UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO
ODDELEK ZA FIZIKO
PROGRAM APLIKATIVNA FIZIKA

Gašper Harej

KVANTNI GENERATORJI NAKLJUČNIH ŠTEVIL

Zaključna naloga

MENTOR: dr. Peter Jeglič
SOMENTOR: prof. dr. Rok Žitko

Ljubljana, 2025

Zahvale

Iskreno se zahvaljujem mentorju dr. Petru Jegliču za vse dragocene nasvete, usmeritve ter hitro odzivnost pri vprašanjih in dilemah. Posebna zahvala gre tudi somentorju dr. Roku Žitku za pripravljenost pomagati, koristne nasvete ter omogočen dostop do kvantnega generatorja, brez katerega eksperimentalni del naloge ne bi bil mogoč.

Velika hvala moji družini za stalno spodbudo, potrpežljivost in razumevanje v času študija in pisanja naloge.

Vsem, ki ste kakorkoli prispevali k nastanku te naloge, se iskreno zahvaljujem.

Kvantni generatorji naključnih števil

Izvleček

V nalogi obravnavam kvantne generatorje naključnih števil (QRNG) kot napredne vire naključnosti, ki presegajo omejitve klasičnih metod. Najprej predstavim teoretično ozadje in pomen naključnosti pri kriptografiji, simulacijah in znanstvenih raziskavah. Posebno pozornost namenim razlikam med psevdonaključnimi (PRNG), strojnimi (TRNG) in kvantnimi generatorji naključnih števil, pri čemer slednji temeljijo na nedeterminističnih kvantnih pojavih.

V praktičnem delu analiziram delovanje naprave Qocka, ki temelji na delitvi posameznih fotonov, ter obravnavam pridobivanje podatkov. Podatke sem obdelal z von Neumannovim in Toeplitzovim ekstraktorjem ter jih ovrednotil s statističnimi testi (Dieharder, PractRand) in oceno min-entropije (NIST SP 800-90B). Rezultati kažejo, da obdelani nizi prestanejo zahtevne preizkuse, vendar to samo po sebi še ne zagotavlja resnične entropije, saj tudi deterministični generator dosega podobne statistične lastnosti. Sklepam, da je za zanesljivo vrednotenje QRNG nujna kombinacija statističnih testov, modeliranja vira in konservativne ocene entropije. Naloga tako prispeva k razumevanju pomena postprocesiranja in metod ocenjevanja pri razvoju varnih kvantnih generatorjev.

Ključne besede: kvantni generatorji naključnih števil, entropija, statistični testi, ekstraktorji, kriptografija

Quantum Random Number Generators

Abstract

This thesis explores quantum random number generators (QRNG) as advanced sources of randomness that overcome the limitations of classical approaches. First, the theoretical background and the role of randomness in cryptography, simulations, and scientific research are presented. Special attention is given to the differences between pseudorandom number generators (PRNG), true random number generators (TRNG), and quantum random number generators (QRNG), with the latter relying on inherently nondeterministic quantum phenomena.

In the experimental part, I analyze the operation of the Qocka device based on single-photon splitting and discuss the acquisition of raw data. The data were processed using von Neumann and Toeplitz extractors and evaluated with statistical tests (Dieharder, PractRand) as well as min-entropy estimation (NIST SP 800-90B). The results show that processed sequences pass stringent tests, but this alone does not guarantee genuine entropy, since a deterministic generator can achieve similar statistical properties. I conclude that reliable evaluation of QRNG requires a combination of statistical testing, source modeling, and conservative entropy estimation. The thesis thus contributes to understanding the importance of post-processing and assessment methods in the development of secure quantum generators.

Keywords: quantum random number generators, entropy, statistical tests, extractors, cryptography

Kazalo

Seznam slik

1. Uvod

Naključna števila so temeljni gradnik sodobnih informacijskih tehnologij: od kriptografije in zaščite podatkov, do znanstvenih simulacij, statistike, loterij in drugih reguliranih postopkov, kjer so varnost, zanesljivost in nepristranskost ključnega pomena [2, 3, 4]. V najstrožjem pomenu so števila naključna takrat, ko izidov ne more predvideti noben opazovalec [5]. To zahtevo neposredno srečamo v kriptografiji, kjer sodobni protokoli po Kerckhoffsovem načelu temeljijo na tajnosti skritega ključa, ki mora biti enakomerno izbran in iz praktičnega vidika informacijsko *nepredvidljiv*, pri čemer velja, da varnost ne temelji na skrivnosti algoritma, temveč zgolj na skrivnosti ključa [2, 6]. Slaba naključnost tako pomeni napadljivo začetno seme ter posledično ranljivost sistema [6].

Generatorje naključnih števil navadno razdelimo na programske (psevdorandom numbers generator (PRNG)) in strojne (true random numbers generator (TRNG)) [1, 6]. PRNG so deterministični algoritmi, ki iz kratkega *semena* proizvajajo navidezno naključne nize; njihova praktična vrednost je hitrost in nizka cena, a ključna omejitev je, da naključnost ni informacijsko-teoretično dokazljiva in na koncu temelji na predpostavkah o računski omejenosti nasprotnika [1, 4, 5]. TRNG po drugi strani črpajo entropijo iz fizičnih pojavov in zato ponujajo »pravo« naključje; vendar mora biti fizični vir modeliran, merjen in nadzorovan, saj neidealnosti (pristranskosti, korelacije, drift) neizogibno vstopijo v merilno verigo [2, 6]. V praksi so zato TRNG in PRNG pogosto *hibridno* spojeni: fizični vir inicializira kriptografsko varen PRNG, ki zagotavlja razširjeno in ponovljivo dobavo bitov, medtem ko fizični del nudi neodvisno entropijo [1].

V zadnjih dveh desetletjih je kvantna fizika pomembno preoblikovala razumevanje varnosti, kriptografije in računanja [2]. **Kvantni generatorji naključnih števil** (quantum random numbers generator (QRNG)) kot vir entropije izkoriščajo kvantnomehanske pojave (superpozicija, naključnost izidov meritev, prepletenost), ki so v osnovi nedeterministični [5, 6]. Za razliko od klasičnih TRNG je pri QRNG jasno, od kod izvira naključnost, kar olajša certificiranje; napake je mogoče nadzirati v realnem času, naprednejše sheme pa omogočajo tudi *certificirano zasebnost* izhodov brez zaupanja proizvajalcu. Ob tem so parametri, kot so hitrost, vgradljivost in poraba, vse bolj konkurenčni; glavna ovira ostaja cena [6]. V praksi QRNG omogočajo tvorbo bitov z informacijsko-teoretičnim jamstvom o izvoru naključnosti [3, 4].

Čeprav so kvantne postavitve v teoriji idealne, v praksi njihovo delovanje omejujejo neidealnosti detektorjev, omejena učinkovitost, mrtvi časi in klasični elektronski šumi. Zaradi teh vplivov surovi izhodi QRNG navadno niso povsem neodvisno niti enakomerno porazdeljeni(independent and identically distributed) (IID) [2, 5]. Zato so QRNG zasnovani kot *dva podsistema*: (i) kvantni vir entropije in (ii) *ekstraktor* naključnosti, ki iz nepopolnih vhodov izlušči skoraj uniformne bite z majhnim var-

nostnim parametrom ϵ (npr. Toeplitzovo univerzalno zgoščevanje, Trevisanov ekstraktor) [1, 4, 6]. Kakovost vira se v praksi kvantificira preko *min-entropije* surovih podatkov, ocenjeno konzervativno in v skladu z modelom naprave [1]. Standard NIST SP 800-90B predpisuje metodologijo ocenjevanja entropijskih virov tako v IID kot ne-IID režimu, z zbirko statističnih in napovednih testov; končna ocena je minimum delnih ocen in je namerno konservativna [6, 7, 8].

Statistični testi (NIST STS, Dieharder, TestU01, PractRand) so *potrebni*, vendar *ne zadostni* pokazatelji kakovosti: deterministični PRNG z neznanim semenom lahko prestane testiranje z zbirkami testov, ne da bi vseboval pravo entropijo [2, 8]. Še izraziteje to pokaže t. i. napad »pomnilniškega ključa«, kjer nasprotnik proda pomnilnik predizdelanih bitov, ki prestanejo vse statistične preizkuse, a so zanj popolnoma znani [5]. Zato mora certificiranje QRNG združiti (i) *model* vira in oceno min-entropije, (ii) *postprocesiranje* z dokazljivimi ekstraktorji in (iii) *statistične teste* ter nadzor delovanja v realnem času [1, 2, 4, 6].

Posebno mesto imajo pristopi z **od naprav neodvisnimi generatorji** (device-independent quantum random numbers generator (DI-QRNG)), kjer naključnost in zasebnost izhajata neposredno iz opazovanih kvantnih korelacij — kršitev Bellovih neenakosti [2, 5]. Takšna certificiranja ne zahtevajo modela notranjega delovanja naprav in so odporna na širok razred skritih pomanjkljivosti; praktična ovira pa so eksperimentalne zahteve (odpravljanje vrzeli detekcije in vrzeli lokalnosti) in trenutno nizke hitrosti [5, 6]. V raziskavah so se uveljavile tudi *delno* neodvisne sheme, ki z omejenim naborom preverljivih predpostavk znižajo zahtevnost, a ohranijo kvantitativna jamstva [2]. V vseh primerih ostaja statistična validacija in ocenjevanje entropije osrednji del certificiranja [9].

Struktura dela. Najprej opredelimo vlogo naključnosti in potrebo po močnih virih entropije v kriptografiji, znanosti in industriji [2, 3, 4, 6]. Nato predstavimo razrede generatorjev (PRNG, TRNG) ter temeljne koncepte QRNG, vključno z radioaktivnimi, atomskimi in optičnimi pristopi ter s kvantnimi računalniki kot viri naključnosti [1, 2, 6, 10]. Sledi poglavje o *ekstraktorjih entropije* in postprocesiranju, zlasti o univerzalnem zgoščevanju (Toeplitz) in von Neumannovem ekstraktorju [1, 4, 6]. V nadaljevanju obravnavamo *statistične teste* in *certificiranje* (NIST SP 800-90B, NIST STS, Dieharder, TestU01, PractRand) ter na koncu izpostavimo DI-QRNG vlogo Bellovih testov in praktične vrzeli [2, 5, 7, 8, 9].

Cilji eksperimentalnega dela. V nalogi želimo empirično preveriti tezo, da uspešno prestani statistični testi naključnosti sami po sebi ne zadostujejo kot dokaz kriptografsko relevantne entropije. V raziskavi smo primerjali izhod kvantnega generatorja naključnih števil z izhodom determinističnega generatorja in pokazali, da lahko oba dosežeta primerljive rezultate na statističnih testih, čeprav deterministični generator zaradi znanih začetnih pogojev ne izkazuje nepredvidljivosti. S tem smo utemeljili, da je za zanesljivo presojo entropije nujna analiza in modeliranje samega izvora ter pravilno postprocesiranje, ne zgolj ugodni rezultati testov naključnosti.

2. Teoretično ozadje

2.1 Potrebe po naključnosti

2.1.1 Zgodovinski in teoretični okvir

Vprašanje naključnosti ima dolgo zgodovino in pomembno vlogo tako v znanstvenem kot tudi praktičnem kontekstu. Po strogi definiciji so števila povsem naključna, če jih ni mogoče napovedati ne uporabniku generatorja ne kateremukoli opazovalcu, obenem pa imajo vse potrebne statistične lastnosti [6]. Že s tem je jasno, da je generiranje naključja brez zunanjega vira entropije nemogoče [5].

Kvantna fizika je na to področje prinesla novo perspektivo. Zaradi lastnosti, kot je kvantna prepletenost, je načeloma mogoče izdelati certificirani kvantni generator naključnih števil, ki izpolnjuje strogo definicijo naključnosti [6]. S tem je kvantna teorija postavila temelje za boljšo, varnejšo in teoretično utemeljeno naključnost, ki presega omejitve klasičnih metod [2].

2.1.2 Sodobne aplikacije naključnih števil

Naključna števila imajo danes ključno vlogo v številnih področjih znanosti, tehnologije in vsakdanjega življenja. Njihova uporaba se v grobem deli na tri glavne kategorije: kibernetska varnost, igralništvo ter raziskave in razvoj [6].

V kriptografiji naključna števila predstavljajo osnovni gradnik sodobnih varnostnih sistemov. Pravilno generirana naključna števila zagotavljajo zaščito pred sistematičnimi napadi, omogočajo varno izbiro ključev, sejnih vrednosti in inicializacijskih vektorjev ter se uporabljajo v številnih protokolih, med drugim pri digitalnem podpisovanju, vrednostih *nonce* in dokazih z ničelnim znanjem [2, 6]. Ključno je, da so ta števila ne le enakomerno porazdeljena, ampak tudi nepredvidljiva, in sicer tako vnaprej kot za nazaj: poznavanje dela zaporedja ne sme omogočiti napovedovanja prihodnjih ali rekonstrukcije preteklih vrednosti z boljšimi možnostmi od naključnega ugibanja [2]. V praksi večina obstoječih PRNG teh zahtev ne izpolnjuje, kar pomeni, da niso primerni za kriptografske namene. Posebej pomembna je zanesljivost naključnosti tudi v kvantni kriptografiji, kjer napačno izbrane baze meritev lahko vodijo do ranljivosti protokolov, kot je BB84 [2].

V igralništvu je glavna motivacija uporabe generatorjev naključnih števil zagotavljanje pravičnosti, kar je posebej pomembno za državne loterije in druge regulirane igre na srečo. Podobno si tudi v tehnologijah veriženja blokov ponudniki prizadevajo izboljšati varnost in transparentnost z uvedbo kvantnih generatorjev naključnih števil [6].

Tretje pomembno področje predstavlja znanstvena in industrijska raba naključnih števil, zlasti v Monte Carlo simulacijah in drugih stohastičnih metodah. Te metode zahtevajo dolge nize kakovostnih naključnih števil, pri čemer pa vprašanje zasebnosti ni ključno. Zato na tem področju zadostujejo tudi javno dostopni nizi

števil, kar pomeni, da raziskave in razvoj sicer močno uporabljajo naključnost, a hkrati ne predstavljajo glavnega tržnega gonila razvoja kvantnih generatorjev [6].

2.1.3 Pomen izboljšane naključnosti

Naključna števila predstavljajo temeljni element sodobnih aplikacij, kjer so varnost, nepristranskost in zanesljivost ključnega pomena. Njihova vloga je bistvena v kriptografiji in kvantni distribuciji ključev, saj omogočajo zaščito občutljivih podatkov in dolgoročno varnost komunikacijskih sistemov. Poleg tega omogočajo transparentne postopke v reguliranih okoljih, kot so športna tekmovanja, igre na srečo in javne storitve, ter nepristranske in ponovljive rezultate v eksperimentalni znanosti [3, 4].

Skratka, potrebe po naključnosti presegajo zgolj tehnične zahteve. Predstavljajo temelj zaupanja v sodobne varnostne protokole, poštenost družbenih procesov in zanesljivost znanstvenih rezultatov. Ker pa večina obstoječih metod za generiranje naključnih števil ne zagotavlja vseh zahtev, bo v nadaljevanju smiselno podrobneje predstaviti obstoječe pristope k generiranju — od PRNG do TRNG — in njihova razmerja do kvantnih virov.

2.2 Vrste generatorjev

2.2.1 Uvod in klasifikacija

Generatorje naključnih števil običajno razvrstimo v dve glavni skupini: *programske* in *strojne* [1, 6]. Programski generatorji so PRNG, katerih izhod je deterministično izračunan in zgolj posnema naključnost, medtem ko strojne naprave označujemo kot TRNG, ker črpajo entropijo iz fizičnega pojava [6]. Johnston [1] opozarja, da je izraz »generatorji pravih naključnih števil« pogosto uporabljen, a ni najbolje definiran, saj obstajajo tudi kriptografsko varni psevdonaključni generatorji CS-PRNG, ki dajejo izhode z zelo dobrimi lastnostmi.

2.2.2 Bistvene zahteve najboljših generatorjev

Za najzahtevnejše namene (kriptografija, znanost) naj generator izpolnjuje naslednje pogoje[6]:

1. **enakomernost (uniformnost)**: vsi nizi se pojavljajo z enako verjetnostjo;
2. **skalabilnost**: če niz prestane testiranje, to velja tudi za njegov poljuben del;
3. **konsistentnost**: ključne lastnosti (npr. entropija) se ohranjajo skozi čas;
4. **nepredvidljivost naprej** (*forward unpredictability*): tudi ob popolnem poznavanju algoritma in *vseh* preteklih izhodov ni mogoče napovedati *naslednjega* bita bolje kot z ugibanjem ($\approx 1/2$)[1, 6];
5. **nepredvidljivost nazaj** (*backward unpredictability/backtracking resistance*): tudi če napadalec razkrije trenutno notranje stanje, ne more rekonstruirati *preteklih* izhodov niti prvotnega semena; v praksi se po razkritju stanje hitro osveži z izbiro novega semena iz vira entropije [1, 6].

2.2.3 Psevdonaključni generatorji števil (PRNG)

PRNG uporabljajo deterministične postopke za razširitev kratkega začetnega *semena* v dolgo zaporedje bitov, ki navzven sledi izbrani statistični porazdelitvi (v

praksi tipično enakomerni) [2, 6]. Njihove glavne prednosti so hitrost, nizka cena in dovolj dobra uporabnost v številnih kontekstih [5]. Varnost, zasebnost in »navidezna naključnost« pri psevdonaključnih generatorjih temeljijo na predpostavkah o omejeni računski moči napadalca [5]; hkrati pa se pri zahtevnih aplikacijah izrecno zahteva neodvisnost od kateregakoli opazovalca. Neodvisnost od napadalca pomeni, da generirani naključni nizi ne razkrivajo nobenih informacij, ki bi jih zunanji opazovalec lahko uporabil za njihovo napovedovanje.

Standardni gradniki in stanje. Depolli *et al.* [6] navaja naslednje sestavne dele: (i) notranje stanje (seme), (ii) funkcije za inicializacijo/deinicializacijo in testiranje neoporečnosti stanja, (iii) funkcijo za generiranje naslednjega izhoda, ki tudi posodobi stanje, ter (iv) mehanizem periodičnega osveževanja semena iz zunanjega vira entropije. Izhod dobrega PRNG-ja je načeloma napovedljiv le ob poznavanju algoritma *in* trenutnega stanja; stanje pa je tipično opisano s semenom, ki enolično določa tako preteklost kot prihodnost zaporedja [1, 6].

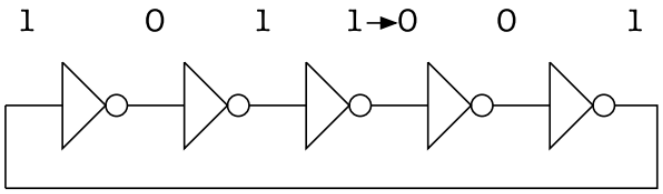
Kriptografsko varni PRNG (CS-PRNG)

PRNG delimo na *kriptografsko varne* in *ne-kriptografske*. Za Kriptografsko varne generatorje naključnih števil (CS-PRNG) sta ključni zahtevi [1]: (i) *nepredvidljivost naprej* in (ii) *nepredvidnljivost nazaj*. Ma *et al.* [4] poudarjajo, da so PRNG na osnovi računske zahtevnosti visoko razviti, a njihova naključnost ni informacijsko-teoretično dokazljiva; deterministično algoritem ostane načeloma razrešljiv ob dovolj veliki računski moči, kar je pri nekaterih aplikacijah problematično. Depolli *et al.* [6] dodajajo, da moramo pri CS-PRNG upoštevati možnost delnega vpogleda ali vpliva napadalca na vir entropije, zato je ocenjevanje dosegljive entropije in njeno konservativno izkoriščanje nujno. Poudarjajo, da so testi naključnosti potrebni, a sami po sebi niso zadostni za dokaz nepredvidljivosti. Čeprav CS-PRNG proizvaja deterministična zaporedja, ponuja formalna jamstva o težavnosti napovedovanja nadaljnjih izhodov [1].

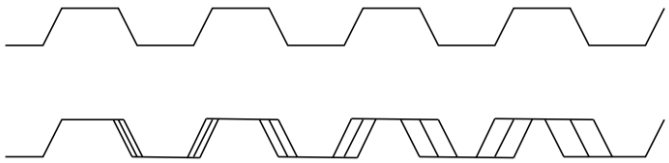
2.2.4 Generatorji pravih naključnih števil (TRNG)

TRNG izkoriščajo težko napovedljive fizične procese (npr. meteorološke pojave ali premikanje miške) [5] in *nimajo* notranjega stanja, od katerega bi bil odvisen izhod; naključnost črpajo neposredno iz fizičnega vira entropije [6]. Sestavljeni so iz *nedeterminističnega vira* in *determinističnega ekstraktorja* naključnosti, ki iz morebiti pristranih meritev izlušči bite, ki so bližje enakomerni porazdelitvi; vir mora biti stabilen, neodvisen od okolice in nespremenljiv na dolgih časovnih skalah [6].

Kaotični in oscilatorski TRNG. Kaotični generatorji temeljijo na deterministčnih, vendar nelinearnih procesih s *praktično* nepredvidljivim dolgoročnim gibanjem (npr. Chuaovo vezje, atmosfersko radiofrekvenčno šumenje) [6]. Najbolj razširjeni so *oscilatorski TRNG*, kjer ključni vir entropije izvira iz *trepetanja* (*jitter*) faze/frekvence zaradi elektromagnetnih (EM) interferenc, fluktuacij napajanja, termičnih fluktuacij ipd. [6]. »Najpreprostejši oscilatorji so krožni oscilatorji (*ring oscillators*) iz verige lihega števila inverterjev, sklenjenih v krog« [6]. Frekvenco določa zakasnitev prehoda skozi logična vrata in dolžina verige; elektronski šum to zakasnitev modulira, zato se perioda akumulativno spreminja. Pri vzorčenju faze v ustreznih intervalih dobimo podatke z entropičnimi lastnostmi, kjer časovni zamiki med cikli tipično približno sledijo normalni porazdelitvi [1].



Slika 2.1: Delovanje obročnega oscilatorja z lihim številom inverterjev; diskontinuiteta potuje po obroču in povzroča prehode med 0 in 1. Vir: Johnston [1].



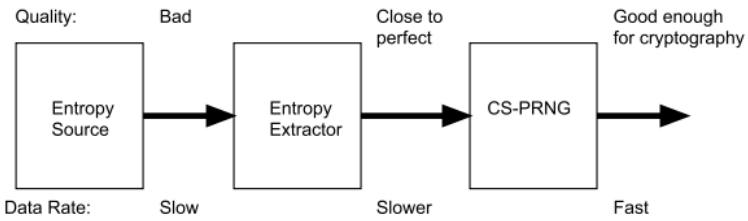
Slika 2.2: Valovna oblika obročnega oscilatorja; prekrivanje več sledi razkrije časovne zamike zaradi šuma. Vir: Johnston [1].

Praktična opozorila. Z redkejšim vzorčenjem se korelacije sicer zmanjšujejo, vendar ne izginejo, kar otežuje uporabo von Neumannovega ekstraktorja (prim. pogl. 2.4). Johnston [1] izpostavljajo *injekcijske napade* s periodičnim vsiljenim signalom prek napajanja ali EM-sklopitve, ki lahko sinhronizira oscilator in degradira naključnost ter nevarnost medsebojne sklopitve pri več verigah. Viri entropije so kvantni, klasično-fizikalni ali šumni; notranji šumi vključujejo Johnson–Nyquistov termični šum, zunanji pa EM motnje, fluktuacije napajanja in kozmične delce. Čeprav je izvor številnih šumov kvantnomehanski, proizvajalci ne jamčijo, da je entropija izključno kvantna (npr. Zenerjeve diode) [6]. Bistvo dobrega strojnega generatorja je jasno definiran fizikalni proces nastajanja entropije in obvladovanje vplivov nanj [6].

2.2.5 Primerjava in hibridni pristopi

Johnston [1] poudari, da TRNG-ji *vedno* vključujejo fizični vir entropije in strojno opremo za izluščanje bitov, medtem ko PRNG tega ne potrebujejo in so nujno deterministični. PRNG-ji sicer lahko uporabijo fizični vir za inicializacijo (seme), vendar to ni potrebno; takrat govorimo o *hibridnih* sistemih, ki združujejo fizični in programski del [1].

Na sliki 2.3 je prikazana sklopitev, kjer TRNG generira seme za CS-PRNG; pred podajo v PRNG je seme običajno potrebno dodatno obdelati, ker fizični generatorji pogosto ne dajejo popolnoma enakomernih porazdelitev (prim. pogl. 2.4) [1]. V simulacijah se TRNG redkeje uporabljajo (pogosteje za inicializacijo PRNG) zaradi počasnosti in otežene ponovljivosti rezultatov; popolna ponovitev bi zahtevala shranjevanje celotnih zaporedij, kar je v Monte Carlo okoljih tipično nepraktično [2].



Slika 2.3: Shema pretoka od vira entropije (*angl. entropy source*) prek ekstraktorja entropije (*angl. entropy extractor*) do *CS-PRNG*. Kakovost naključnosti se izboljšuje (slaba → skoraj popolna → dovolj dobra za kriptografijo), hitrost prenosa pa se giblje od počasne preko počasnejše do hitre. Vir: Johnston [1].

Sklep PRNG so hitri in praktični, TRNG pa nudijo neodvisno (fizikalno) nepredvidljivost in s tem močno osnovo za varnostno kritične aplikacije. Hibridne arhitekture združujejo prednosti obeh svetov [1], vendar zahtevajo skrbno ocenjevanje in ekstrakcijo entropije [6]. Ker klasični fizični viri ostajajo potencialno izpostavljeni neznanim napadom [6], je naraven naslednji korak obravnava *kvantnih* generatorjev naključnih števil (QRNG).

2.3 Kvantni generatorji naključnih števil

2.3.1 Uvod: temeljni principi in mesto med fizičnimi generatorji

QRNG izkoriščajo kvantne procese, katerih izidi so po kvantnomehanski razlagi *intrinzično* nedeterministični: naključnost vstopi ob aktu meritve, medtem ko je evolucija zaprtih sistemov deterministična [5, 6]. V praksi to pomeni, da naključni bit nastane kot rezultat posamezne kvantne meritve (npr. fotona v superpoziciji dveh poti ali dveh polarizacij), pri čemer verjetnosti izidov določajo izbrana bazna stanja za meritev [3].

Ker entropija v QRNG izhaja iz *fizičnega* (kvantnega) pojava, ti generatorji po klasifikaciji sodijo med strojne/fizikalne generatorje, tj. v družino TRNG [6]. Tipične realizacije vključujejo radioaktivni razpad (časovne intervale dogodkov), razcep enega fotona na delilniku žarka ali polarizacijskem delilniku, štetje fotonov v fiksnih oknih ter fazni šum laserjev; v vseh primerih se analogni kvantni signal digitalizira in po potrebi obdela z ekstraktorjem, da dobimo uniformne bite [2, 6].

Za razliko od drugih TRNG je pri QRNG jasno, od kod izvira njihova naključnost, kar olajša certificiranje. Napake je lažje zaznati in nadzirati v realnem času; naprednejše (raziskovalne) oblike omogočajo, da uporabniku ni treba zaupati proizvajalcu, nizi pa so certificirano zasebni. Tudi hitrost, velikost in poraba energije govorijo v prid QRNG; največja ovira ostaja cena [6].

Ključna prednost QRNG pred klasičnimi pristopi je konceptualna utemeljitev naključnosti: kvantni izidi so v temelju nepredvidljivi, zato je naključnost načeloma možno obravnavati tudi informacijsko-teoretično [4]. To odpira pot k strožjemu *certificiranju* naključja, v skrajnem primeru tudi v od naprav neodvisnih shemah, kjer sklepamo neposredno iz opaženih kvantnih korelacij [3, 5]. V nadaljevanju najprej predstavimo fizikalne vire in merilne sheme, nato pa obdelavo in certificiranje, ki sta nujna za praktično, robustno in ponovljivo generiranje naključnih bitov [2, 4].

2.3.2 Osnove kvantne mehanike za QRNG

QRNG temeljijo na osnovnih postulatih kvantne mehanike, kjer je ključna razlika do klasičnega sveta v superpoziciji stanj in v tem, da naključnost vstopi ob izvedbi meritve. Osnovna enota je kvantni bit (kubit) z baznima stanjem $|0\rangle$ in $|1\rangle$; splošno stanje zapišemo kot

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1, \tag{2.1}$$

meritev v računski bazi pa da izid 0 ali 1 z verjetnostima $|\alpha|^2$ in $|\beta|^2$ [3, 11]. Časovno evolucijo zaprtih sistemov opisujejo deterministične unitarne transformacije; *naključnost* se pojavi šele pri meritvi (Bornovo pravilo) [6, 11].

Za QRNG je posebej nazorna fotonska realizacija kubita prek baze: $H \equiv |0\rangle$ in $V \equiv |1\rangle$. Če pripravimo foton v stanju $(|H\rangle + |V\rangle)/\sqrt{2}$ in merimo v bazi $\{H, V\}$ (npr. s polarizatorjem in dvema detektorjema), sta izida enako verjetna (1/2–1/2) in posamezne meritve niso napovedljive; v nasprotju s klasičnimi sistemi (npr. »met kovanca«), kjer bi popolno znanje začetnih pogojev v principu omogočilo determinističen opis [3]. Porazdelitev izidov lahko aktivno nastavimo z izbiro merilne osnove (npr. rotacija polarizatorja), s čimer vplivamo na $|\alpha|^2$ in $|\beta|^2$ [3].

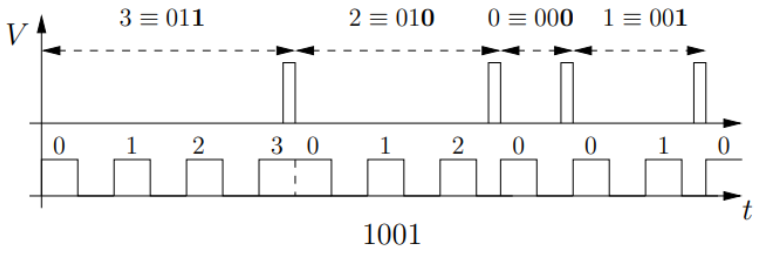
Kvantna prepletenost uvaja korelacije, ki jih ni mogoče reproducirati s klasičnimi skritimi spremenljivkami. Tipičen primer je Bellovo stanje

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.2}$$

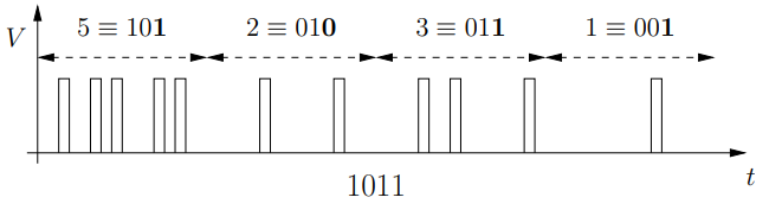
ki ob ustreznih meritvah vodi do kršitev Bellovih neenakosti [11]. Takšne *nelokalne* korelacije zagotavljajo, da izidov meritev ne more vnaprej poznati noben (morebitni) opazovalec. Na tem temelji *od naprav neodvisno* generiranje naključnih števil: v DI-QRNG se naključnost in zasebnost certificirata neposredno iz opazovane kršitve Bellovih neenakosti, brez zaupanja v notranjost naprav. Omogočata tudi postopke raztezanja naključnosti, kjer se iz majhne začetne zaloge naključja pridobi večja količina naključnih bitov [3].

2.3.3 QRNG na osnovi radioaktivnega razpada

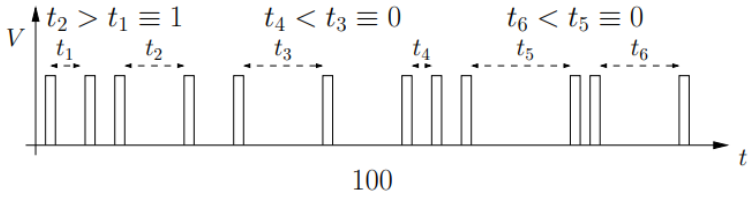
Prvi praktični QRNG so kot vir entropije uporabili radioaktivni razpad, zaznan z Geiger–Müllerjevimi (G–M) cevmi: časi med dogodki sledijo eksponentni porazdelitvi, število razpadov v intervalu pa Poissonovi porazdelitvi; dogodke pretvorimo v bite [2, 6]. Pogosti postopki pretvorbe so: *(i) metoda hitre ure*, kjer se ob dogodku odčita vrednost števca z visoko frekvenco (slika 2.4); *(ii) metoda počasne ure*, kjer se prešteje število pulzov v fiksnem intervalu (slika 2.5) in *(iii) primerjava dveh zaporednih intervalov*, t_1 proti t_2 (slika 2.6) [2].



Slika 2.4: Metoda hitre ure: števec teče z visoko frekvenco in se ob dogodku prebere.



Slika 2.5: Metoda počasne ure: število pulzov v intervalu določi izhod (npr. pariteta).



Slika 2.6: Metoda časovnih intervalov: bit je določen s primerjavo t_1 in t_2.

Omejitve in nadgradnje. Glavne omejitve so nizka bitna hitrost (tipično do nekaj 100 kb/s) ter zahteva po radioaktivnem izvoru; mrtvi čas detektorja in degradacija polprevodniških senzorjev pa vplivata na robustnost [2, 6]. Pristranskosti se odpravljajo s parnostjo, pri čemer se iz vsake izmerjene vrednosti uporabi le informacija o tem, ali je število sodo ali liho. S tem se iz eksponentno porazdeljenih časovnih intervalov pridobi enakomerno porazdeljen bit [2]. Takšni QRNG pogosto služijo kot inicializator PRNG [2].

2.3.4 QRNG na osnovi spinske polarizacije

Kvantna naključnost se lahko črpa iz kolektivnega *spinskega šuma* v razredčenih plinih alkalijskih kovin. Atomsko paro (npr. cezijevo) osvetlimo z laserjem, naključna nihanja kolektivne spin-polarizacije vplivajo na polarizacijo prepuščene svetlobe, ki jo zaznamo in pretvorimo v električni signal z naključno komponento; naključnost izhaja iz kvantnega šuma atomskih spinov [6, 10].

2.3.5 Kvantni računalniki kot QRNG

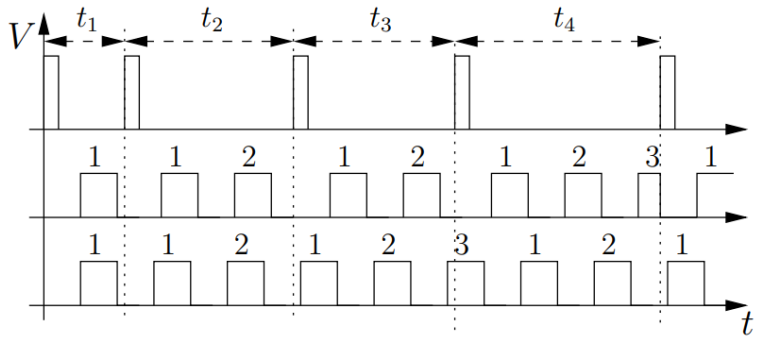
Kvantni računalnik lahko deluje kot QRNG tako, da iz kvantne superpozicije in meritve neposredno izdela naključne bite. Najpreprostejši je t. i. Hadamardov protokol: vse kubite pripravimo v stanju $|0\rangle$, na vsak kubit uporabimo Hadamardova vrata (nastavijo superpozicijo $|0\rangle$ in $|1\rangle$), nato pa vse kubite izmerimo. Vsaka meritev da 0 ali 1 z verjetnostjo približno 1/2, zato dobimo binarni niz naključnih bitov. Slabost tega pristopa je občutljivost na napake v realnem procesorju (priprava stanj, delovanje vrat, meritev), ki lahko porušijo idealno enakomerno porazdelitev izidov in zmanjšajo entropijo niza [6].

2.3.6 Optični QRNG

Optični QRNG temeljijo na kvantni naravi svetlobe oz. fotonov [6]. Večina sodobnih implementacij uporablja laserske izvore, LED-svetilke ali enofotonske izvore ter detektorje, kot so fotopomnoževalke (PMT) ali lavinske fotodiode (SPAD); sistemi dosegajo hitrosti od nekaj Mbps do desetine Gbps [2].

Delitev poti in polarizacija. Najenostavnejša zasnova uporablja vir posameznih fotonov, delilnik svetlobe (angl. beam splitter) in dva prostorsko ločena detektorja posameznih fotonov (SPD). Uravnotežen delilnik klasično svetlobo razdeli 50/50; če v delilnik vstopi en foton, nastane superpozicija dveh poti, meritev v enem izhodu pa povzroči klik z verjetnostjo 1/2, ki ga preslikamo v bit (npr. $D_0 \to 0$, $D_1 \to 1$). Ob enakomernem toku fotonov dobimo idealno nepristranski binarni niz [2, 6]. Alternativa je uporaba polarizacijskih stanj: foton v linearni superpoziciji (npr. 45°) usmerimo na polarizacijski delilnik (PBS), ki horizontalno/vertikalno komponento vodi na različna SPD. Verjetnosti izhodov so 1/2-1/2, zato so biti nepristranski [2, 6]. Različice vključujejo tudi večkratno razvejanje poti (W-stanja) in integrirana optična vezja, ki iz ene meritve izluščijo več bitov [2].

Časovne metode. Druga velika skupina optičnih QRNG izkorišča naključne *čase zaznave* fotonov. Ker časi prihodov pri šibkih virih sledijo eksponentni porazdelitvi, lahko primerjamo dva zaporedna intervala (t_1, t_2) in definiramo bit ($t_2 > t_1 \Rightarrow 1$, sicer 0). Alternativno lahko fotone vzorčimo v časovne razdelke (parni/neparni) ali pa uporabimo spodnje bite digitaliziranih časov in jih »pobelimo« s kriptografskimi funkcijami. Beljenje (*whitening*) je postopek, pri katerem iz surovega (morda pristranskega ali koreliranega) niza bitov pridobimo niz, ki je bližje enakomerno porazdeljen in statistično neodvisen [1, 2]. Ključna omejitev teh metod je mrtvi čas detektorjev, ki uvaja antikorelacije med sosednjimi biti. Te vplive lahko omilimo z uporabo resetirnih ur, ki se ob vsakem detekcijskem pulzu ponastavijo, kot prikazuje Slika 2.7. V tem primeru primerjava zaporednih intervalov omogoča generiranje uniformnih bitov, saj se zmanjša pristranskost zaradi omejene časovne ločljivosti [2].



Slika 2.7: Shema generiranja naključnih bitov na osnovi časovnih razlik zaznav. Detekcijski pulzi sprožijo štetje urinih ciklov. Ura je lahko neodvisna (spodaj) ali resetirna (sredina). Primerjava zaporednih intervalov ($t_2 > t_1$, $t_4 > t_3$) določi vrednosti bitov. Vir: Herrero-Collantes in Garcia-Escartin [2].

Štetje fotonov. Podobno kot pri radioaktivnih generatorjih lahko v fiksnem intervalu T štejemo fotone; število zaznav sledi Poissonovi porazdelitvi, iz katere izluščimo bite (npr. parnost števila zaznav) ali celo več bitov na meritev z ustreznim grupiranjem izidov in uporabo najmanj pomembnih bitov števca [2].

Vakuumske fluktuacije. Homodinska detekcija meri kvadrature elektromagnetnega polja in izkorišča Gaussovsko porazdeljeni kvantni šum: lokalni oscilator (laser) se zmeša z vakuumom na uravnoteženem delilniku, signala dveh detektorjev se odštejeta, rezultat pa se digitalizira in z ekstraktorjem entropije pretvori v bite.

Implementacije dosegajo Gbps in se dodatno izboljšajo s stisnjenimi vakuumskimi stanji (višja kvantna entropija v merjeni kvadraturi) [2].

Fazni šum laserjev. Fazni šum (difuzija faze) enomodne laserske svetlobe je kvantnega izvora; z neuravnoteženim Mach–Zehnderjevim interferometrom fazo pretvorimo v amplitudo in iz vzorčenih napetosti po postprocesiranju dobimo bite. Posebej učinkoviti so pulzni laserji, kjer vsak pulz zaradi spontane emisije začne z novo naključno fazo; interferenca zaporednih pulzov omogoča hitro in skoraj uniformno porazdelitev izhodov (več deset Gbps). Hibridne sheme, ki kvantni šum kombinirajo s kaotično dinamiko z optičnim povratnim vezjem, dosegajo stotine Gbps, a tam večina nepredvidljivosti izvira iz deterministčnega kaosa (fizikalni PRNG) [2].

Praktični viri: LED in SPAD. Poleg (dražjih) enofotonskih virov in vrhunskih detektorjev je mogoče uporabiti *zelo kratke svetlobne pulze iz LED* kot kvantni vir: spontana emisija je kvantnomehanski proces, število fotonov na pulz pa fluktuira Poissonsko. *SPAD* deluje na osnovi fotovzbuditve nosilcev in ima naključno uspešnost zaznave posameznih fotonov. LED in SPAD tako prispevata dodatne *kvantne* izvore entropije; dodatno entropijo zagotavljata še časovna naključnost emisije in končna natančnost detekcije [6].

Omejitve, kalibracija in zasebnost. Mrtvi čas, naknadni dogodki (*afterpulsing*), temni dogodki in neuravnoteženost kanalov/detektorjev povzročajo pristranskosti in korelacije; nujna sta modeliranje in kompenzacija (kalibracija pragov, uravnoteženje, naknadna obdelava) [2]. Naprave lahko kažejo *spominske učinke*, kar ustvarja skrite korelacije [5]. Zasebnost izhodnih bitov v standardnih optičnih QRNG tipično predpostavlja čistost stanj in odsotnost sklopitve; za *certificirano* naključnost so potrebne *napravno-neodvisne* sheme na osnovi kršitve Bellovih neenakosti [5].

2.3.7 Od naprav neodvisni QRNG (DI-QRNG)

Od naprav neodvisni DI-QRNG zagotavljajo protokole, kjer naključnost (in zasebnost) certificiramo zgolj iz opazovanih kvantnih korelacij, npr. z dokazljivo kršitvijo Bellovih neenakosti, ob minimalnih predpostavkah (veljavnost kvantne fizike ipd.) in brez zaupanja v notranjost naprav (obravnava kot »črne škatle«) [5, 6]. Kršitev implicira čistost stanja (nekoreliranost z okoljem) in prepletenost, kar je osnova od naprav neodvisnega generiranja in razširjanja naključnosti (*angl. randomness expansion*; več v pogl. 2.5) [5].

2.3.8 Primerjava QRNG in TRNG

Von Neumannovo razlikovanje, da je kvantna naključnost *individualna* (tudi posamezen elektron je v osnovi naključen), klasična pa *ansambelska* (reducibilna na variacije v ansamblu), izostri konceptualno prednost QRNG pred klasičnimi TRNG - QRNG izkoriščajo fundamentalno kvantno naključnost in omogočajo višjo raven zaupanja ter lažje certificiranje [12]. V preglednici 2.1 so povzete ključne razlike [3].

Tabela 2.1: Primerjava tradicionalnih TRNG in QRNG [3].

Lastnost	**TRNG**	**QRNG**
Vir entropije	Kompleksni fizični procesi in delna nevednost o stanju.	Fundamentalna kvantna naključnost.
Enostavnost certificiranja	Preverjanje približnih modelov; posredna potrditev.	Certificiranje iz preverljivih kvantnih procesov/korelacij.
Odpornost proti manipulaciji	Občutljivi na okoljske vplive in manipulacije vira.	Zaščita prek osnovnih zakonitosti kvantne mehanike.
Kakovost entropije	Pogosto potrebna ekstrakcija.	Visoka že na izvoru; DI-pristopi dajejo certificirano zasebnost.
Hitrost	Zelo visoka z združevanjem virov.	Visoka; omejena z detekcijo in optiko.
Velikost	Od čipa do namiznih naprav.	Od integriranih čipov do laboratorijskih DI-postavitev.

Sklep QRNG nudi fizikalno utemeljeno nepredvidljivost in bolj neposredno certificiranje kot klasični TRNG. V praksi so ključni: (i) *modeliranje naprave*, (ii) *spremljanje delovanja v realnem času* in (iii) *naknadna obdelava/ekstrakcija* za pretvorbo surovega izhoda v uniformne bite (prim. pogl. 2.4) [2, 3, 4, 5].

2.4 Ekstraktorji entropije

2.4.1 Uvod

Surovi izhodi QRNG praviloma niso popolnoma uniformni in neodvisni (IID), saj se kvantni signal v praksi pomeša s klasičnimi šumi merilne verige (npr. analogno–digitalni pretvornik (ADC)) in z neidealnostmi detektorjev. Zato QRNG, podobno kot tudi TRNG, zasnujemo kot dva podsistema: *nedeterministični vir entropije* (kvantni pojav) in *deterministični ekstraktor*, ki iz nepopolnega vhoda izlušči skoraj uniformne bite [6]. Tudi če so podatki IID, so lahko *pristranski* (npr. $P(1) \neq 1/2$), a brez korelacij; v realnih napravah pa se pojavljajo še korelacije (mrtvi čas, spominski učinki), zato surovi izhodi brez naknadne obdelave niso primerni za kriptografsko rabo [1, 2].

Na konceptualni ravni ekstrakcijo utemeljuje *lema o ostanku ob zgoščevanju* (*angl. leftover hash lemma*): če vhodne podatke karakteriziramo z min-entropijo $H_{\min}$, lahko s primerno (običajno naključno izbrano) preslikavo izluščimo krajši izhod, ki je po variacijski metrikah *skoraj* uniformen [4, 6]. Ker deterministično algoritem ne more ustvariti več entropije, velja $m < n$; cilj je povečati *entropijo na bit*, ne pa absolutne entropije [1]. Standardi (npr. NIST SP 800-90A/B) ločujejo *entropijo* in *stopnjo entropije* (bits/bit) ter priporočajo kondicioniranje strojnih virov [1, 6]. V praksi splošna metoda za točno oceno $H_{\min}$ ne obstaja; zato uporabljamo konzervativne modele vira in napada, iz katerih izpeljemo varne spodnje meje, kakovost izhoda pa opišemo z varnostnim parametrom ϵ (manjše je boljše) [1, 4].

V nadaljevanju obravnavamo tri sklope metod postprocesiranja: *deterministične debiaserje*, *kombinatorje z več viri* ter *ekstraktorje s semenom* [1, 2, 4, 6].

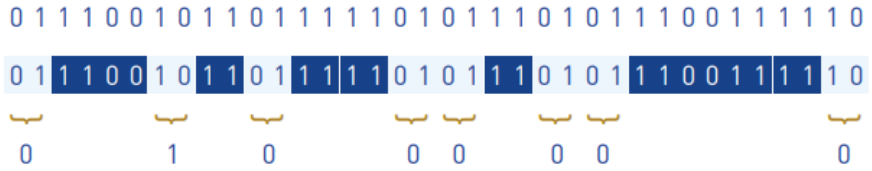
2.4.2 Deterministični ekstraktorji

Deterministični ekstraktor je preslikava

$$\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m, \tag{2.3}$$

ki brez dodatnega semena preslika vhod v krajši, bolj uniformen izhod. Privlačnost je operativna preprostost, a univerzalen deterministični ekstraktor za *poljubne* šibke vire ne obstaja; dosegljivi so pod omejenimi predpostavkami o vhodu (npr. IID, šibke korelacije) [2].

Von Neumannov debiaser. Algoritem zaporedje razdeli v pare (x_{2i-1}, x_{2i}) in uporabi pravila: $00, 11 \mapsto$ zavrzi; $01 \mapsto 0$; $10 \mapsto 1$. Tako odstrani pristranskost (ob predpostavki neodvisnih vhodnih bitov), a cena je *nepredvidljiva* in pogosto *krajša* dolžina izhoda (v najboljšem primeru približno polovična). Pri močno pristranskih ali koreliranih vhodih je izplen majhen in izhod lahko prazen [1, 6].



Slika 2.8: Von Neumannov debiaser: parjenje bitov in zavrženje enakih parov vodita do nepristranskega izhoda (ob IID predpostavki). Vir: Piani *et al.* [3].

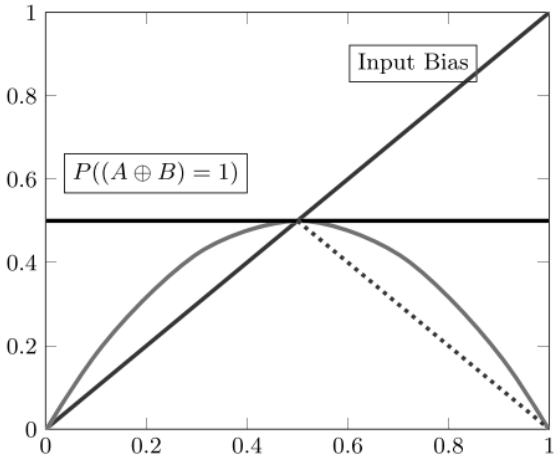
Peresova razširitev. Peresov debiaser nadgradi von Neumanna z več *globinami* obdelave: iz zavrženih parov sestavi nova zaporedja (npr. XOR parov in kodiranje $00{\to}0$, $11{\to}1$) in nanje rekurzivno ponovno uporabi isti postopek. Združevanje delnih izhodov poveča izplen in se z večjo globino hitro približa Shannonovi meji; globina pa ne sme preseči tiste, ki jo dopušča izmerjena min-entropija, sicer tvegamo prekomerno »iztiskanje« [1].

2.4.3 Ekstraktorji z več viri

Če imamo dva ali več *neodvisnih* šibkih virov, lahko s primerno kombinacijo dosežemo bistveno bolj uniformen izhod kot z vsakim virom posebej. Konceptualno preprost primer: vzamemo dva n-bitna vektorja u in v z zadostno min-entropijo in izračunamo **parnost** bitnega AND,

$$\langle u, v \rangle \;=\; \bigoplus_{i=1}^{n} (u_i \wedge v_i),$$

kjer je $\wedge$ logična konjunkcija (AND), $\oplus$ pa ekskluzivna disjunkcija (XOR). Ob neodvisnosti virov ima tako dobljen izhod dokazljivo dobre lastnosti [2]. V praksi se pogosto uporabi tudi **bitni XOR** dveh (ali več) tokov: praviloma *zmanjša* pristranskost in približa $P(1)$ proti $1/2$; popolna nepristranskost pa je zagotovljena, če je *vsaj eden* vhodov popolnoma uniformen. Pri koreliranih ali odvisnih virih se učinek poslabša, zato je ključno, da so viri res neodvisni in/ali da pred/poobdelava naslovi korelacije [1, 4].



Slika 2.9: Pristranskost izhoda XOR glede na pristranskost enega od vhodov. Prekinjena črta predstavlja idealen nepristranski primer ($P = 0,5$), medtem ko ukrivljena črta prikazuje dejanski rezultat XOR operacije. Vir: [1]

2.4.4 Ekstraktorji s semenom

Ekstraktorji s semenom dodajo vhodu kratek niz uniformnih bitov (seme), pogosto dolžine $O(\log n)$, in omogočajo *univerzalno* pretvorbo širokega razreda šibkih virov v skoraj uniformen izhod [2]. Varnost in kakovost izhoda sta formalno vezani na min-entropijo vhodnih podatkov in izbrani varnostni parameter ϵ [4].

Toeplitzovo zgoščevanje (univerzalno zgoščevanje)

Praktično najpogostejši je pristop *dvo-univerzalnega zgoščevanja* s *Toeplitzovimi* binarnimi matrikami. Toeplitzova matrika je določena s svojo prvo vrstico in prvim stolpcem (preostali elementi se ponavljajo po diagonalah), zato za matriko $T \in \{0,1\}^{m\times n}$ potrebujemo $n+m-1$ bitov semena [6]. Za blok vhodnih podatkov $x \in \{0,1\}^n$ izračunamo

$$y = Tx,$$

pri čemer so operacije nad biti realizirane z osnovnimi logičnimi vrati: množenje elementov kot AND, seštevanje po vrsticah kot XOR. Dolžino izhoda izberemo skladno s spodnjo mejo min-entropije k in varnostnim parametrom ϵ; tipično [4]:

$$m = k - 2\log_2\!\left(\tfrac{1}{\epsilon}\right).$$

Toeplitzovo zgoščevanje je atraktivno zaradi enostavne in hitre implementacije (tokovna izvedba, možnost recikliranja semena, paralelizacija) ter dokaznih lastnosti preko *leme o ostanku ob zgoščevanju* [2, 4]. V QRNG se uporablja tudi v ojačanju zasebnosti v kvantni kriptografiji [4].

Izbira dimenzij in korelacije. Ker so kratkosežne korelacije v vhodu pogoste (npr. zaradi mrtvega časa ali omejene pasovne širine ADC), dimenzije T izberemo tako, da jih preslikava učinkovito "odreže". V praksi uporabimo razmerje med številom vhodnih bitov N, izmerjeno min-entropijo $H_{\min}$ in velikostjo bloka b za določitev števila izhodnih bitov a [10]:

$$a = \frac{b\,H_{\min}}{N}.$$

Postopek se izvaja blokovno: za vsak b-bitni vektor $\mathbf{x}$ izračunamo $\mathbf{y} = T\mathbf{x}$ in izhode združimo. Tako dobimo kompresiran tok z višjo entropijo na bit ter zreduciranimi korelacijami [10].

Standardi in hibridne sheme. Standardi (npr. NIST SP 800-90B) pred uporabo zahtevajo kondicioniranje surovih bitov s kriptografskimi zgoščevalnimi funkcijami (npr. SHA-2), kar ustvari *hibrid* strojnega vira in programskega modula [6]. Samo zgoščevanje s SHA lahko zakrije težave (tudi *ničelno* entropijo na vhodu) in še vedno proizvaja psevdonaključne nize, ki prestanejo teste; Toeplitzovo zgoščevanje pa ohrani vidnost degradacij vira (odziv na spremembe $H_{\min}$) [6]. V praksi je smiselna kombinacija: Toeplitz za kompresijo in formalno ekstrakcijo, nato SHA za dodatno "glajenje" statistike izhoda [6].

Trevisanov ekstraktor

Trevisanov ekstraktor doseže močna teoretična jamstva z zelo kratkim semenom in odpornostjo tudi na *kvantne* napadalce; deluje kot *močan* ekstraktor, kar je ugodno za upravljanje semena [2, 4]. Slabost je visoka računska zahtevnost in posledično nižja hitrost realnih implementacij v primerjavi s Toeplitzovimi metodami. Zato je posebej zanimiv, ko je količina razpoložljivega semena strogo omejena ali ko sta dokazna moč in kvantna robustnost primarna cilja [4].

2.4.5 Praktična izvajanja in ocenjevanje

Za zanesljiv *end-to-end* sistem so ključni trije koraki [1, 2, 4, 6]: (i) realističen model naprave in konzervativna ocena $H_{\min}$ (vključno s prispevki klasičnega šuma); (ii) kontinuiran nadzor pristranskosti in korelacij (mrtvi čas, afterpulsing, neuravnoteženje kanalov) ter (iii) ekstrakcija z jasnim varnostnim parametrom ϵ in dokumentiranim upravljanjem semena (generacija, hramba, morebitno recikliranje). Vrednotenje naj ne temelji le na standardnih statističnih testih (ti so *potrebni*, ne pa zadostni), temveč tudi na preverjanju skladnosti z modelom entropije in na odzivu izhodov ob namernih spremembah vhodnega vira (npr. znižanje intenzitete, dvig temperature, injekcije šuma) [4, 6].

2.4.6 Povzetek

Ekstraktorji entropije so *nepogrešljiv* del QRNG: iz neidealnih, pristranskih in potencialno koreliranih surovih podatkov izdelajo skoraj uniformne, nepredvidljive bite. Deterministični debiaserji (von Neumann, Peres) so preprosti in koristni pod strogimi predpostavkami; kombinatorji z več viri (XOR, parnost AND) izkoriščajo neodvisnost virov; najmočnejša in v praksi najpomembnejša pa sta razreda *ekstraktorjev s semenom* — univerzalno zgoščevanje (Toeplitz) in Trevisan — ki ob pravilni oceni min-entropije in izbranem ϵ nudita formalna jamstva o kakovosti izhoda [1, 2, 4, 6]. V kombinaciji z nadzorom naprave in konservativnim modeliranjem entropije, ekstraktorji tvorijo jedro sodobnega postprocesiranja v QRNG.

2.5 Statistični testi in certificiranje generatorjev naključnih števil

2.5.1 Uvod

Kako lahko zagotovimo, da je izhod iz naprave res naključen? Acín in Masanes [5] poudarjata, da morajo biti biti porazdeljeni enakomerno in *nekorelirani z okoljem*,

kar vključuje tudi odsotnost povezave z morebitnim napadalcem. V praksi se uporabljajo statistični testi, a ostaja nejasno, kaj natančno pomeni »uspešen« prehod: zaradi omejene računske moči je *nemogoče* z gotovostjo potrditi, da je dano končno zaporedje zares naključno [5]. V skrajnem primeru bi bilo vprašanje podobno temu, ali je bit »0« bolj naključen od bita »1«; brez neizračunljive Kolmogorovove kompleksnosti za končne nize ni odločilnega kriterija [2]. Statistični testi pa kljub temu *zaznajo* sumljive strukture: če generator dosledno proizvaja več enic kot ničel, ali če se pojavljajo periodike, bo to razkrito v rezultatih testov [2, 5].

V nadaljevanju najprej uvedem osnovne pojme (uniformnost, IID, entropija, p-vrednost), nato povzamem glavne tipe testov (preverjanje pravilnosti algoritmov, uniformnosti in strukture, samopreizkus) in si ogledam standardizirane nabore testov(NIST STS, Dieharder, TestU01, PractRand). Osrednji del poglavja je namenjen *certificiranju* TRNG in zlasti QRNG, kjer so poleg testiranja ključni: model entropijskega vira, metodologija ocenjevanja entropije (npr. NIST SP 800-90B) in — pri napravno neodvisnih pristopih — verifikacija preko kršitev Bellovih neenakosti [1, 2, 4, 5].

2.5.2 Osnovni pojmi

Naključnost in lastnosti zaporedij

Statistične lastnosti naključnih nizov se kažejo v porazdelitvi in medsebojnih povezavah bitov. Ključna je *enakomernost* (nepristranskost), *skalabilnost* (poljuben podniz izpolnjuje iste statistične lastnosti), *konsistentnost* (stabilne entropijske značilnosti) in *nepredvidljivost* naprej/nazaj [6]. V kriptografskih aplikacijah je posebej pomembna nezmožnost napovedovanja in rekonstrukcije, saj neposredno vpliva na varnost [6].

Entropija

Shannonova entropija meri povprečno informacijo, pridobljeno ob razkritju izida X:

$$H(X) = -\sum_{x} p_x \log p_x, \tag{2.4}$$

in narašča z enakomernostjo porazdelitve [11]. Za varnostno oceno virov je uporabna tudi *min-entropija*,

$$H_\infty(X) = -\log_2 \big(\max_i P(x_i) \big), \tag{2.5}$$

ki je konzervativna mera »težavnosti ugibanja« najbolj verjetnega simbola [1]. Največje število skoraj uniformnih bitov, ki jih lahko izluščimo iz n-bitnega vhoda z min-entropijo k, je omejeno s k, ne glede na n [2]. V praksi se *ocena* entropije izvaja na *surovih* podatkih vira (pred postprocesiranjem), saj najbolj zvesto odražajo fiziko generatorja [1].

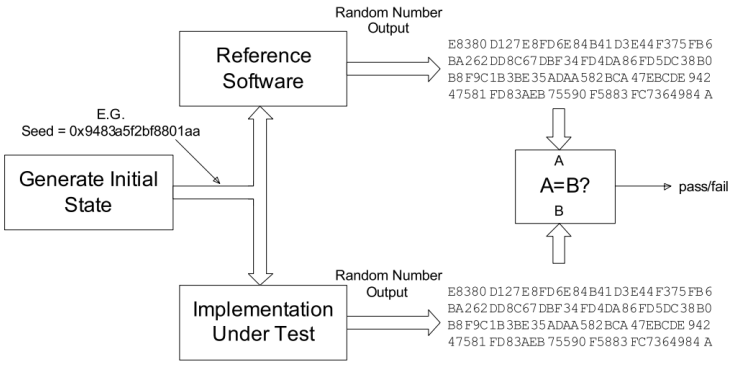
p-vrednost in statistična značilnost

Pri statističnem testiranju postavimo ničelno hipotezo, da je zaporedje generirano z idealnim IID virom. Izračunamo testno statistiko in p-vrednost, ki meri verjetnost, da bi »idealni« vir ustvaril tako (ali bolj) ekstremen rezultat. Zavrnitev ničelne hipoteze v vsaj enem testu pomeni odstopanje od IID (*neIID*) [2, 6, 8]. Različni testi so občutljivi na različne nepravilnosti (npr. pristranskost, periodike, serijske korelacije), zato se uporabljajo *zbirke* testov [2, 8].

2.5.3 Vrste statističnih testov

Kriptografska varnost je odvisna od nepredvidljivosti, zato je nujno preverjati *ustreznost* generatorjev. V praksi ločimo (i) *teste pravilnosti delovanja* (validacija implementacije) in (ii) *teste statističnih lastnosti* (uniformnost, struktura, entropija), dopolnjene s *samopreizkusi* za nadzor v realnem času [1, 2, 6, 8].

Testi pravilnosti algoritmov. Za PRNG (in programabilne dele TRNG/QRNG) se pogosto uporablja preizkus z znanimi odgovori (angl. Known Answer Testing): iz znanega semena nastane referenčni izhod, ki ga mora testirana implementacija *bitno* ponoviti; odstopanja razkrijejo napake v programju ali konfiguraciji [1]. Primer poteka prikazuje slika 2.10.



Slika 2.10: Preizkus z znanimi odgovori (KAT): primerjava izhodov referenčne in testirane implementacije. Vir: Johnston [1].

Testi uniformnosti in razlikovanja. *Distinguishability* testi preverjajo, ali je zaporedje ločljivo od idealne uniformne porazdelitve; vključujejo **frekvenčni test** (delež 0/1 in blokovne variante) ter **runs test** (dolžine zaporedij enakih bitov) [1, 2]. Namenjeni so predvsem zgodnjemu odkrivanju očitnih pomanjkljivosti in validaciji implementacij [1].

Testi odvisnosti in strukture. Med pogoste preizkuse sodijo **spektralni test** (periodike), **Maurerjev univerzalni test** (stisljivost) in **avtokorelacijski testi** (serijske korelacije) [2]. Ti ciljno detektirajo strukture, ki jih osnovni frekvenčni testi ne zaznajo.

Samopreizkus. Generatorji lahko *spontano* degradirajo; zato sistemi vključujejo sprotne teste (*angl. online health tests*), ki v realnem času spremljajo tipične anomalije (predolge serije, nenadna pristranskost, korelacije). NIST SP 800-90B opisuje pristope *blocking* (začasno hranjenje in odločanje o posredovanju) in *tagging* (označevanje vzorcev »v živo«) [1]. Ti testi *ne dokazujejo* naključnosti, temveč delujejo kot sistemi zgodnjega opozarjanja in dopolnjujejo *offline* analize [1, 2]. V QRNG so pogoste še *samopreverbe* (self-testing) vira entropije (npr. ocena minimalne entropije), ki ločujejo kvantno naključnost od tehničnega šuma in dinamično prilagajajo kompresijo v ekstraktorju [2].

2.5.4 Standardizirani nabori testov

Definicija naključnosti za končna zaporedja je problematična: število možnih vzorcev narašča eksponentno, zato popolnega preverjanja ni; to je v skladu z omejitvami

algoritmične (Kolmogorovove) definicije [9]. Zato zbirke, kot so NIST STS, Dieharder, TestU01 in PractRand, ponujajo *kompromis* med pokritostjo nepravilnosti in izvedljivostjo [8].

NIST SP 800-22. Standard opredeli cilje zagonskih testov: stabilnost porazdelitve skozi čas, neodvisnost od pozicije bita v nizu in odsotnost informacije v preteklih zagonskih sekvencah [3, 6]. Vendar je nabor v trenutni obliki *zastarel* in z znanimi programskimi težavami; raba je smiselna le, kjer je predpisana, sicer so priporočljive sodobnejše alternative [8].

Dieharder in TestU01. Dieharder je preprost in široko dostopen; rezultate podaja s p-vrednostmi, pri čemer so sumljive tako *zelo majhne* kot *zelo velike* vrednosti. Ekstremne p-vrednosti ali več hkratnih spodrsljajev kaže na strukture ali korelacije; ponovitve testov in naknadni KS-test porazdelitve p-vrednosti izboljšajo zanesljivost [8]. TestU01 (nabori Alphabit, BlockAlphabit, Rabbit; SmallCrush/Crush/BigCrush) velja za najcelovitejši akademski nabor brez »lažnih pozitivnih«; zahteva integracijo prek knjižnice, a omogoča zelo poglobljeno preverjanje [8].

PractRand. PractRand cilja na *zelo dolge* tokove (uporabno pri PRNG) in vključuje nove teste, ki se ne prekrivajo z Dieharder/TestU01; priporočljiva je *kombinacija* s TestU01 za širšo pokritost [8].

2.5.5 Testiranje in certificiranje TRNG in QRNG

Depolli *et al.* [6] ločijo teste pravilnosti delovanja (zagonski testi, testi popolne odpovedi, sprotni testi, testi na zahtevo) in teste *kakovosti* (ocena entropije vira in uniformnosti izhoda). Pri TRNG/QRNG je *certificiranje* neločljivo povezano z *ocenjevanjem entropije* na podlagi modela vira; statistični testi izhodov so *potrebni*, vendar *ne zadostni* [1, 2].

Napad s pomnilniškim ključem. Acín in Masanes [5] ponazorita, da lahko nasprotnik proda generator, ki je zgolj pomnilnik predizdelanih bitov; tak »izhod« bo prestal vse statistične teste, a ni *zaseben*. To poudari mejo testnih zbirk in potrebo po modelu vira ter (kadar je mogoče) neodvisnem certificiranju zasebnosti [5].

Modeli entropijskih virov in ocenjevanje entropije

Osnovna težava je, da iz *samosvojega* izhodnega toka ni mogoče razlikovati pravega naključja od kriptografsko varnega PRNG. Nepredvidljivost je *relacijska* lastnost glede na znanje opazovalca: kdor pozna ključ PRNG, izhod deterministično reproducira. Če pa poznamo *fizični model* vira, lahko utemeljimo spodnjo mejo $H_{\min}$ in na tej osnovi določimo varno stopnjo ekstrakcije [1]. V praksi se pogosto uporabi TRNG/QRNG kot entropijski vir za inicializacijo PRNG; s tem se zanesljivost opre na *fizični* model in *računsko* varnost PRNG [1].

NIST SP 800-90B. Metodologija predpisuje ocenjevanje kakovosti entropijskih virov v dveh režimih: IID in ne-IID. Pri IID se entropija oceni iz porazdelitve simbolov; pri ne-IID se uporabijo testi statističnih lastnosti (npr. najpogostejša vrednost, trki, Markovske verige, stisljivost) in *prediktorji* (napovedovanje naslednjega simbola iz zgodovine). Končna ocena je *minimum* vseh ocen (tudi začetne teoretične), kar je konzervativno in zmanjšuje tveganje precenjevanja [6, 7, 8]. Znano je, da je

ocena pogosto *nižja* od intuitivne, saj posamezne metode sistematično podcenjujejo entropijo [6, 8].

Raba entropijske ocene. V varni zasnovi določimo prag minimalne $H_{\min}$ (z varnostno rezervo), spremljamo degradacije (sprotni testi) in celotno verigo (vključno s postprocesiranjem), saj lahko odpove tudi ekstraktor. Bolj zahtevni testi lahko periodično tečejo na vgrajenem procesorju (npr. v FPGA), če dopuščajo časovne omejitve. Pri PRNG po ekstrakciji je smiselno govoriti o *računski* nepredvidljivosti (ne o min-entropiji izhoda), skladno s kriptografskim modelom [1].

Certifikacija QRNG

Samo s statističnimi testi ni mogoče dokazati *kvantnega* izvora naključnosti; klasični generator lahko namreč posnema rezultate. Brez dodatnih predpostavk je edino proizvajalec zagotovilo kakovosti izvora, kar pomeni, da je *zasebnost* za uporabnika nepreverljiva (primer napada s pomnilniškim ključem) [5]. To motivira *napravno neodvisne* (DI-QRNG) ali delno neodvisne sheme, kjer naključnost in zasebnost certificiramo *iz opazovanih kvantnih korelacij* [5, 6].

Bellovi testi in CHSH. Zgodovinsko izvirajo iz EPR-paradoksa in Bellovega izreka; kršitev Bellovih neenakosti izključuje lokalne skrite spremenljivke [2]. Pogosta formulacija je CHSH (Clauser–Horne–Shimony–Holt). Dva prostorsko ločena merilna sistema izbirata nastavitvi x, y in pridobita izida a, b; iz verjetnosti ujemanja/neujemanja izračunamo korelacijsko funkcijo I:

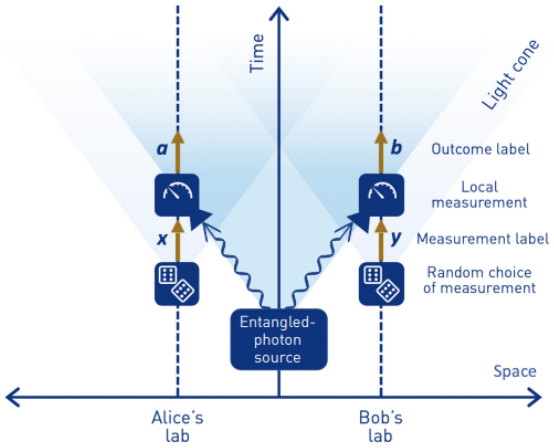
$$I = \sum_{x,y} (-1)^{xy} \big[P(a = b \mid xy) - P(a \neq b \mid xy) \big]. \tag{2.6}$$

Klasično je $I \leq 2$, kvantna mehanika pa dopušča $I > 2$ (do $2\sqrt{2}$). V kontekstu QRNG kršitev zagotavlja, da izidi *niso* razložljivi s klasičnimi modeli, zato so naključni in (ob dodatnih predpostavkah) zasebni [2].

Predpostavke in »vrzeli«. Za DI-QRNG so ključne predpostavke: (**C1**) *nekorelirani* vhodi (neodvisna izbira meritev) in (**C2**) *odsotnost izmenjave signalov* med napravama (ni komunikacije med generiranjem izhodov) [5]. Pri realnih napravah moramo zapreti *detekcijsko vrzel* (premajhna učinkovitost omogoča klasične razlage odstopanj), *lokalnostno vrzel* (prostorsko-časovna ločitev meritev) ter paziti na *vrzel svobodne volje* in *vrzeli kolapsa valovne funkcije* (naključnost izbire nastavitev in časovna ureditev dogodkov) [5]. Današnja fotonska tehnologija in optimizirane postavitve omogočajo zaprtje teh vrzeli, a zahteve so eksperimentalno zahtevne [2, 5].

Samopreverjanje in delna neodvisnost. Poleg popolnega DI-QRNG obstajajo *delno* neodvisne sheme, kjer se uvedejo omejene in *preverljive* predpostavke o napravi (npr. omejena energija), s čimer se znižajo eksperimentalne zahteve ob ohranitvi kvantitativnih garancij [2, 5]. V obeh primerih opazovana kršitev Bellovih (ali sorodnih) neenakosti prevede v *kvantitativno* oceno izluščljive naključnosti in vodi do *privacy amplification* v ekstraktorju [4].

Hitrost in uporabnost. Depolli *et al.* [6] poudarijo, da so DI-QRNG danes *počasni* (reda bit/s) in večinoma v demonstracijski fazi, medtem ko delno neodvisne sheme ponujajo boljše razmerje med zahtevnostjo in zanesljivostjo. V vseh primerih se certificiranje kvantne naključnosti *operativno* zreducira na statistične analize in entropijske ocene (vključno z robustnim postprocesiranjem) [4, 9].



Slika 2.11: Shema DI-QRNG: vir ustvarja prepletene fotone, ki potujejo v ločena laboratorija (Alice in Bob), kjer se izvajajo lokalne meritve z naključnimi nastavitvami. Korelacije izidov se uporabijo za test CHSH in certificiranje naključnosti. Vir: Piani *et al.* [3].

Zunanja (javno preverljiva) validacija. Ker kompleksnost celovitega testiranja narašča eksponentno, lokalni viri pogosto niso dovolj za zaznavanje dolgosežnih korelacij. Predlagani so protokoli, ki validacijo prenašajo na zunanje (oblake, celo kvantne računalnike) in omogočajo *javno preverjanje* brez razkritja nizov, kar razbremeni lokalne omejitve in krepi zaupanje [9].

2.5.6 Povzetek

Statistični testi so *nujni*, a *ne zadostni*. Deterministični PRNG z neznanim semenom lahko prestane testiranje, a ne vsebuje *prave* entropije. Zato uspešno prestani testi *postprocesiranih* nizov še ne pomenijo, da TRNG/QRNG ustvarja pričakovano mero naključnosti [2, 8]. Zanesljivo certificiranje zahteva kombinacijo: (i) *model* entropijskega vira in konzervativno oceno $H_{\min}$ (npr. po NIST SP 800-90B), (ii) *postprocesiranje* z dokazljivimi ekstraktorji (glej §2.4) ter (iii) *statistične teste* za odkrivanje odstopanj in degradacij. QRNG imajo dodatno prednost: naključnost izvira iz *kvantnih* procesov; v skrajnem primeru jo je mogoče *certificirati* preko kršitev Bellovih neenakosti, kar predstavlja najvišjo raven zaupanja, četudi je danes pogosto omejena s hitrostjo in eksperimentalno zahtevnostjo [2, 3, 5, 9].

3. Eksperimentalna zasnova in rezultati

V praktičnem delu preverjam, ali uspešno prestane zbirke testov naključnosti zadoščajo za utemeljitev prisotnosti kriptografsko relevantne entropije. Primerjam surove in obdelane izhode kvantnega generatorja naključnih števil in izhod deterministčnega generatorja s poznanim semenom. Na vseh vzorcih izvedem uveljavljene zbirke testov ter ocene min-entropije (NIST SP 800-90B) in pokažem, da lahko deterministični nizi dosegajo primerljive statistične kazalnike kot obdelani kvantni nizi, čeprav niso nepredvidljivi. S tem utemeljim, da sama statistična skladnost z zbirko testov ne predstavlja dokaza entropije brez modeliranja vira in ustrezne ekstrakcije.

3.1 Opis eksperimentalne postavitve

3.1.1 Kvantni pojav v viru *Qocka* in pridobivanje surovih podatkov

Za praktični del sem uporabil napravo *Qocka*, ki je zasnovana kot samostojen kvantni generator naključnih števil z vgrajenim postprocesiranjem in vmesnikom 1Gbps Ethernet. Naprava je opisana v dokumentaciji proizvajalca [13]; tukaj povzemam le ključne elemente z vidika vira entropije in pridobivanja surovih podatkov.

V uporabljenem viru naključnosti je temeljni mehanizem kvantna delitev posameznih fotonov na delilniku žarka z razmerjem 50:50. Foton, pripravljen v pulznem snopu, pri srečanju z idealnim delilnikom ne gre deterministično po eni poti, temveč je v superpoziciji obeh poti; šele detekcija povzroči kolaps v enega izmed izhodov. Tak dogodek predstavlja binarni poskus: zaznava na levem detektorju kodira bit 0, zaznava na desnem bit 1. Neodvisno od makroskopskih nastavitev izhaja nepredvidljivost iz same kvantne meritve, zato je ta mehanizem primeren za gradnjo QRNG. V napravi *Qocka* pulzno krmiljena telekomunikacijska LED (Broadcom HFBR–1505) generira kratke optične pulze, ki jih po vlaknu vodimo na delilnik (Thorlabs TH200FS1A) in nato na dva silicijeva fotopomnoževalna detektorja (onsemi MicroFC–10035–SMT). Ob zaznavi nastanejo napetostni pulzi na hitrem izhodu detektorja, ki jih zajamemo in nadalje obdelamo.

Za realizacijo enostavnega modela (»en foton – ena kvantna meritev«) je ključna pulzna ekscitacija vira. Višino in širino optičnih pulzov se nastavlja v dveh stopnjah: (i) z generiranjem $\sim 5\,\mathrm{ns}$ pulzov preko faznega zamikanja dveh 10 MHz PLL zank v FPGA in (ii) z nastavljivo prednapetostjo LED prek DAC (AD5691). Tako je mogoče znižati število fotonov na pulz in se približati režimu posameznih fotonov.

Detekcija je sinhronizirana s proženjem vira in poteka v časovnih oknih pri 10 MHz, pri čemer je vsako okno razdeljeno na deset intervalov. Aktivno *gate* okno se vključi le v pričakovanem intervalu prispetja pulza, kar bistveno zmanjša temna

štetja in naknadne pulze. Dogodke z dvojnim zadetkom ali brez zadetka zavržemo, kar daje zaporedje veljavnih, vendar še ne nujno nepristranih bitov.

Pridobivanje podatkov. Za potrebe tega dela sem iz naprave *Qocka* odjemal izključno dogodke iz kvantnega kanala. Ti nizi niso povsem surovi, saj so (zaradi pristranskosti) v strojni opremi že enkrat obdelani z von Neumannovim algoritmom, vendar sem jih kljub temu uporabil kot vhodne podatke. V nadaljevanju bom niz imenoval kot surov. Vzorce sem shranjeval v binarne datoteke in jih nato dodatno obdelal z lastnimi skriptami (glej poglavje 3.2.1).

3.1.2 Deterministični generator na osnovi SHA-256

Kot kontrolni (deterministični) vir sem uporabil preprost generator, ki izkorišča kriptografsko zgoščevalno funkcijo SHA-256 v *števnem* načinu [14]. Jedro konstrukcije je

$$R \;=\; \mathrm{Trunc}_n\Big(H(s \,\|\, \langle 0\rangle_{64}) \,\|\, H(s \,\|\, \langle 1\rangle_{64}) \,\|\, H(s \,\|\, \langle 2\rangle_{64}) \,\|\, \cdots\Big),$$

kjer je $H = \mathrm{SHA}{-}256$, s morebitni *prefiks* (npr. »seme«), $\langle i\rangle_{64}$ zapis števca i, $\|$ pa to da niza zlepimo skupaj. Funkcija $\mathrm{Trunc}_n(\cdot)$ na koncu izbere prvih n bajtov, ostale pa po potrebi prireže, in tako proizvede točno zahtevano število bajtov v izhodni datoteki. *Stanje* generatorja je zato zgolj števec i, ki se pri vsakem koraku poveča za 1, entropija izhoda pa v kriptografskem smislu obstaja le, če je s tajen.

Ta konstrukcija je tipičen *PRG* v slogu »hash–counter«: če bi bil s tajen, bi deloval kot CSPRNG, v našem nastavitvenem profilu pa je s znan, zato ima izhod *nič* kriptografske entropije. Prav ta lastnost je za eksperiment ključna: generator praviloma zaradi lastnosti SHA-256 doseže zelo dobre statistične kazalnike, vendar je popolnoma predvidljiv. S tem služi kot negativna kontrola pri tezi, da sama skladnost z zbirkami testov ni zadosten dokaz entropije.

3.2 Obdelava podatkov

V tem poglavju opisujem, kako sem pridobljene surove bite iz *Qocke* obdelal z ekstraktorji, da sem dobil nepristranske nize za nadaljnje testiranje. Opišem ekstrakcijo ter nize statističnih testov in oceno min-entropije, ki sem jih izvedel na surovih in obdelanih nizih.

3.2.1 Ekstrakcija naključnosti

V praktičnem delu sem surove bite najprej »pobelil« z *von Neumannovim* ekstraktorjem, nato pa izvedel še *Toeplitzov* 2:1 ekstraktor, enkrat na surovem enkrat pa na nizu obdelanim z von Neumannovim ekstraktorjem. Spodaj je kratek opis, kako sta skripti za ekstrakcijo zgrajeni in uporabljeni.

Von Neumannov ekstraktor

Bite obravnavam v parih: $01 \to 0$, $10 \to 1$, 00 in 11 zavrže. Če so pari dovolj neodvisni, dobimo nepristranski izhod. Pri idealnem vhodu preživi približno polovica parov, kar je okoli **25%** vseh vhodnih bitov.

Izvedba.

- Skripta bere vhodno datoteko *po kosih*, tako da ni potrebe po velikem pomnilniku, ki mi je delo z velikimi datotekami precej oteževal.

- Skripta uporablja *majhno tabelo LUT* (angl. *look-up table*), ki je vnaprej izračunana tabela. Ta za vsak možni bajt določi, katere in koliko izhodnih bitov ustvari, tako da pri obdelavi namesto bitno-po-bitnih izračunov le dostopam do tabele in rezultat hitro pripnem na izhod.
- Za vsak prebran bajt samo pogleda v LUT in sproti zapiše rezultate v izhodno datoteko, vmes pa izpisuje kratek napredek.

Toeplitzov ekstraktor

Vhodni niz x preslikamo v krajši niz y dolžine $m = \lfloor n/2 \rfloor$ s *Toeplitzovo* linearno preslikavo. V praksi deluje kot »enakomerno stiskanje« ob predpostavki dovolj velike min-entropije vhoda [1, 4].

Seme. Za diagonalo Toeplitzove matrike potrebujemo dolg bitni niz. Vzel sem surovi niz iz *ločenega* QRNG zajema (torej neodvisen od obdelovanega vhoda), ga obdelal z von Neumannovim ekstraktorjem in ga razširil na potrebno dolžino s SHAKE256, ki je raztegljiva izhodna funkcija (angl. extendable-output function - XOF) s poljubno dolgo izhodno dolžino [15]. Tako dobim enakomerno porazdeljene bite in ohranim neodvisnost semena od vhoda.

Ocena min-entropije pred ekstrakcijo (in prag za $m = n/2$). Pred izvedbo Toeplitzovega ekstraktorja sem surovi niz ovrednotil z oceno *min-entropije* z NIST SP 800-90B(več v poglavju 3.2.2). Naj bo zato $\hat{h}_{\min}$ (v bitih na bit) *konzervativna spodnja meja* min-entropije in $k = \lfloor n\,\hat{h}_{\min} \rfloor$ skupna min-entropija za n vhodnih bitov. Po *Leftover Hash Lemmi* za univerzalne preslikave—ki vključujejo tudi Toeplitzove matrike—mora za izhod dolžine m veljati

$$m \;\le\; k \;-\; 2\log_2\!\big(1/\varepsilon\big), \tag{3.1}$$

zato izberemo m skladno s ciljno napako ε (npr. $\varepsilon = 2^{-128}$) [4]. Ker Toeplitzova preslikava dimenzije $n \times m$ potrebuje seme dolžine $n + m - 1$ bitov, sem to tudi zagotovil pri konstrukciji matrike. Za moje podatke (n = 23,625,760,768) in $\varepsilon = 2^{-128}$ je prag na entropijo na bit po enačbi 3.1:

$$\hat{h}_{\min} \;\ge\; \tfrac{1}{2} + \frac{256}{n} \;=\; 0.5 + \frac{256}{23{,}625{,}760{,}768} \;\approx\; \mathbf{0.5000000108356},$$

zato je kompresija 2:1 (tj. $m = n/2$) utemeljena že pri vsaki $\hat{h}_{\min} > 0.5$ (ocenjeni z ustreznim, po potrebi *non–IID*, postopkom).

Zaradi velikosti datotek in omejitev pomnilnika sem za ekstrakcijo uporabil postopek, opisan v nadaljevanju.[1]

Izvedba. Toeplitzova preslikava je množenje z matriko, v kateri so vse diagonale konstantne; zaradi te strukture je popolnoma ekvivalentna *linearni konvoluciji* med vhodnim nizom x in vektorjem diagonale h (ta nastane iz semena dolžine $n+m-1$), kar v praksi pomeni, da lahko produkt $y = T_h x$ izračunamo kot $c = x * h$ in dobimo isti rezultat kot pri »teoretičnem« množenju matrike z vektorjem [4, 16]. Konvolucija (»drsenje« enega zaporedja prek drugega s seštevanjem prispevkov) se najučinkoviteje izvede v frekvenčni domeni s *FFT* (hitra Fourierjeva transformacija) in *IFFT* (njena inverzna): natančno velja

$$c = \mathrm{IFFT}\big(\mathrm{FFT}(x) \cdot \mathrm{FFT}(h)\big),$$

[1] Pri oblikovanju operativnega opisa in terminoloških pojasnil sem si pomagal z orodjem ChatGPT (OpenAI), postopek pa je povzet iz Hayashi in Tsurumaru [16].

kjer $\cdot$ pomeni *točkovno množenje* (množenje element–po–element) spektralnih koeficientov; ta postopek ne spreminja matematike, le zniža časovno zahtevnost iz $O(n^2)$ na $O(n \log n)$ [4, 16]. Nazadnje rezultat v tem odseku reduciramo glede na to, ali je vsota prispevkov soda ali liha, in s tem dobimo izhodne bite [16].

Dvojna ekstrakcija

Poleg neposredne obdelave surovega toka sem niz obdelan z von Neumannovim ekstraktorjem dodatno stisnil še s **Toeplitzom** (spet 2:1). Namen je, da najprej odstranim bias, nato pa z linearnim stiskanjem dodatno zmanjšam morebitne preostale neidealnosti. Za ekstrakcijo sem uporabil *drugačno*, neodvisno izbrano seme od novega vhoda, izvedel pa sem oba prej omenjena postopka.

Uporaba orodja za nabor idej

Občasno sem pri pisanju skript (npr. generiranje ogrodij funkcij, predlogi LUT-pristopa, zapis FFT-konvolucije) uporabil ChatGPT (OpenAI, model GPT-5 Thinking) kot pomoč pri oblikovanju izhodiščnih različic. Orodje ni bilo uporabljeno kot vir tehničnih dejstev; končno kodo in algoritme sem avtorsko pregledal, popravil in validiral na testnih primerih.

3.2.2 Statistični testi in ocena min-entropije

Tako obdelane kot tudi surov niz sem podvrgel v nadaljevanju omenjenim zbirkam testov in oceni min-entropije.

Dieharder Kot osnovni filter sem uporabil *Dieharder* (verzija 3.31.1) z osnovnimi nastavitvami in privzetim pragom p-vrednosti 0.01. Za vsak niz sem izvedel celoten nabor testov in zanemaril dokumentirano nezanesljive teste. Ta nabor sem izbral zaradi enostavne uporabe, njegove stabilnosti in razširjenosti v literaturi [8].

PractRand Kot dopolnilo sem uporabil *PractRand* (verzija 0.95) s privzetim pragom p-vrednosti 0.01. Ta nabor sem izbral, ker uporablja drugačne teste v primerjavi z Dieharder. Pomemben je bil tudi za boljšo oceno statističnih lastnosti psevdonaključnega niza, ker učinkovito testira neomejeno dolge sekvence [8].

NIST SP 800-90B *NIST SP 800-90B* je standardiziran postopek za ocenjevanje entropije vira. Ponuja dva pristopa: *IID* (za neodvisne in identično porazdeljene podatke) ter *Non-IID* (za realne vire z odvisnostmi). Standard kot rezultat podaja *konzervativno spodnjo mejo* (min-entropijo), definirano kot minimum prek več testov[8].

Za svoje podatke sem uporabil *Non-IID* postopek, ker podatki niso IID (kar sem tudi preveril, tako da sem pognal IID test in dobil zavrnitev predpostavke o IID nizu). Tako sem dobil oceno *spodnje meje entropije* svojega vira, ki je služila kot varna (konzervativna) ocena za nadaljnje varnostne odločitve (npr. izbira kompresije Toeplitzovega ekstraktorja). Prav tako sem za zagotovitev primerljivosti vse nize obrezal na dolžino najkrajšega, tako da dolžina vzorca ni mogla vplivati na ocene entropije.

3.3 Interpretacija rezultatov

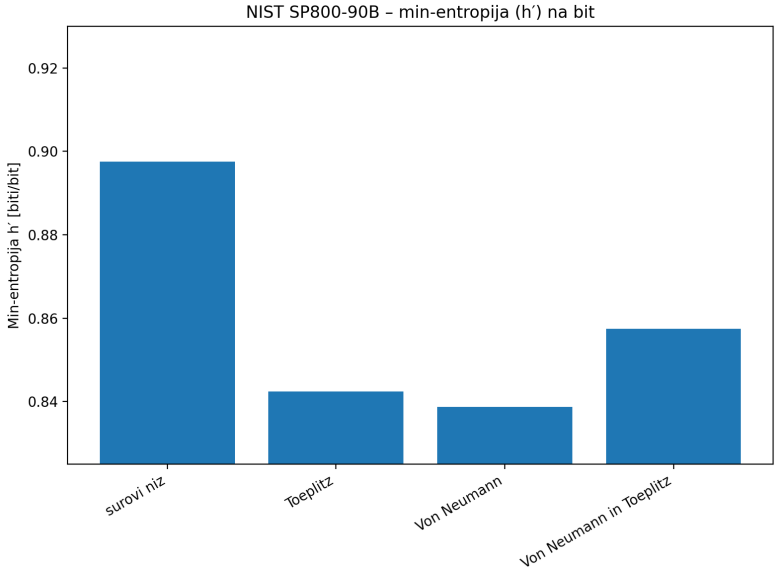
V tem poglavju so predstavljeni in interpretirani pridobljeni rezultati, pri čemer je analiza razdeljena na ocene entropije ter na rezultate statističnih testov naključnosti.

3.3.1 Analiza ocene entropije

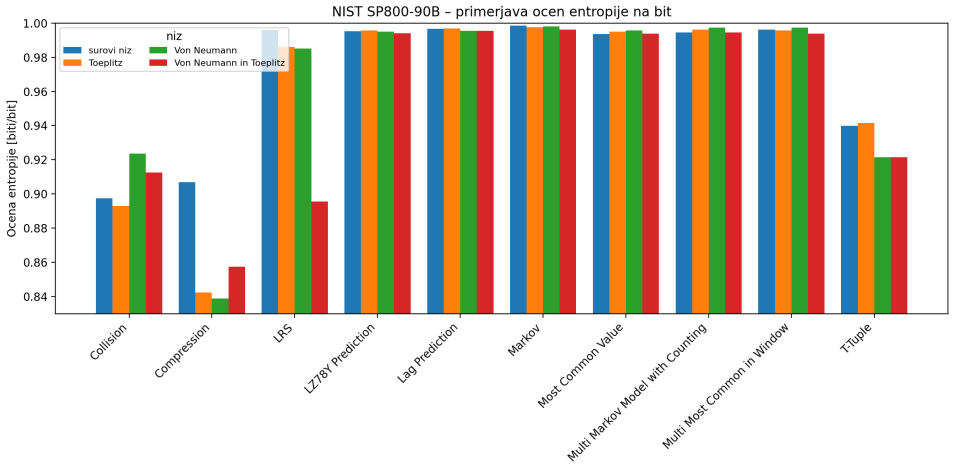
V splošnem bi pričakovali, da ima **surov niz** zaradi pristranskosti in korelacij nižjo oceno min-entropije na bit, medtem ko **kondicionirani nizi** (npr. von Neumann, Toeplitz matrika) dosegajo višje ocene, ker obdelava odstrani pristranskost in zmanjša odvisnosti. Naši rezultati pa pokažejo obratno: surov niz ima višjo min-entropijo/bit kot obdelani nizi.

V nadaljevanju sem na izhodu iz psevdonaključnega generatorja izvedel oceno entropije, kljub temu da ima izhod po teoriji nič entropije (znano seme). Dobljena vrednost je bila 0.8835 na bit, kar je zelo blizu vrednosti obdelanih kvantnih nizov (glej sliko 3.1). To kaže, da sama ocena min-entropije ne more razlikovati med dejansko entropijo in dobro statistično skladnostjo brez entropije.

Slika 3.2 prikazuje primerjavo vseh ocen po posameznih testih iz SP 800-90B, slika 3.1 pa povzetek končne min-entropije h' na bit za vse obravnavane nize.



Slika 3.1: Končna ocena min-entropije h' na bit za surovi in obdelane nize. Vidno je, da je surovi niz višje ocenjen kot obdelani.



Slika 3.2: Primerjava ocen entropije po testih NIST SP 800–90B za surovi niz in obdelane nize.

Za boljše razumevanje dobljenih rezultatov je smiselno podrobneje predstaviti posamezne teste, ki jih določa standard NIST SP 800–90B, ter pojasniti, kaj njihove ocene pomenijo za zaznano entropijo obravnavanih nizov.

Most Common Value (MCV). MCV ocena temelji na verjetnosti najpogostejšega simbola; min-entropija se definira kot $H = -\log_2(p_{\max})$ [7]. V naših rezultatih so vse vrednosti blizu ≈ 1, kar pomeni, da *bias* praktično ni prisoten.

Collision. Collision ocena izpelje entropijo iz pogostosti ponovitev enakih simbolov v zaporedju; manjše ujemanje simbolov pomeni višjo entropijo [7]. Pri nas se surovi niz in obdelani nizi ne razlikujejo bistveno, niz obdelan z von Neumannovim algoritmom je rahlo boljši, s Toeplitzovim pa nekoliko slabši.

Markov. Markov ocena upošteva verjetnosti za prehode med stanji (bitoma 0/1); večja determinističnost prehodov pomeni nižjo entropijo [7]. Vsi nizi dosegajo zelo visoke vrednosti, kar pomeni, da se zaporedje bitov obnaša skoraj kot povsem neodvisno (vrednost posameznega bita ni bistveno odvisna od prejšnjega).

Compression (Lempel–Ziv). Compression ocena meri stisljivost niza z LZ postopkom; večja stisljivost pomeni več struktur in zato nižjo entropijo [7]. Tu je opazna največja razlika: surovi niz doseže ~ 0.91, obdelani pa le ~ 0.84–0.86 (glej sliko 3.2).

t-Tuple in LRS. t-Tuple ocena gleda ponovitve vzorcev dolžine t, LRS pa *najdaljši ponovljeni podniz* [7]. Pri nas imata von Neumann in zlasti niz obdelan z von Neumannom in Toeplitzem nekoliko slabše vrednosti kot surovi niz.

Prediktorji (MCW, Lag, MultiMMC, LZ78Y). Ti testi merijo uspešnost različnih napovedovalcev naslednjega bita [7]. Vsi nizi so tu zelo visoki (~ 0.995–0.997), kar kaže, da ni praktične napovedljivosti.

Sklep

Surov vir je zelo kakovosten: brez pomembnega bias-a in brez smiselne napovedljivosti. Kondicioniranje z von Neumannom in Toeplitzom, ki sicer izboljšata slabše vire, tukaj ne prinese koristi. Razlike v ocenah, ki jih zaznajo *Compression*, *t-Tuple*

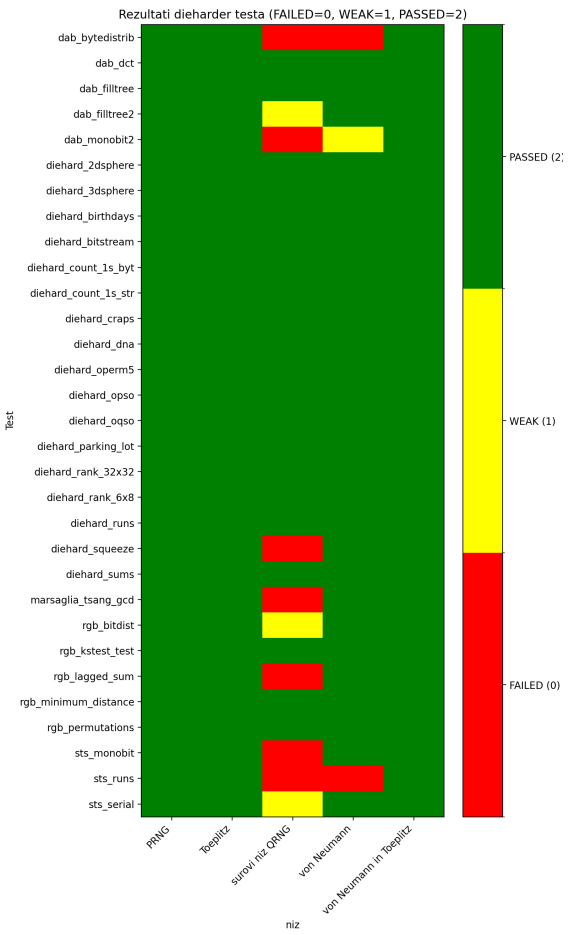
in *LRS* estimatorji, niso posledica dejanskih struktur v nizu, temveč predvsem značilnost metodologije NIST SP 800-90B. Ti estimatorji so namreč konservativni in pogosto podcenijo entropijo, tako da tudi za idealne nize vračajo vrednosti v območju 0.8–0.9. Enak rezultat (≈0.8–0.9) je bil dobljen tudi za PRNG niz, ki ima zaradi znanega semena teoretično nič entropije, a statistično deluje zelo dobro. To potrjuje, da razlike izhajajo iz konzervativnosti NIST ocen, ne pa iz dejanskih slabosti virov – vsi obravnavani nizi so v resnici kakovostni.

3.4 Statistični testi naključnosti

V prejšnjem poglavju smo obravnavali ocene min-entropije po metodologiji NIST SP 800-90B. Videli smo, da je imel surovi vir najvišjo oceno entropije na bit, medtem ko so obdelani nizi dosegli nekoliko nižje vrednosti. Pomembno pa je poudariti, da ocena entropije in uspešnost statističnih testov nista isto merilo kakovosti niza. Medtem ko SP 800-90B konzervativno ocenjuje *najslabši primer entropije*, zbirke testov, kot sta *Dieharder* in *PractRand*, preverjajo, ali niz »izgleda naključen« glede na širok nabor statističnih kriterijev [7].

3.4.1 Rezultati zbirke testov Dieharder

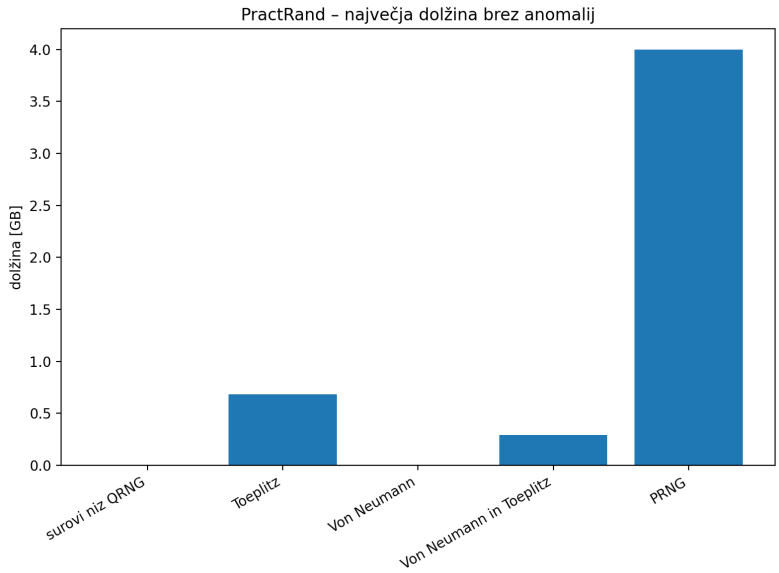
Na sliki 3.3 je prikazana toplotna karta rezultatov zbirke Dieharder. Vsaka vrstica predstavlja posamezen test, barve pa pomenijo: zelena = *PASS*, rumena = *WEAK*, rdeča = *FAIL*. Opazimo, da **surovi niz QRNG** pade na več testih (npr. *dab bytedistrib*, *sts monobit*), kar kaže na prisotnost struktur, ki jih SP 800–90B ni zaznal kot kritične. Tudi niz, obdelan samo z **von Neumannovim algoritmom**, pade na nekaj testih, kot so *sts runs* in *dabbytedistrib*. Razlog je v tem, da algoritem odstrani pristranskost tako, da zavrača določene pare bitov (00 in 11), s čimer spremeni porazdelitev dolžin zaporedij in frekvenco določenih vzorcev. Nasprotno pa obdelana niza s **Toeplitzem** in s **Toeplitzem po von Neumannovem ekstraktorju** prestaneta vse teste, saj taka ekstrakcija učinkoviteje odstrani prepoznavne strukture in izboljša statistični videz nizov.



Slika 3.3: Rezultati testov Dieharder za surovi in obdelane nize ter PRNG.

3.4.2 Rezultati zbirke PractRand

Na sliki 3.4 so prikazane največje dolžine zaporedij, pri katerih v PractRand niso bile zaznane anomalije. Vidimo, da niza obdelana s **Toeplitzem** in **von Neumannom ter Toeplitzem** nista pokazala anomalij skozi celotno razpoložljivo dolžino, podobno kot tudi referenčni niz iz **PRNG-ja**. Nasprotno pa sta surovi niz QRNG in niz obdelan samo z von Neumannovim algoritmom začela kazati anomalije bistveno prej. To pomeni, da so v teh nizih prisotne **statistične strukture ali ponavljajoči se vzorci**, ki jih PractRand zazna kot odstopanja od idealne naključnosti. Tak rezultat kaže, da zaporedje ne deluje več kot popolnoma naključno in da bi ga bilo mogoče v določenih situacijah ločiti od resnično naključnega niza.



Slika 3.4: Rezultati PractRand: največja dolžina niza brez anomalij.

3.4.3 Povzetek

Rezultati obeh zbirk testov kažejo, da učinkovito razkrivajo prisotnost strukturnih nepravilnosti v zaporedjih. Surovi niz QRNG in niz, obdelan le z von Neumannovim algoritmom, sta padla na več testih, kar pomeni, da vsebujeta statistične vzorce, ki odstopajo od idealne naključnosti. Nasprotno pa niza, obdelana s Toeplitzovo matriko in z zaporedno uporabo von Neumannovega ekstraktorja in Toeplitza, nista pokazala anomalij in sta uspešno prestala praktično vse preizkuse. Pomembno pa je poudariti, da tudi referenčni **PRNG** prestane vse statistične teste, čeprav je deterministično in ga je zato mogoče v celoti reproducirati. To jasno pokaže, da uspešno prestajanje statističnih testov samo po sebi še ne zagotavlja resnične naključnosti niza, temveč zgolj potrjuje, da niz nima prepoznavnih statističnih odstopanj glede na uporabljene kriterije.

3.5 Ugotovitve

Rezultati statističnih testov jasno pokažejo, da obstaja razlika med **oceno entropije** in **statistično naključnostjo**. Čeprav ima surovi vir najvišjo oceno min-entropije po SP 800-90B, vsebuje strukture, ki jih Dieharder in PractRand zaznata kot anomalije. Obdelani nizi pa dosegajo nižje ocene min-entropije, a vseeno uspešno prestanejo zahtevne statistične zbirke.

Še posebej pomembno je poudariti, da tudi referenčni **PRNG** prestane vse statistične teste, čeprav je povsem deterministično in ima v teoriji 0 prave entropije. To jasno pokaže, da **statistični testi sami po sebi niso zanesljiv kriterij za presojo kakovosti vira**. Njihova vloga je predvsem v tem, da pomagajo odkriti grobe napake v implementaciji, medtem ko mora kakovosten vir temeljiti na ustreznem stohastičnem modelu ter na eksperimentalnem preverjanju parametrov tega modela.

4. Zaključek

V tej nalogi sem obravnaval problematiko generiranja naključnih števil s poudarkom na kvantnih generatorjih in njihovi primerjavi z drugimi pristopi. Poudaril sem pomen naključnih števil v kriptografiji, varnostno kritičnih aplikacijah in znanstvenih simulacijah, kjer zanesljivost in nepristranskost tvorita osnovo zaupanja. Kvantna mehanika daje QRNG-jem posebno prednost, saj se opirajo na intrinzično nedeterministične procese, kar jih loči od klasičnih strojnih generatorjev in še bolj od psevdonaključnih generatorjev, ki temeljijo na deterministčnih algoritmih.

Eksperimentalni del je bil usmerjen v oceno kakovosti surovega kvantnega vira in obdelanih nizov s pomočjo von Neumannovega algoritma ter Toeplitzovega ekstraktorja. Rezultati so pokazali presenetljiv pojav: čeprav je imel surovi vir najvišjo oceno min-entropije po metodologiji NIST SP 800-90B, so statistični testi Dieharder in PractRand zaznali prisotnost struktur in anomalij. Nasprotno pa so obdelani nizi, ki so imeli nižje ocene entropije, prestali praktično vse teste. Dodatno se je izkazalo, da tudi PRNG, ki ima v teoriji nič prave entropije zaradi znanega semena, doseže podobne ocene entropije (≈ 0.88) in uspešno prestane vse statistične preizkuse. To potrjuje, da ocene po SP 800-90B pogosto podcenijo entropijo in da statistični testi sami po sebi ne povedo veliko o resnični kakovosti vira – njihova vloga je predvsem v preverjanju, da v implementaciji ni očitnih napak.

Iz tega sledi, da resna ocena kakovosti QRNG ne more temeljiti zgolj na statističnem videzu zaporedij, ampak mora biti zasnovana na ustreznem stohastičnem modelu vira in na eksperimentalnem preverjanju parametrov tega modela. Statistični testi služijo kot dopolnilo za odkrivanje grobih odstopanj, a niso merilo naključnosti. Eksperiment je tako pokazal, da QRNG ob ustrezni obdelavi podatkov lahko zagotovijo kakovostne vire, a njihovo vrednotenje zahteva previdnost in večplastni pristop.

V prihodnje se odpira prostor za razvoj od naprav neodvisnih kvantnih generatorjev, ki z izkoriščanjem Bellovih neenakosti omogočajo certificirano naključnost, ter za raziskave integracije QRNG z obstoječimi kriptografsko varnimi PRNG, da bi dosegli optimalno razmerje med hitrostjo, zanesljivostjo in varnostjo. Sklepno lahko povzamem, da QRNG predstavljajo obetavno in nujno tehnologijo prihodnosti: čeprav zahtevajo dodatno obdelavo in premišljeno vrednotenje, nudijo edinstveno lastnost – naključnost, ki izvira iz samih zakonov narave.

5. Literatura

[1] D. Johnston, *Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers* (Walter de Gruyter, 2018).

[2] M. Herrero-Collantes in J. C. Garcia-Escartin, *Quantum Random Number Generators*, Reviews of Modern Physics **89**, 015004 (2017).

[3] M. Piani, M. Mosca in B. Neill, *Quantum Random-Number Generators: Practical Considerations and Use Cases*, Teh. por. (evolutionQ, 2021) research report by evolutionQ, published January 13, 2021. Available online.

[4] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi in H.-K. Lo, *Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction*, arXiv preprint arXiv:1207.1473 (2013).

[5] A. Acín in L. Masanes, *Certified randomness in quantum physics*, arXiv preprint arXiv:1708.00265 (2017).

[6] M. Depolli, P. Jeglič, R. Novak, E. Zupanič in R. Žitko, *Stanje na področju generatorjev naključnih števil*, IJS (2022).

[7] E. Barker in J. Kelsey, *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST Special Publication 800-90B (National Institute of Standards and Technology, 2018).

[8] M. Depolli, P. Jeglič, R. Novak, E. Zupanič in R. Žitko, *Statistični testi za generatorje naključnih števil*, IJS (2024).

[9] J. E. Jacak, W. A. Jacak, W. A. Donderowicz in L. Jacak, *Quantum random number generators with entanglement for public randomness testing*, Scientific Reports **10**, 1 (2020).

[10] M. Koterle, S. Beguš, J. Pirman, T. Mežnaršič, K. Gosar, E. Županič, R. Žitko in P. Jeglič, *Mbit/s-range alkali vapour spin noise quantum random number generators*, EPJ Quantum Technology **11**, 1 (2024).

[11] M. A. Nielsen in I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010) 10th Anniversary Edition.

[12] A. Khrennikov, *Randomness: quantum versus classical*, arXiv preprint arXiv:1512.08852 (2015).

[13] R. Žitko *et al.*, *Kriptografsko varen generator naključnih vstevil "Qocka": Verzija 1.4*, Institut "Jožef Stefan", Ljubljana, Slovenija (2025), prosta licenca CC BY. Kontakt: rok.zitko@ijs.si.

[14] National Institute of Standards and Technology, *Recommendation for Key Derivation Using Pseudorandom Functions (KDFs)*, Teh. por. SP 800-108 (NIST, Gaithersburg, MD, 2009) opisuje KDF v *counter mode* z uporabo PRF (npr. HMAC-SHA-256).

[15] National Institute of Standards and Technology, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, Teh. por. FIPS PUB 202 (NIST, Gaithersburg, MD, 2015) definira XOF funkciji SHAKE128 in SHAKE256.

[16] M. Hayashi in T. Tsurumaru, *More Efficient Privacy Amplification with Less Random Seeds via Dual Universal Hash Function*, arXiv preprint (2015), version v5; used for Toeplitz/modified-Toeplitz properties and $O(n \log n)$ implementation details.