2), čime prelazi u (C, T, N, C);
- Susjedstvo (T, O, T, I) konfiguracije (1, 0, 1, 0) pomiče se za (+5, -5, +5, -5), čime prelazi u (A, L, A, Đ).



Slika 19. Preostale iteracije zamjena kraće verzije demonstracijskog primjera, izvor: rad autora

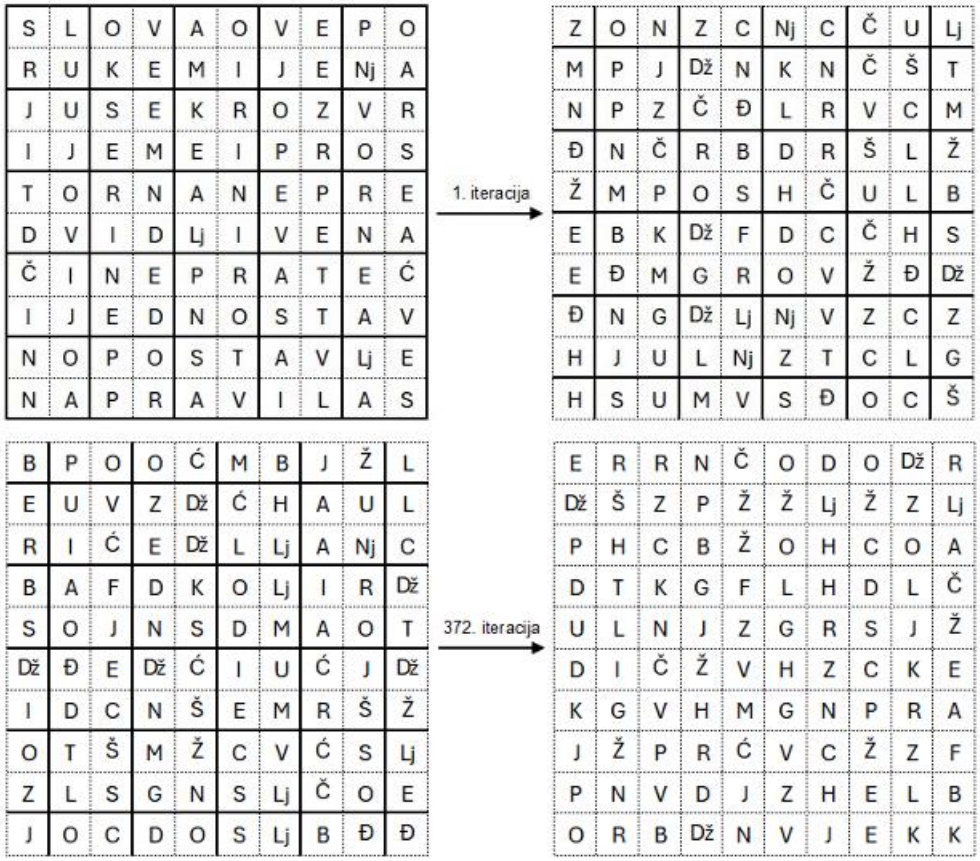
Slika 19 prikazuje preostale tri iteracije kraće verzije ključa, nakon kojih se dobiva zakritak „SAPNČ CČČŽS ZĐMČĆ I.“



Slika 20. Rezultati nekih iteracija zamjena duže verzije demonstracijskog primjera, izvor: rad autora

Slika 20 kao i u premještajnim sustavu prikazuje rezultate 25., 50. i konačne 95. iteracije duže verzija ključa čiji zakritak glasi „ZAĐTD KBMDF ANjGĐŠ Đ“

Zamjenskim sustavom zakrit će se i isti složeniji primjer korišten u premještajnim sustavu.



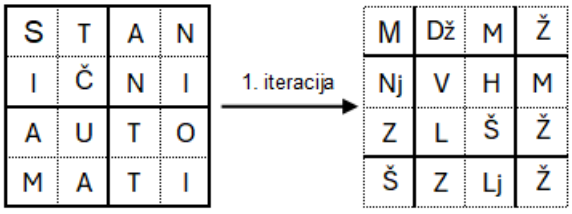
Slika 21. Složeniji primjer zamjena, izvor: rad autora

Slika 21 prikazuje ponovno zakrivanje jasnopisa „Slova ove poruke mijenjaju se kroz vrijeme i prostor na nepredvidljive načine prateći jednostavno postavljena pravila“ koristeći ključ „Tko rano rani dvije sreće grabi,“ s time da se ovaj put koristi zamjenski kritopisni sustav. Također je ponovno korišteno slovo S kako bi se upotpunio prostor poruke. Prikazane su iste iteracije kao u prethodnom slučaju, a rezultat konačne 372. iteracije glasi „ERRNČ ODODžR DžŠZPŽ ŽLjŽZLj PHCBŽ OHCOA DTKGF LHDLČ

ULNJZ GRSJŽ DIČŽV HZCKE KGVHM GNPRA JŽPRĆ VCŽZF PNVDJ ZHEČB ORBDžN VJEKK.“

5.3 Zakrivanje složenim kritopisnim sustavom

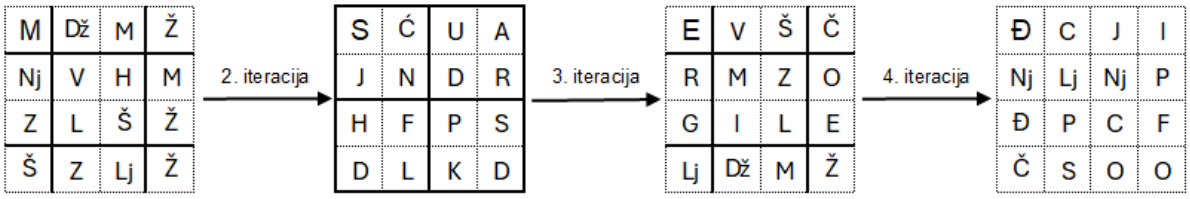
Kao i u prethodna dva sustava, koristi se isti demonstracijski primjer jasnopisa „stanični automati“ koji se zakriva pomoću ključa „prst.“



Slika 22. Prva iteracija kombinacija demonstracijskog primjera, izvor: rad autora

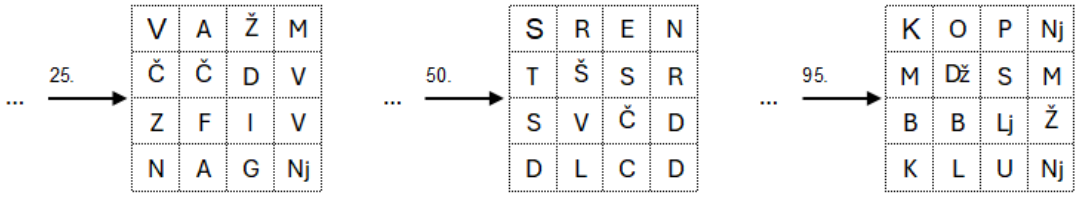
Slika 22 prikazuje prvu iteraciju zakrivanja poruke složenim kritopisnim sustavom. Iščitavajući prilog 1 zaključuje se:

- Susjedstvo (S, T, I, Č) konfiguracije (1, 1, 0, 1) pomiče se za (-6, -6, -6, -6) te premještanjem drugog i trećeg člana prelazi u (M, Dž, Nj, V);
- Susjedstvo (A, N, N, I) konfiguracije (0, 0, 0, 0) pomiče se za (-1, -1, -1, -1) te premještanjem prvog i drugog te trećeg i četvrtog člana prelazi u (M, Ž, H, M);
- Susjedstvo (A, U, M, A) konfiguracije (0, 0, 1, 0) pomiče se za (-2, -2, -2, -2) te premještanjem drugog i trećeg člana prelazi u (Z, L, Š, Ž);
- Susjedstvo (T, O, T, I) konfiguracije(1, 0, 1, 0) pomiče se za (+4, +4, +4, +4) te premještanjem prvog i drugog te trećeg i četvrtog člana prelazi u (Š, Ž, Lj, Ž).



Slika 23. Preostale iteracije kombinacija kraće verzije demonstracijskog primjera, izvor: rad autora

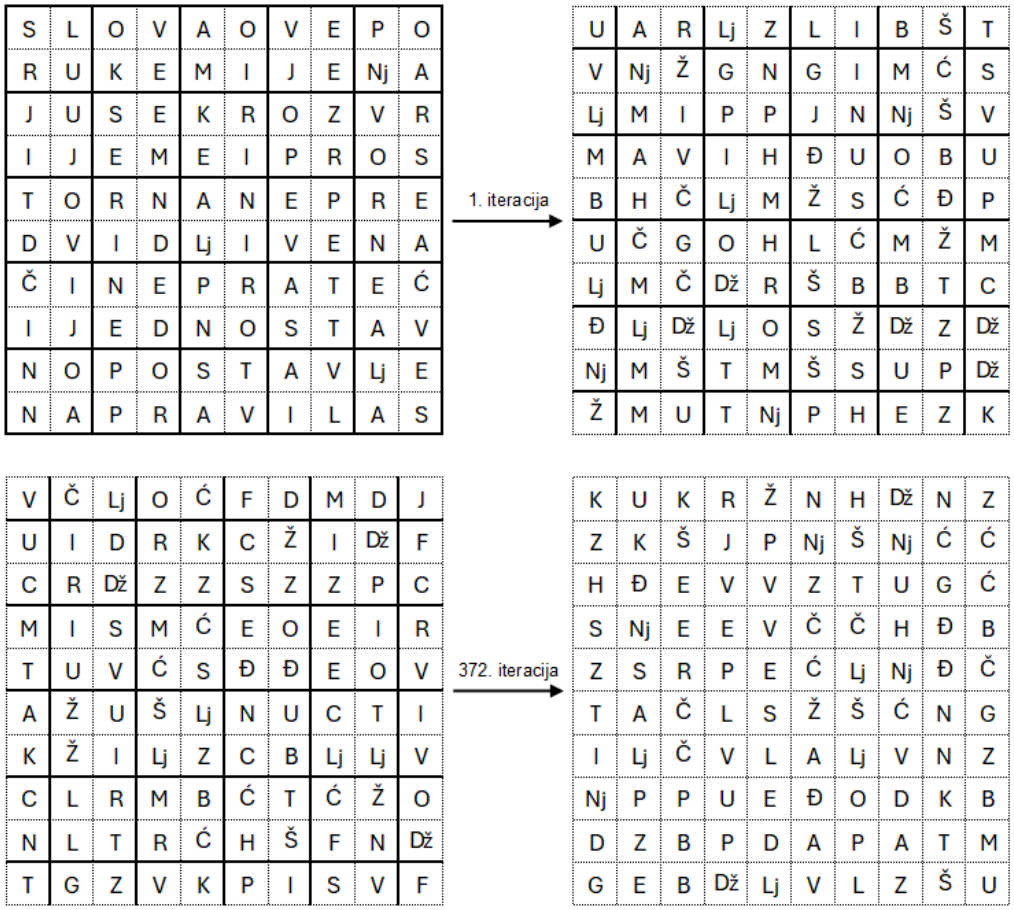
Slika 23 prikazuje preostale tri iteracije kraće verzije ključa, nakon kojih se dobiva zakritak „ĐCJINj LjNjPĐP CFČSO O.“



Slika 24. Rezultati nekih iteracija kombinacija duže verzije demonstracijskog primjera, izvor: rad autora

Što se tiče duže verzije ključa, slika 24 prikazuje rezultate 25., 50. i konačne 95. iteracije čiji zakritak glasi „KOPNjM DžSMBB LjŽKLU Nj.“

Isti složeniji primjer jasnopisa „Slova ove poruke mijenjaju se kroz vrijeme i prostor na nepredvidljive načine prateći jednostavno postavljena pravila“ s ključem „Tko rano rani dvije sreće grabi“ zakrit će se složenim kritopisnim sustavom.



Slika 25. Složeniji primjer kombinacija, izvor: rad autora

Slika 25 prikazuje kako je zbog dosljednosti ponovno korišteno slovo S kako bi se upotpunio prostor te prikazuje iste iteracije kao i u prošlim slučajevima. Zakritak dobiven konačnom 372. iteracijom glasi „KUKRŽ NHDžNZ ZKŠJP NjŠNjĆĆ HĐEVV ZTUGĆ SNjEEV ČČHĐB ZSRPE ĆLjNjĐČ TAČLS ŽŠĆNG ILjČVL ALjVNZ NjPPUE ĐODKB DZBPD APATM GEBDžLj VLZŠU.“

6. Evaluacija razvijenih kritopisnih sustava

Prema kriterijima koje su opisali Dujella i Maretić (2007), sva tri razvijena kritopisna sustava se definiraju kao blokovski i simetrični sustavi, pošto se poruka obrađuje u blokovima umjesto element po element te se za zakrivanje i raskrivanje koristi isti ključ. Ovaj dio rada bavit će se evaluacijom ovih kritopisnih sustava. Razmatrat će se njihova sigurnost općenito, praktičnost te neki konkretni problemi koji su se javili pri zakrivanju.

Temeljni cilj svakog kritopisnog sustava jest da služi kao siguran način za zaštitu podataka. Stinson i Paterson (2018) opisuju tri različita aspekta koje se mora uzeti u obzir pri razmatranju sigurnosti nekog kritopisnog sustava:

- Informacije koje su dostupne napadaču;
- Što znači da je kritopisni sustav probijen;
- Koji su resursi potrebni za probijanje sustava.

Što se tiče informacijama dostupnim napadaču, može se razmatrati slučaj kada napadač ne zna koji je kritopisni sustav korišten i slučaj kada napadač zna koji je kritopisni sustav korišten. Zbog veće sigurnosti, pretpostavlja se drugi slučaj u kojem je sustav poznat napadaču, a ovo načelo naziva se Kerckhoffsovo načelo. Kerckhoffsovo načelo je srž modernog shvaćanja sigurnosti jer odbacuje dvojbu zna li ili ne napadač koji je kritopisni sustav korišten. Disciplina koja se bavi daljnjim metodama probijanja kritopisnih sustava naziva se kriptoanaliza, a temelj moderne kriptoanalize upravo je Kerckhoffsovo načelo (Dujella i Maretić, 2007).

S time na umu, svi klasični kritopisni sustavi smatraju se nesigurnim. Doista, ako se kritopisne sustave razvijene u ovom radu smatra poznatima, odnosno ako su pravila koja se primjenjuju poznata, jedino što sustav čini sigurnim su informacije koje nosi ključ: početno odjeljenje i broj iteracija. Sigurnost ovih sustava stoga može se stoga evaluirati kroz tri aspekta koja su opisali Stinson i Paterson (2018):

- Napadaču je poznat čitav algoritam kritopisnog sustava;
- Sustav je probijen kad je otkriveno početno odjeljenje i broj iteracija;
- Resursi potrebni za probijanje sustava su identični onima koji su potrebni za zakrivanje poruke, osim vremenskog resursa koje je dvostruko veće zbog dva moguća početna odjeljenja.

Iz gornje evaluacije može se zaključiti kako je jedini način na koji bi se mogla pružiti veća sigurnost sustava uključivanje velikog broja iteracija. Međutim, provođenje velikog broja iteracija je vremenski vrlo zahtjevno, pogotovo s eksponencijalnim rastom prostora poruke u slučajevima dužih jasnopisa. Korištenjem računala izbjegao bi se problem utrošenog vremena, ali to podrazumijeva da napadač također koristi računalnu brzinu pri svojem napadu, što znači da nije bitno koliko iteracija postoji.

Osim sigurnosti, vrijedi spomenuti jedan problem praktičnosti: nadopunjavanje. Ako poruka nema dovoljan broj slova da upotpuni prostor poruke, prazna mjesta se nadopunjavaju nasumično izabranim slovima. Ovo je problem jer duljine koje poruka mora biti fiksne: $4^2 = 16$, $6^2 = 36$, $8^2 = 64$ i tako dalje. To znači da u slučaju kada je poruka primjerice duljine 17, ona ne stane u prostor poruke veličine četiri puta četiri te se mora postaviti u prostor poruke šest puta šest. Međutim, u tom slučaju potrebno je upotpuniti prostor poruke s 19 nasumičnih slova, što znači da bi se stanični prostor sastojao od više nasumičnih slova nego koliko slova čini poruku koja se želi prenijeti – zalihost nadopunjene poruke bila bi veća od 50%. Stoga se na duljinu poruke koja se zakriva mora obratiti posebna pažnja.

Pri zakrivanju se otkrio temeljni problem u jednom od kritopisnih sustava. Naime, premještajni kritopisni sustav razlikuje se od ostala dva po tome što konfiguracije (0, 0, 0, 0) i (1, 1, 1, 1) ostaju nepromijenjene što se tiče parnosti slova. To znači da za razliku od ostala dva sustava, omjer parnih i neparnih slova je konstantan u svakoj iteraciji, što rezultira puno većom mogućnosti da se nakon određenog broja iteracija prostor poruke vrati na izvorno stanje. Zato je za demonstracijski primjer uzet jasnopis „stanični automati.“ Zakrivanjem se pokazalo kako se prostor poruke ovog jasnopisa vrati u svoje izvorno stanje svakih dvadeset iteracija. Drugim riječima, za taj primjer postoji samo dvadeset mogućih iteracija koje se ponavljaju. Doista, ako se prouči rezultat dvadeset i pete iteracije na slici 14, primijetit će se kako je ona identična sljedećoj iteraciji nakon četvrte iteracije prikazane u slici 13. Razlog tome jest činjenica da se prostor poruke vratio na izvorno stanje u dvadesetoj iteraciji, što znači da je rezultat dvadeset i četvrte iteracije identičan rezultatu četvrte iteracije prikazan na slici 13, a sljedeće iteracija oba rezultata dat će identičan rezultat prikazan na slici 14. Ovaj problem uočen je samo u premještajnim kritopisnim sustavu te samo u slučajevima kad je korišten najmanji moguć prostor poruke veličine četiri puta četiri. Najmanji

uočeni broj mogućih iteracija jednog prostora iznosio je četiri iteracije nakon kojih bi se prostor vratio na izvorno stanje.

Zbog navedenih razloga, može se zaključiti kako kritopisni sustavi razvijeni u ovom radu nisu adekvatno sigurni za moderne potrebe kriptografije te imaju konkretne probleme koji se mogu javljati u određenim situacijama. Međutim, cilj rada nije bio osmisliti praktične kritopisne sustave s mogućom namjenom u današnjem svijetu. Cilj rada bio je osmisliti kritopisne sustave koji koriste klasične metode zamjene i premještanja po uzoru na slojevita ponašanja staničnih automata. U današnje vrijeme se klasična kriptografija koristi u akademskim okruženjima kao temelj koji služi za priopćavanje rada modernih kritopisnih sustava. Kritopisni sustavi razvijeni u ovom radu mogu se stoga koristiti kao temelj za priopćavanje rada staničnih automata koji imaju široku primjenu u čitavom području kriptografije, kao i za priopćavanje rada blokovskih kritopisnih sustava koji su aktualni u današnjem svijetu. Za takav pristup, lako se mogu izbjeći konkretni problemi nadopunjavanja prostora poruke ili ponavljanja iteracija u premještajnim sustavu uspostavljanjem jasnopisa nad kojima se mogu primjenjivati ovi kritopisni sustavi u obrazovne svrhe i za koje je poznato da ne stvaraju navedene probleme.

7. Zaključak

Primjena jednostavnih pravila nad skupinama od četiri slova u svrhu njihovog premještanja, zamjene ili oboje koja kroz više iteracija vodi nepredvidljivom zakritku pokazala se kao intuitivan način na koji se osnovni princip staničnih automata može predočiti pomoću klasične kriptografije.

Primjenom opisane teorije razvijeni su zamjenski, premještajni i složeni kritopisni sustavi čije metode zakrivanja prate pravila prijelaza blokovskog staničnog automata osmišljenog upravo za tu namjenu. Prikazom postupka zakrivanja ovim sustavima pokazala se primjena koja je jednostavna ako se gleda blok po blok susjeda, ali složena ako se gleda čitava jedna iteracija odjednom, a kamoli više iteracija. Rezultat ovog postupka je zakritak nepredvidljiv čak i kriptografu koji primjenjuje dotični kritopisni sustav. Ovo čini razvijene sustave vrlo efikasnim kad ih se usporedi s ostalim klasičnim kritopisnim sustavima koji koriste metode zamjene, premještanje i kombinaciju obje.

Međutim, evaluacija ovih sustava pokazala je kako nisu bez mana. Pri odabiru jasnopisa koji će se zakriti, mora se posebno obratiti na duljinu poruke. Također, kratke poruke pokazale su se neprimjerenima za premještajni kritopisni sustav. Konačno, računalna brzina učinila je ove sustave zastarjelima prije nego su se osmislili.

Unatoč tome, kritopisni sustavi razvijeni u ovome radu djelotvorni su kao spoj teorije staničnih automata s klasičnom kriptografijom i mogu poslužiti kao koristan primjer izučavanja učenjacima koji se bave teorijom automata i kriptologijom.

8. Literatura

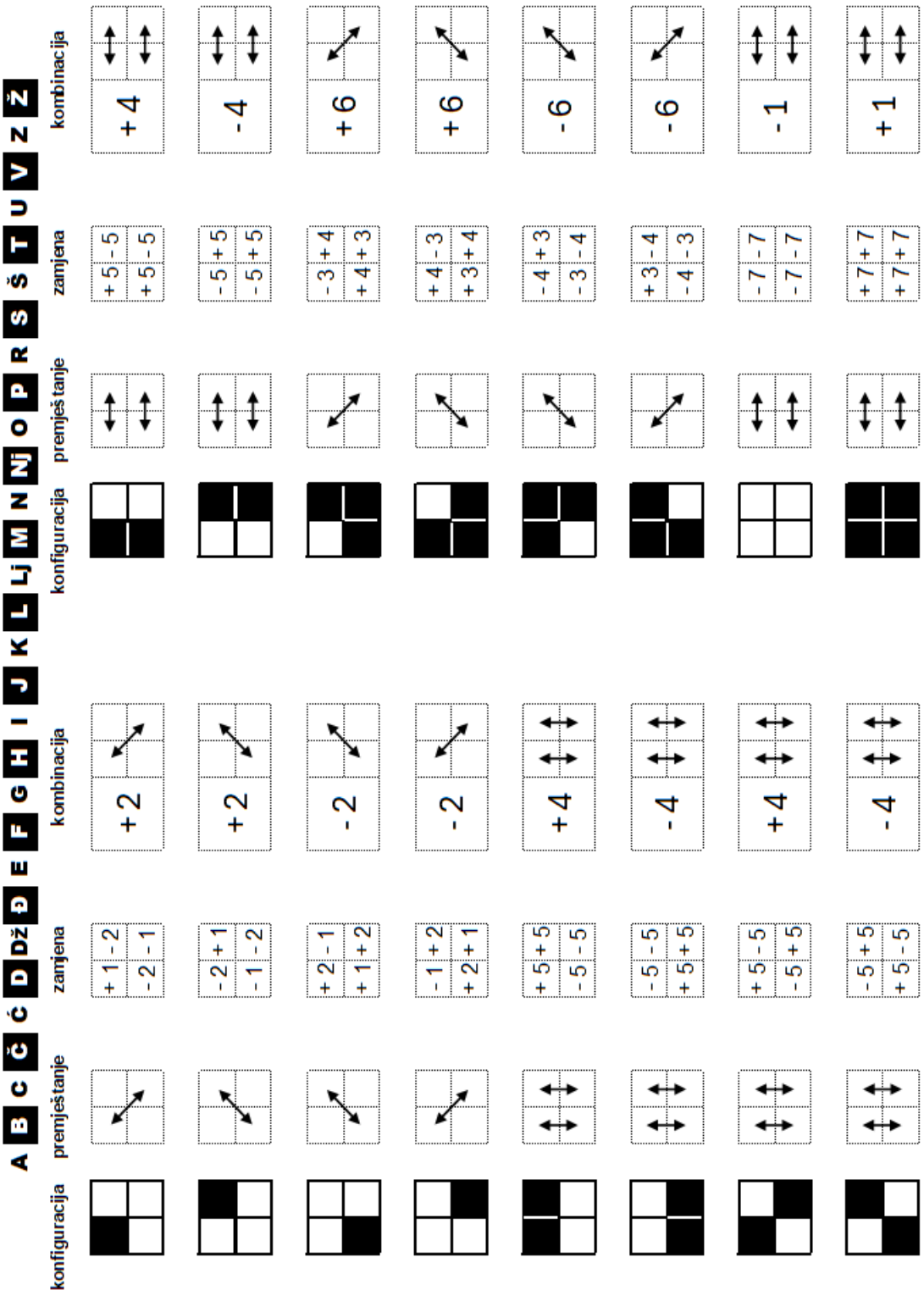
1. Abusham, E., Ibrahim, B., Zia, K. i Rehman, M. (2023). *Facial image encryption for secure face recognition system*. Electronics, 12(3), 774. doi:https://doi.org/10.3390/electronics12030774
2. Banoth, R. i Regar, R. (2023). *Classical and modern cryptography for beginners*. Springer Nature.
3. Becher, V. i Carton, O. (2023). *Nested perfect toroidal arrays*. [online] arXiv.org. Dostupno na: https://arxiv.org/abs/2301.00633 [29.5.2024.].
4. Berto, F. i Tagliabue, J. (2023). *Cellular automata*. [online] The Stanford Encyclopedia of Philosophy. Dostupno na: https://seop.illc.uva.nl/entries/cellular-automata/ [29.5.2024.].
5. Bhattacharjee, K. (2019). *Cellular Automata: Reversibility, Semi-reversibility and Randomness*. [online] arXiv.org. https://arxiv.org/abs/1911.03609 [29.5.2024.].
6. Chopard, B. i Droz, M. (1998). *Cellular automata modeling of physical systems*. Cambridge University Press.
7. Dujella, A. i Maretić, M. (2007). *Kriptografija*. Element.
8. Hadeler, K. i Müller, J. (2018). *Cellular Automata: analysis and applications*. Springer.
9. Klima, R. E. i Sigmon, N. (2018). *Cryptology: Classical and Modern*. CRC Press.
10. Levina, A., Mukhamedjanov, D., Bogaevskiy, D., Lyakhov, P., Valueva, M. i Kaplun, D. (2022). *High performance Parallel Pseudorandom Number Generator on cellular Automata*. Symmetry, 14(9), 1869. doi:https://doi.org/10.3390/sym14091869.
11. Morita, K. (2018). *Reversible Cellular Automata*. U: Adamatzky, A. (ur) *Cellular Automata*. Encyclopedia of Complexity and Systems Science Series. Springer. doi:https://doi.org/10.1007/978-1-4939-8700-9_455.
12. Shao, C., Shao, F., Liu, X., Yang, D., Sun, R., Zhang, L. i Jiang, K. (2024). *A Multi-Information dissemination model based on cellular automata*. Mathematics, 12(6), 914. doi:https://doi.org/10.3390/math12060914.
13. Simmons, G. J. (2023). *Cryptology*. [online] Encyclopaedia Britannica. Dostupno na: https://www.britannica.com/topic/cryptology [29.5.2024.].

14. Stănică, G. C. i Anghelescu, P. (2023*). Cryptographic algorithm based on Hybrid One-Dimensional Cellular Automata*. Mathematics, 11(6), 1481. doi:https://doi.org/10.3390/math11061481.
15. Stinson, D. R. i Paterson, M. B. (2018). *Cryptography: Theory and Practice*. CRC Press, Taylor & Francis Group.
16. Toffoli, T. i Margolus, N. (1987). *Cellular automata machines: A New Environment for Modeling*. MIT Press.
17. Weisstein, E. W. (2024). *Game of Life*. [online] Mathworld. Dostupno na https://mathworld.wolfram.com/GameofLife.html [29.5.2024.].
18. Wolfram, S. (2002). *A new kind of science*. Wolfram Media.
19. Wu, S. i Chang, J. (2023). *Secure One-Way hash function using cellular automata for IoT*. Sustainability, 15(4), 3552. doi:https://doi.org/10.3390/su15043552.
20. Yin, X. i Hadjiloucas, S. (2023). *Digital filtering techniques using Fuzzy-Rules based logic control*. Journal of Imaging, 9(10), 208. doi:https://doi.org/10.3390/jimaging9100208.

Popis slika

Prilozi

Prilog 1 – pomoćni prikaz pravila



Slika 26. Pomoćni prikaz pravila zakrivanja, izvor: rad autora

Primjena staničnih automata u razvoju kritopisnih sustava

Sažetak

Stanični automat je mreža stanica u kojoj se prema unaprijed određenim pravilima stanje svake stanice mijenja ovisno o stanjima njezinih susjednih stanica. S vremenom, jednostavno definirana pravila mogu proizvesti izrazito složene uzorke ponašanja. Kritopisni sustavi mogu koristiti sličnu mrežu kao prostor za organizaciju poruke u kojoj se u svakom polju nalazi po jedan element poruke te se ti elementi zamjenjuju ili premještaju prema određenom algoritmu. Ovaj rad povezuje područja teorije automata i kriptologije koristeći takvu mrežu kao poveznicu između staničnih automata i kritopisnih sustava. Istražuje se primjena staničnih automata u kritopisnim sustavima kroz razvoj kritopisnih sustava koji zamjenjuju, odnosno premještaju elemente poruka na način nalik radu staničnog automata. Implementacijom i evaluacijom ovih sustava promatra se doprinos staničnih automata u razvoju kritopisnih sustava.

Ključne riječi: kriptografija, kritopisni sustavi, stanični automati, blokovski stanični automati

The application of cellular automata in the development of cryptosystems

Summary

A cellular automaton is a grid of cells in which each cell's state changes according to predetermined rules applied depending on the states of that cell's neighbours. With time, simple rules may produce extremely complex patterns of behaviour. Cryptosystems may use a similar grid as an organizational space in which each element of the plaintext represents one cell in the grid and such are substituted or transposed based on the system's algorithm. This paper connects the fields of automata theory and cryptology by employing such a grid as the link between cellular automata and cryptosystems. The application of cellular automata in cryptosystems is explored through the development of cryptosystems that substitute or transpose elements of the plaintext in a manner similar to the way cellular automata work. Through implementation and evaluation of this systems, this work examines the contribution of cellular automata in the development of cryptosystems.

Key words: cryptography, cryptosystems, cellular automata, block cellular automata