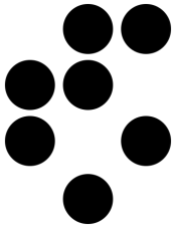


Stanje na področju generatorjev naključnih števil

Poročilo IJS

Poročilo IJS-CRP-V1-2119-P1
Verzija 1.0
18. oktober 2022

Ciljna skupina: razvijalci programske in strojne opreme, administratorji računalniških sistemov, strokovnjaki za varnost, uporabniki naključnih števil v znanstvene namene, delavci v loteriji

---

Izjava o omejitvi odgovornosti:
Poročilo upošteva tveganja, ki so bila znana v času objave tega poročila.

---

1. Uvod

Vprašanje, ali prava naključnost v naravi resnično obstaja, je eno izmed temeljnih znanstvenih vprašanj novejše dobe. Odgovor ima jasne posledice tudi za tvorbo naključnih števil za najbolj zahtevne aplikacije, denimo v kriptografiji. Po najbolj strogi definiciji so števila povsem naključna, če jih nikakor ne more napovedati niti uporabnik generatorja naključnih števil niti noben drug opazovalec. Takšna števila imajo vse potrebne **statistične lastnosti**, nezmožnost napovedovanja vseh drugih opazovalcev pa uporabniku jamči še **zasebnost** in zagotavlja varnost v kriptografski uporabi teh naključnih števil. Če je kvantna teorija pravilen opis našega sveta, za kar obstaja širok konsenz med znanstveniki, potem je načeloma možno izdelati napravo, **certificirani kvantni generator naključnih števil**, ki uporablja nedvomno najbolj zagoneten kvantnomehanski pojav kvantne prepletenosti in ki povsem zadosti tej strogi definiciji. (Za pionirske eksperimente, v katerih je bila kvantna prepletenost jasno demonstrirana in ki predstavljajo bistveno podlago za porajajoče se kvantne tehnologije, je bila nedavno podeljena Nobelova nagrada za fiziko leta 2022.) Ker so takšni generatorji še na zelo zgodnji stopnji razvoja in so zelo počasni, se v praksi uporablja vrsta drugih pristopov, ki temeljijo na drugih nenapovedljivih oz. težko napovedljivih fizikalnih pojavih, ki jih opisuje kvantna oz. klasična fizika, ali pa na deterministčnih algoritmih, ki so težko obrnljivi. Bistvene zahteve in lastnosti, ki jih mora imeti generator naključnih števil za najbolj zahtevne namene (kriptografija, znanost), so:

- **enakomernost** (uniformnost) - vsi nizi naključnih števil se morajo pojavljati z enako verjetnostjo;
- **skalabilnost** - če niz naključnih števil uspešno opravi preverjanje/testiranje naključnosti, mora to veljati tudi za poljuben del tega niza;
- **konsistentnost** - lastnosti generatorja naključnih števil (npr. entropija) se morajo ohranjati za vsa generirana števila;
- **nezmožnost napovedovanja v naprej** (angl. forward unpredictability) - na podlagi prejšnjega naključnega števila ali niza ne moremo napovedati naslednjega števila ali niza;
- **nezmožnost napovedovanja za nazaj** (angl. backward unpredictability) - na podlagi trenutnega naključnega števila ali niza ne moremo napovedati prejšnjega števila ali niza.

Cilj tega poročila je opisati stanje na področju različnih tipov varnih generatorjev naključnih števil, upoštevajoč tudi grožnje s strani porajajočih se kvantnih tehnologij, ter predlagati morebitne potrebne ukrepe.

1.1 Pomen naključnih števil v kriptografiji

Naključna števila so osnovni gradnik številnih kriptografskih postopkov. Nasprotnik lahko z razbitjem naključnosti popolnoma razvrednoti zaščito, ki je predmet kriptografskega postopka. Med bolj znanimi kriptografskimi postopki, ki so še posebej občutljivi na trdnost generatorjev naključnih števil, so:

- generiranje izzivov v protokolu izziv-odziv, ki so izmenjani na odprtem kanalu,
- izbira naključnih praštevil v številnih protokolih na osnovi modularne aritmetike,
- digitalno podpisovanje,
- izbira sejnih ključev v simetričnih varnostnih protokolih,
- izbira začetnih vektorjev in števil za enkratno uporabo,
- generiranje semen,
- zapolnitev podatkovnih blokov do zahtevane dolžine,
- dokazi z ničelnim znanjem.

Pravilno generirana naključna števila zagotavljajo varnost pred sistematičnim ugibanjem, ponovitvenimi in korelacijskimi napadi. Znanih je več varnostnih **incidentov**, ki so neposredno povezani s pomanjkljivo generiranimi naključnimi števili (denimo ranljivost v OpenSSL odkrita leta 2008 ali pa slabo generirani ključi RSA za Tajvanske pametne kartice) in tudi primer podtaknjenega namerno pomanjkljivega algoritma v uradnem standardu za generatorje naključnih števil (algoritem Dual_EC_DRBG). Tudi certificirani generatorji se lahko naknadno izkažejo za pomanjkljive: znan primer je deterministični generator naključnih števil, ki je bil del operacijskega sistema Windows 2000 [Dorrendorf 2007].

1.2 Osnovna načela delovanja generatorjev naključnih števil

Naključni niz
V tem razdelku bomo uporabljali naslednjo definicijo: niz je naključen, če ob podani poljubno dolgi zgodovini niza ne moremo napovedati vrednosti, ki bodo generirane v prihodnje.

Generator psevdo-naključnih števil (deterministični generator)
Generator psevdo-naključnih števil je algoritem, ki generira (uporabniku podaja) nize števil, ki izgledajo naključni, a so določeni algoritemsko, so torej deterministični. Če definicijo povežemo z zgornjo definicijo naključnih nizov lahko rečemo, da izhod dobrega generatorja psevdo-naključnih števil lahko napovemo le, če poznamo tako algoritem kot njegovo trenutno stanje. Stanje determinističnega generatorja je tipično definirano z enim samim številom – semenom. Seme enolično definira tako zgodovino generiranih števil, kot tudi njihovo prihodnost. Z vsakim novo generiranim številom se seme spremeni. Ob dovolj veliki zalogi vrednosti za seme (npr. 2^{128} vrednosti) in dovolj dobrem skrivanju vrednosti semena, lahko dober generator psevdo-naključnih števil služi tudi kot osnova za kriptografsko varen generator naključnih števil.

Generator pravih naključnih števil (nedeterministični generator)
Generatorji pravih naključnih števil nimajo notranjega stanja, od katerega bi bil odvisen njihov izhod. Namesto tega naključnost črpajo iz fizičnega **vira entropije**. Primeri fizičnih virov so kvantni viri, viri šuma in viri, pri katerih naključnost vnaša uporabnik s svojimi dejanji. Šum je tu izraz za neželene signale, ki se tipično obnašajo naključno in jih ni mogoče popolnoma izločiti iz meritev fizičnih količin. Generatorji pravih naključnih števil so sestavljeni iz dveh komponent: nedeterminističnega vira entropije in determinističnega **ekstraktorja naključnosti**. Vir entropije je osnovan na zajemanju šuma, ga ni mogoče upravljati, in generira števila z nepredvidljivo vrednostjo a potencialno neenakomerno porazdelitvijo. Zanj moramo predpostaviti (še raje pa dokazati), da ustvarja entropijo. Ekstraktor naključnosti vzame zajete vrednosti iz vira entropije in jih z matematično funkcijo pretvori v bite z enakomerno porazdelitvijo vrednosti oziroma jim poveča mero entropije na bit [Killmann 2011]. Izhod iz ekstraktorja je zato po številu bitov krajši od vhoda, ekstraktor torej na račun zmanjšanja števila bitov premakne njihovo porazdelitev bližje k enakomerni.

Testiranje generatorjev
Glede na izbrano definicijo naključnega niza je zastavljeno tudi preverjanje generatorjev naključnih števil. Primarno se preverjanje opravlja na izhodnem nizu generatorja, v katerem se išče **statistične anomalije**, ki bi jih bilo možno zlorabiti v namen napovedi naslednje generirane vrednosti. Primer je zbirka orodij TestU01 za empirično testiranje naključnih generatorjev. Orodja so dokumentirana in na voljo je izvorna koda za njihovo izvedbo, kar olajša in predvsem močno pohitri razvoj in testiranje generatorjev naključnih števil.
V grobem delimo obstoječe teste generatorjev v dve skupini: v teste prvega reda in teste drugega reda. Testi prvega reda delujejo na enem nizu naključnih števil, katerega statistično preverjajo. Testi drugega reda pa delujejo na skupini nizov naključnih števil in preverjajo njihove (ne)odvisnosti. Vsi testi so zasnovani tako, da vračajo *p*-vrednost, preko katere se odločimo, ali ničelno hipotezo za posamezen test zavrnemo ali ne. Pri tem je ničelna hipoteza, da generator deluje pravilno, torej da ustvarja nekorelirana števila z uniformno porazdelitvijo.

Napotki za izvedbo

Splošni napotki za izvedbo (implementacijo) generatorjev psevdo-naključnih števil so zbrani v viru [Barker 2015] in črpajo iz dolgoletnega razvoja na področju. Standardno arhitekturo generatorja psevdo-naključnih števil sestavljajo:

- Notranje stanje (seme), ki je osrednji element generatorja.
- Funkcije za inicializacijo, deinicializacijo in testiranje neoporečnosti stanja generatorja. Initializacija nastavi vrednost semena ter ostale parametre generatorjevega notranjega stanja, deinicializacija nastavi nevtralno (ničto) stanje, testiranje neoporečnosti pa preverja, če generatorjevo trenutno notranje stanje dovoljuje pravilno generiranje novih števil.
- Funkcija za generiranje naslednjega naključnega števila. Generiranje vedno ustvari enako število novih bitov na izhodu in spremeni notranje stanje generatorja. Za generiranje več števil se podano funkcijo kliče večkrat zapored.
- Mehanizem za povezovanje z virom entropije za periodično nastavljanje nove vrednosti semena generatorja.

Predstavljena arhitektura, napotki za implementacijo in uporabo so vsi zasnovani z varnostjo na prvem mestu, to pomeni s skrivanjem stanja generatorja, inicializacijo z entropijo iz različnih virov ipd. Za izvedbo algoritma so predlagane in podrobno opisane kriptografske zgoščevalne funkcije, ki nimajo znanih inverznih funkcij, blokovne šifre (angl. block cyphers) in teoretični številski problemi (na primer problem diskretnega logaritma eliptičnih krivulj). Te izvedbe predstavljajo trenutno najmodernejše prijeme za izvedbo generatorjev naključnih števil, tako deterministčnih kot nedeterminističnih, v slednjem primeru v vlogi ekstraktorja naključnosti.

Snovanje sistemov, ki naj tvorijo naključen in nepredvidljiv niz števil, je zahtevno, a s sledenjem podanim smernicam se lahko izognemo znanim pastem v razvoju in zmanjšamo verjetnost za napake v izvedbi algoritmov. Vir entropije zagotavlja nedeterminističnost generatorja, ki je pomembna za uporabo v kriptografiji. Dobre prakse za izbiro virov entropije so zbrane v [Turan 2018].

Vire entropije modeliramo kot digitalen vir šuma, povezan na pogojevalnik signalov (angl. conditioning) in logiko za testiranje neoporečnosti vira. Digitalni viri šuma so lahko že izvirno digitalni ali pa so sestavljeni iz analognega vira šuma in analogno-digitalnega pretvornika. Nadalje je vir šuma lahko fizičen ali nefizičen.

Pogojevalnik signalov je deterministična funkcija zadolžena za izenačevanje verjetnosti različnih vrednosti signala na izhodu iz vira entropije ter za zagotavljanje izhoda s konstantnim in vnaprej definiranim številom bitov na posamezno vrednost izhodnega signala. Tipično se za pogojevalnik uporabljajo preizkušene kriptografske funkcije [Turan 2018].

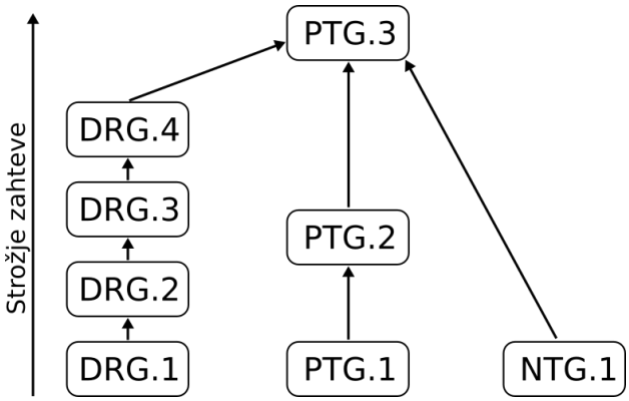
O šumu

Viri fizičnega šuma izkoriščajo šum navzoč v vseh digitalnih senzorjih. Kot primer vzemimo pametni telefon, ki ga postavimo na trdno podlago in prebiramo vrednosti iz njegovih senzorjev premikanja, tipično senzorjev pospeškov (pospeškometrov); kljub mirovanju se odčitki hitro spreminjajo. Razloga sta dva: ambientalni šum v merjeni količini (podlaga se zaradi seizmičnih aktivnosti in drugih vplivov ves čas mikroskopsko premika) ter omejena natančnost uporabljenega senzorja (elektronika in elektromehanski elementi senzorja imajo omenjeno kvaliteto izdelave, omejeno natančnost odčitavanja ter delujejo pod nepopolnimi merilnimi pogoji). Ambientalni šum je možen

kandidat za fizični vir naključnosti, a ima svoje pomanjkljivosti. Na pospeškometre, denimo, vpliva seizmična aktivnost Zemlje do te mere, da jo je mogoče meriti in izločati iz celotnega šuma. Naključna števila, ki bi preveč temeljila la na okoljskem šumu bi zato bila ogrožena. Napadalec na pospeškometer bi, na primer, lahko omejil nabor možnih generiranih števil danega generatorja za nazaj ob znani pretekli seizmični aktivnosti. Prav tako bi lahko s fizičnim dostopom do senzorja vplival na generator v trenutku vzorčenja entropije s premišljenim premikanjem senzorja.
Drugi tip šuma, ki lahko služi kot vir entropije, je šum v odčitavanju senzorjev. Tipično vnašajo velik del šuma v meritve digitalnih senzorjev analogno-digitalni pretvorniki (ADC). Napake na odčitkih ADC (oziroma šum ADC) so lepo porazdeljene in obstajajo dobro raziskane tehnike izboljšave, ki temeljijo na zajemanju dodatnih vzorcev ter njihovem povprečenju za doseganje večje natančnosti. Navkljub tehnikam za odpravo šuma je le-ta vseeno dovolj zaznaven na senzorjih, ki jih najdemo v mobilnih napravah. Najbolj nazoren primer so slike iz vgrajene kamere pri nizki osvetlitvi. Tudi ta tip šuma ima svoje slabosti, saj je lahko precej odvisen od temperature, nihanja napajalne napetosti, magnetnega polja v okolici, sevanja ozadja, ipd. Na vse to bi napadalec s fizičnim dostopom do vira entropije lahko vplival.
Navkljub možnosti vpliva na vse oblike fizičnega šuma (razen kvantnega) ostaja fizični šum dober kandidat za generatorje pravih naključnih števil. Napadalec ima vendarle na vire šuma večinoma zelo omejen vpliv. Nadaljujmo primer s pospeškometri – četudi bi napadalec imel možnost apliciranja natančno določenih pospeškov na napravo s pospeškometrom, bi se izmerjene vrednosti pospeškov še vedno razlikovale od apliciranih zaradi omejene točnosti pospeškometrov, zaradi nedoločljivosti točnega časa, ko pospeškometer zajame posamezen vzorec signala, ter ker na zajete vrednosti vplivajo tudi mehanske lastnosti mobilne naprave, katerih ni mogoče simulirati dovolj natančno, da bi lahko modelu primerno priredili zunanje vplive. Odčitkov senzorjev torej zaradi naštetih omejitev napadalec ne more nikoli popolnoma predvideti, lahko pa si zmanjša zalogo možnih vrednosti odčitkov. A ob pravilni oceni entropije v viru šuma lahko poskrbimo, da zmanjšana zaloga vrednosti odčitkov ne izboljša verjetnosti, da bi bilo mogoče uganiti naslednji niz generiranih naključnih števil.
Pri izkoriščanju ne-kvantnih virov fizičnega šuma ostaja še zadnja nevarnost: *nepredvideni napadi s prijemi, katerih danes še ne poznamo*. Verjetnost, da se bo v prihodnosti pojavil nov, še neznan pristop za manipulacijo podanega senzorja ni zanemarljiva. Zato so najbolj varni kvantni generatorji šuma, saj s kvantnim "šumom" napadalci ne morejo manipulirati.

1.3 Standardizacija in klasifikacija generatorjev

Priporočila za varno generiranje naključnih števil imajo dolgo zgodovino. V Evropi jih je prvi izdal nemški zvezni urad za varnost v informacijski tehnologiji BSI že konec prejšnjega stoletja. Del priporočil je **klasifikacija** generatorjev. Razdeljeni so na deterministične (Deterministic Random number Generator ali DRG), strojne (Physical True random number Generator ali PTG) in ne-fizikalne (Non-physical True random number Generator ali NTG).



Klasifikacija generatorjev naključnih števil po BSI

Deterministični generatorji so razdeljeni v štiri razrede po naraščajočih varnostnih zahtevah. DRG.1 predvideva le navidezno naključnost generiranih nizov, torej da generirana števila niso napovedljiva. DRG.2 dodaja zahtevo, da iz danega generiranega niza števil ne moremo (enostavno) določiti, katera števila so bila generirana pred njimi. DRG.3 dodatno zahteva še, da tudi ob znanem notranjem stanju generatorja napadalec ne more uganiti števil, ki so bila generirana v preteklosti (nezmnožnost napovedovanja za nazaj). Zadnji razred DRG.4 dodaja zahtevo, da ob znanem notranjem stanju generatorja napadalec ne more uganiti števil, ki bodo generirana v prihodnosti (nezmožnost napovadovanja za naprej). Zadnja zahteva torej predvideva, da bo generatorjevo stanje periodično ponastavljeno iz zunanjega vira entropije.

Strojni generatorji se delijo na tri razrede. Za PTG.1 je predpisano, da mora generirati števila iz strojnih (fizičnih) virov a brez jamstev o predvidljivosti naključnih števil niti o njihovi porazdelitvi. PTG.2 dodaja zahtevo o nepredvidljivosti, kar implicitno zahteva tudi porazdelitev generiranih števil z minimalnim odstopanjem od enakomerne. PTG.3 dodaja še zahtevo po vključitvi algoritma DRG.3 v naknadno procesiranje generiranih števil.

Razred NTG.1 so generatorji, ki entropijo zajemajo iz računalniške strojne opreme (mrežni promet, različne latence, interakcija z uporabnikom, ipd.) ali iz delovanja programov (razporejanje procesov, trajanje procesov, ipd.). Ta razred tudi zahteva, da vire entropije procesira algoritem DRG.3 za generiranje naključnih števil.

Po BSI je priporočila oblikoval ameriški nacionalni inštitut za standarde in tehnologijo NIST (serija SP 800) in kasneje še ameriški nacionalni inštitut za standardizacijo ANSI. Na mednarodnem nivoju predstavlja konsenz nacionalnih standardizacijskih teles standard ISO/IEC 18031, katerega značilnost je velika generičnost, saj ne predpisuje aplikacijskih vmesnikov niti konkretnih evalvacijskih postopkov. Zaenkrat se standard NIST tako terminološko kot v klasifikaciji razlikuje od standarda BSI. Zato obstajajo *težnje po harmonizaciji* in te se nadejamo že z naslednjimi različicami standardov. BSI je, denimo, 15. septembra 2022 objavil prvi osnutek novih priporočil, ki so zdaj v fazi zbiranja pripomb.

Trenutno objavljena priporočila in standardi omenjenih standardizacijskih teles so tako:

• ISO/IEC 18031:2011: Information technology - Security techniques - Random bit generation
• American National Standard (ANS) X9.82, Random Number Generation - Parts 1-4
• NIST Special Publication 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, junij 2015
• NIST Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, januar 2018
• NIST Special Publication 800-90C: Recommendation for Random Bit Generator (RBG) Constructions, april 2016
• NIST Special Publication 800-22 Revision 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, april 2011
• BSI AIS 20, Version 1: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, Version 2.0, december 1999
• BSI AIS 31, Version 1: Functionality Classes and Evaluation Methodology for Physical Random Number Generators, september, 2001

2. Kriptografsko varni generatorji psevdonaključnih števil

Kriptografsko varne generatorje naključnih števil moramo zasnovati s predpostavko, da ima nasprotnik (napadalec) lahko omejen vpogled v vir entropije ali celo vpliv nanj. Dober ekstraktor naključnosti lahko varno deluje tudi z delno kompromitiranimi viri entropije in viri, v katerih so navzoče medsebojne odvisnosti med izhodnimi biti. Če je vir entropije fizičen senzor, na primer mikrofon ali kamera, potlej ima napadalec možnost vplivati na sliko oziroma zvok zajet s senzorjem, na temperaturo okolice in podobne vidike s signifikantnim vplivom na vir entropije. Vsak vpliv na vir entropije lahko zmanjša njegovo izhodno entropijo, vendar lahko za dobre vire predpostavljamo, da napadalec nikoli ne more dobiti popolnega vpliva in izničiti vse entropije. V nasprotnem primeru bi bil vir neuporaben in bi generator naključnih števil izgubil vso varnost. A zaradi možnega vpliva na vir entropije moramo kritično oceniti količino entropije, ki je na voljo in iz vira ne poskušati dobiti več entropije, kot jo je zmožen generirati navkljub zunanjim vplivom nanj.
Pogosto navedeni pogoji, da se smatra generator naključnih števil za **kriptografsko varnega**, so:

- Dobre statistične lastnosti generiranih števil - generirane vrednosti so statistično neodvisne od predhodnih in naslednjih generiranih vrednosti, verjetnosti za generiranje posameznih vrednosti so enake za vso zalogo vrednosti ter so neodvisne od časa.
- Poznavanje nekega generiranega niza števil omejene dolžine napadalcu pomaga le insignifikantno pri določanju števil generiranih pred ali po tem nizu.
- Poznavanje internega stanja generatorja napadalcu ne poveča signifikantno verjetnosti ugibanja preteklih generiranih vrednosti (nezmožnost napovedovanja za nazaj). Ta lastnost omogoča generiranje nezlomljivih naključnih števil navkljub nevarnosti, da v prihodnosti napadalec dobi dostop do generatorja.
- Poznavanje notranjega stanja algoritma napadalcu ne poveča signifikantno verjetnosti ugibanja števil generiranih v prihodnje (nezmožnost napovedovanja za naprej). Ta lastnost onemogoča napadalcu, da bi si s časovno omejenim dostopom do generatorja lahko zagotovil

prednost pri ugibanju generiranih števil v prihodnje. Te lastnosti popolnoma deterministični generatorji ne izpolnjujejo, zato moramo pri njihovi uporabi redno menjati seme.

- Robustnost - napadalec s fizičnim in ali programskim dostopom do generatorja ne more vplivati na generator tako, da bi mu to pomagalo uganiti generirane nize števil.

Testiranje kriptografske varnosti

V standardu NIST [Bassham 2010] so predstavljeni testi za ocenjevanje naključnosti generatorjev. V osnovi moramo kriptografsko varne generatorje testirati enako kot običajne generatorje, vendar z nekaj dodatnimi pogoji – predvsem je nujna **nepredvidljivost** generiranih števil. Pravega testa za slednjo seveda ni, *zato so testi le nujen, ne pa tudi zadosten pogoj, da določen generator lahko označimo za kriptografsko varnega*. Nujna je tudi kripto-analiza generatorjev, ki se jo najbolj temeljito lahko izvede ob poznavanju točnega namena podanega generatorja.

Primeri pogosto uporabljenih implementacij

Podjetje Apple za operacijski sistem za mobilne naprave iOS uporablja kriptografsko varne generatorje naključnih števil, vgrajene v samo jedro operacijskega sistema. Navajajo, da njihovi generatorji integrirajo vire entropije iz:

- virov v posebej zavarovanem delu strojne opreme (angl. secure enclave) znotraj procesorja, ki temeljijo na uporabi več krožnih oscilatorjev, katerih izhod je matematično obdelan z blokovnimi šiframi,
- meritev časov med prižiganjem naprave,
- statistike prekinitev izvirajočih iz strojne opreme,
- posebne semenske datoteke,
- posebnih procesorskih ukazov, na strojnih platformah, ki take ukaze ponujajo.

Moderni algoritem, po katerem deluje generator, je izvedenka algoritma **Fortuna**, ki je izpeljanka predhodnika, algoritma Yarrow.

Operacijski sistem Android uporablja programsko knjižnico SecureRandom iz programskega jezika Java v namene generiranja kriptografsko-varnih naključnih števil. SecureRandom nima predpisane izvedbe, a pogosto je uporabljen algoritem SHA1PRNG, katerega definicija se spreminja z revizijami programskega jezika Java. V osnovi je SHA1PRNG deterministične algoritem na osnovi kriptografske zgoščevalne funkcije SHA1. Njegova uporaba je torej smiselna le ob dobrem zunanjem viru entropije, ki ga Android ne predpisuje. V okviru Jave je vir entropije vezan na sistemski generator naključnih števil, ki je na operacijskih sistemih po vzoru UNIXa (mednje spada tudi Android) ponujen v obliki programske naprave /dev/random.

Naprava /dev/random v operacijskih sistemih Linux je generator pravih naključnih števil, ki je izveden v jedru operacijskega sistema. Entropijo zbira med delovanjem sistema in vrača – glede na analizo raziskovalcev iz 2006 – kriptografsko varne naključne nize. Njegovo delovanje je sicer slabo definirano in slabo dokumentirano, vemo pa, da jemlje entropijo iz uporabnikovih dejanj (pritiski na tipke, premiki miške), vhodno-izhodnih operacij na trajnem pomnilniku in njihovih časov ter statistike prekinitev iz strojnih naprav. Generator v jedru Linux sicer doživlja obsežno prenovo v zadnjih letih in analize prenovljene različice še niso na voljo.

Operacijski sistemi Windows že od verzije 95 dalje zagotavlja kriptografsko varna naključna števila preko generatorja, katerega algoritem ni razkrit. Analiza s pomočjo inverznega inženirstva je razkrila kup napak v njegovi izvedbi za Windows 2000. Generator se po poročanju avtorjev le občasno napaja iz sveže entropije, seme za inicializacijo je delno predvidljivo, sam generator pa ni varen ne za naprej, ne za nazaj. Dobra lastnost po drugi strani je, da se inicializira instanca za vsak proces posebej, zato napad nanj zahteva najprej eskalacijo sistemskih pravic ali pa kako drugo obliko napada, preko katerega lahko napadalec prebere spomin dodeljen napadenemu procesu. V novejših različicah operacijskega sistema ja generator že prenovljen, njegova izvedba pa ostaja skrita in neodvisni raziskovalci je niso analizirali.

3. Strojni generatorji naključnih števil

V tem razdelku opisujemo različne tipe strojnih (fizičnih) generatorjev naključnih števil, ki temeljijo na raznovrstnih fizikalnih procesih, ki ustvarjajo entropijo, tako kvantnih kot klasičnih. Te naprave spadajo v skupino nedeterminističnih generatorjev. Rečemo tudi, da gre za "generatorje pravih naključnih števil" (**TRNG**, true random number generator, to okrajšavo bomo uporabljali tudi v nadaljevanju). Osnovna pravila pri tovrstnih generatorjih so stabilnost vira entropije (proizvajajo konstantno entropijo na enoto časa), neodvisnost od okolice (temperatura, viri napajanja, elektromagnetna valovanja) in da se ne starajo (ni sprememb na zelo dolgi časovni skali). Zaželeno je, da je entropija merljiva oz. določljiva, kar je pogosto težko dosegljivo in predstavlja največji izziv.

3.1 Kvantni generatorji

Kvantni generatorji naključnih števil (**QRNG**, quantum random number generator) kot vir naključnosti uporabljajo kvantne pojave, ki so v osnovi nedeterministični (nenapovedljivi, probabilistični) in na katere ni mogoče vplivati. Temeljijo na **Bornovem načelu**, enem izmed osnovnih postulatov kvantne teorije, ki pravi, da izide meritev opravljenih na kvantnomehanskih sistemih ne moremo napovedati, določimo lahko le verjetnosti za različne možne izide. QRNG temeljijo na kvantnih pojavih, kot sta, denimo, superpozicija stanj in kvantna nedoločenost.

3.1.1 Generatorji z radioaktivnimi viri

Najenostavnejši in hkrati prvi kvantni generatorji so kot vir entropije uporabljali radioaktivni razpad, pri katerem nastanejo ionizirajoči delci, ki jih zazna Geiger-Muellerjev (G-M) števec. Delec povzroči v G-M cevi ionizacijski proces, ki po ojačanju ustvari električni pulz na izhodu števca. Časi med posameznimi zaznanimi dogodki so, tako kot časi radioaktivnih razpadov, popolnoma naključni in neodvisni od predhodnih dogodkov. Izmerjene čase pretvorimo v številke in dobimo nize naključnih števil. Čeprav dobljena števila izpolnjujejo vse zahteve kvalitetnih naključnih števil, imajo ti generatorji nekaj slabosti: za svoje delovanje potrebujejo radioaktiven vir in so relativno počasni, saj lahko generirajo največ milijon bitov na sekundo.

3.1.2 Optični QRNG

Optični QRNG temeljijo na kvantni naravi svetlobe oz. fotonov. Najenostavnejša izvedba vključuje izvor posameznih fotonov, delilnik svetlobe (angl. beam splitter) in dva prostorsko ločena detektorja posameznih fotonov (SPD, angl. single photon detector). Delilnik svetlobe ima lastnost, da 50%

vpadle klasične svetlobe prepusti, ostalih 50% pa odbije (polprepustno zrcalo). Če na tak delilnik svetlobe posvetimo s posameznimi fotoni, ima vsak foton 50% verjetnost, da bo prepuščen in zaznan s prvim SPD in 50% verjetnost, da bo odbit in zaznan z drugi SPD. Govorimo o **kvantni superpoziciji stanj** – foton je v kvantnem stanju, ko je "hkrati prepuščen in odbit". Šele ko opravimo meritev (ko pride foton do SPD), je njegova pot določena. Če zazna foton prvi detektor, spremenimo to v število 0, če ga zazna drugi, pa v število 1. Ob enakomernem toku fotonov tako dobimo popolnoma naključen niz števil 0 in 1.

Podobno deluje QRNG, ki uporablja za svoje delovanje superpozicijo polarizacijskih stanj posameznega fotona. V tem primeru uporabimo polarizacijski delilnik svetlobe (PBS, angl. polarizing beam splitter) in vir posameznih fotonov, ki generira linearno polarizirane posamezne fotone (s polarizacijo pod kotom 45 stopinj glede na prepustno smer PBSja). Take fotone pošljemo na PBS, ki usmeri horizontalno polarizirane fotone na prvi ter vertikalno polarizirane fotone na drug SPD. Po prehodu skozi PBS obstaja foton v superpoziciji obeh polarizacij. Verjetnost, da bomo detektirali foton na prvem ali na drugem detektorju, je popolnoma naključna.

Tudi optični kvantni generatorji naključnih števil imajo nekaj slabosti: mrtvi čas (angl. dead time) detektorjev fotonov omejuje najkrajši čas med posameznimi zaznanimi fotoni in s tem hitrost generiranja naključnih števil; zakasnjeni dodatni pulzi (angl. afterpulsing) lahko povzročijo korelacije med biti; šum v detektorjih lahko povzroči lažne zaznave; različna občutljivost detektorjev privede do neenakomerne porazdelitve v številu zaznav na enem in drugem detektorju. Poleg tega za delovanje kvantnih generatorjev uporabljamo številne klasične elektronske elemente, na primer analogno-digitalne pretvornike, ki s svojim klasičnim šumom dodatno neželeno prispevajo k entropiji kvantnega procesa. Zato so, podobno kot drugi TRNG, tudi QRNG sestavljeni iz dveh podsistemov: nedeterminističnega (kvantnega) vira entropije ter determinističnega ekstraktorja naključnosti.

Izvori posameznih fotonov in detektorji, ki so sposobni zaznati posamezne fotone ob čim nižjem šumu ozadja, so relativno veliki in dragi. Zato so bile razvite metode, ki ne temeljijo na zaznavi posameznih fotonov temveč na uporabi zelo kratkih pulzov svetlobe. Kot vir svetlobe lahko služi kar običajna svetleča dioda (LED, angl. light emitting diode), kot detektor pa SPAD (angl. single-photon avalanche detector). LED in SPAD so cenovno ugodni v primerjavi z izvori posameznih fotonov in detektorjev posameznih fotonov na osnovi superprevodnih nanožic. Dodatna prednost je možnosti miniaturne izdelave LED in SPAD komponent s postopki klasične polprevodniške proizvodnje. Tako je danes na trgu že mogoče kupiti komercialen izdelek optičnega kvantnega generatorja naključnih števil, ki deluje na opisanem principu, je kompakten in cenovno ugoden. Poleg prednosti cene in velikosti pa je že sama svetleča dioda vir kvantnega naključja, saj je **spontana emisija**, kot osnovni princip delovanja polprevodniške svetlobne diode, po svoji naravi kvantnomehanski pojav. Število fotonov, ki jih LED odda v vsakem pulzu, niha okoli neke povprečne vrednosti, porazdelitev pa je Poissonska, kar je karakteristika kvantno zašumljenih izvorov. Tudi SPAD, ki deluje na osnovi kvantnomehanskega procesa **fotovzbuditve** nosilcev naboja, je že sam po sebi vir kvantnega naključja. Verjetnost uspešne detekcije fotonov, ki padejo na SPAD, je namreč popolnoma naključna.

Tako z uporabo LED in SPAD komponent dobimo dodatne kvantne vire entropije.
Naključen je tudi čas izsevanja fotonov svetlečih diod in laserskih izvorov svetlobe. Preprost primer je časovno enakomerno proženje LED in natančna časovna detekcija pulzov. Če je čas prihoda med pulzi krajši oziroma daljši kot časovni interval med proženjem LED, to predstavlja število 0 oziroma 1. Poleg točnega časa generiranja fotonov je naključna tudi prostorska porazdelitev fotonov v posameznem pulzu svetlobe. S ploskovnim detektorjem fotonov lahko rekonstruiramo prostorsko porazdelitev intenzitete svetlobe in tudi to informacijo uporabimo kot vir entropije.

3.1.3 QRNG z atomi

Kot vir naključnosti lahko uporabimo kvantna stanja v atomskih sistemih. V razredčenih plinih alkalijskih kovin lahko optično merimo kolektivni spinski šum, ki je kvantne narave in je posledica interakcije med posameznimi atomi v plinu.

3.1.4 QRNG na osnovi kvantnih računalnikov

Tudi kvantne računalnike lahko uporabimo kot generatorje naključnih števil. V najbolj preprosti različici (tako imenovani Hadamardov protokol) vsak kubit najprej pripravimo v kvantnem stanju 0. Nato na vsak tak kubit delujemo s Hadamardovimi vrati, ki kubit postavijo v superpozicijo kvantnih stanj 0 in 1. V zadnjem koraku na vsakem kubitu izvedemo meritev. V polovici primerov bo valovna funkcija kubita po meritvi kolapsirala v stanje 0, v preostalih primerih pa v stanje 1. Na izid posamezne meritve ni mogoče vplivati in je povsem naključna. Slabost pristopa je občutljivost na napake med izvajanjem računa na kvantnem računalniku, tako ob inicializaciji začetnega stanja kubitov, pri izvajanju kvantnih operacij (kvantnih vrat), kot tudi ob meritvi stanj, kar lahko opazno vpliva na enakomernost porazdelitve in na entropijo.
Slabosti Hadamardovega protokola za generiranje naključnih števil s kvantnim računalnikom odpravi protokol, ki temelji na prepletenosti kubitov (angl. entanglement protocol). V tem primeru začnemo z N kubiti v stanju 0 in jih v naslednjem koraku medsebojno prepletemo s pomočjo enokubitnih (Hadamardova vrata) in dvokubitnih (vrata CNOT) operacij. Na koncu znova na vsakem kubitu izvedemo meritev. Po M ponovitvah dobimo N nizov naključnih števil dolžine M. Enega izmed nizov uporabimo za kontrolo parnosti, s čimer lahko izločimo primere, ko se je pri izračunu zgodila napaka. Glavna prednost protokola je v tem, da je izmed preostalih N-1 nizov za testiranje statističnih lastnosti dovolj uporabiti le en niz, saj imajo po definiciji preostali nizi enake statistične lastnosti.

Uporaba kvantnih računalnikov za generiranje naključnih števil seveda terja velik in relativno drag kos opreme, zato pa ponuja certificirano generiranje naključnih števil. Tukaj velja omeniti podjetje Cambridge Quantum Computing, ki skupaj s podjetjem IBM želi na trg ponuditi tovrstno storitev. Lahko predvidevamo, da bo v prihodnosti ta storitev nadgrajena tudi z “od naprave neodvisnim” (angl. device-independent) konceptom generiranja naključnih števil, ki bo zagotavljal privatnost generiranega niza tudi v primeru, ko ima napadalec dostop do same naprave. Pri večini preostalih kvantnih generatorjev naključnih števil, ki so voljo na na trgu, moramo proizvajalcu oziroma sami napravi zaupati (angl. trusted device).

3.1.5 Stanje na trgu QRNG

Tehnologija QRNG je dovolj zrela, da lahko že v kratkem času postane pomembna za končnega uporabnika. Čeprav si je težko zamisliti sektor ali industrijo, kjer ne bi potrebovali naključnih števil, lahko v grobem uporabo naključnih števil razdelimo v tri kategorije: kibernetska varnost, igralništvo ter raziskave in razvoj (R&D).

V kategorijo uporabe QRNG za kibernetsko varnost sodijo na primer mobilne naprave, internet stvari (IoT), podatkovni centri in spletno bančništvo. Dolgoročno gledano lahko predvidevamo, da si bodo v teh panogah želeli ponudniki svoje storitve prej ali slej nadgraditi s QRNG. Največji tržni potencial za QRNG je njihova uporaba za elektronsko poslovanje in storitve na mobilnih 5G napravah. Tako je Samsung že leta 2020 na korejski trg ponudil mobilno napravo Galaxy A Quantum, ki ima vgrajen QRNG čip švicarskega podjetja IDQuantique in ga uporablja v nekaterih aplikacijah elektronskega poslovanja (SK Pay, ID Login, Initial). Hkrati je SK Telecom s QRNG nadgradil svoj center za avtentikacijo naročnikov, kar zagotavlja povečano varnost na obeh straneh komunikacije. V bančnem sektorju velja omeniti ameriški JPMorgan Chase, avstralski Westpac Bank in britanski NS&I, ki veliko vlagajo v kvantno-varne tehnologije, saj predvidevajo, da bodo te tehnologije v prihodnosti pomembne za njihove stranke in kliente. Tudi EU preko Quantum Flagship programa vlaga v razvoj QRNG, primer je projekt QRANGE, ki ima za cilj komercializacijo QRNG za varne komunikacije in visoko-zmogljivo računanje (HPC). V kontekstu varnega prenosa podatkov velja omeniti trend, da se za post-kvantne kriptografske algoritme zahteva uporabo ključev daljših od 10.000 bitov, kar bi lahko pospešilo razvoj hitrih QRNG na čipih. Ko bo cena QRNG dovolj padla, bodo postali zanimivi tudi za IoT naprave, kjer naj bi trenutno okoli 98% celotne izmenjave podatkov potekala nekriptirano. Tudi v blockchain tehnologiji si želijo ponudniki teh storitev dodati nov nivo varnosti z uporabo QRNG (švicarski Mt Pelerin).

V kategoriji igralništva so v ospredju predvsem spletne igralnice, saj je v kazinojih število iger in uporabnikov omejeno. Glavna motivacija za vpeljavo QRNG je zagotavljanje fair-playa, zato so zanimivi tudi za državne loterije. Podjetje IDQuantique kot svoji stranki navaja Loterie Romande (švicarska loterija) in Francaise des Jeux (francoska loterija). Ima pa svoje stranke tudi med ponudniki spletnih igralnic (Novomatic, BetCruise, A Bet A, PokerMatch). Omeniti velja tudi PokerStars, ki za mešanje kart uporablja QRNG, ki ga je certificiral Gaming Labs.

Zadnja kategorija je sicer tržno najmanj zanimiva, je pa uporaba Monte-Carlo simulacij in drugih stohastičnih metod v porastu v raziskavah in v razvojnih oddelkih podjetij. Za te namene so potrebni kvalitetni nizi naključnih števil, kar po definiciji zagotavljajo QRNG. Ampak ker privatnost podatkov v tem sektorju ni zahtevana, zadostujejo spletne storitve in zbirke dobrih nizov naključnih števil. V tem smislu ta sektor predvidoma ne bo pospešil razvoja QRNG.

Glavna tržna prednost QRNG je v tem, da je za razliko od drugih TRNG jasno od kod izvira njihova naključnost, kar olajša certificiranje. Velja tudi, da je v QRNG lažje zaznati napake v delovanju in se lahko monitoring izvaja v realnem času. Poleg tega za naprednejše oblike QRNG, ki so sicer še v fazi raziskav in razvoja, velja, da nam kot uporabniku ni potrebno zaupati proizvajalcu opreme in so nizi naključno generiranih števil certificirano zasebni. Tudi ostali parametri, kot so hitrost generiranja naključnih števil, velikost naprave in poraba energije, so v prid QRNG. Morda je še največja ovira cena, kjer se še išče cenejšo tehnologijo za obenem hitrejšo izdelavo čipov.

QRNG lahko po kriteriju, v kakšni obliki so na voljo na trgu, delimo na čipe, razširitvene kartice in samostojne naprave. Čipe že vrsto let izdeljuje podjetje IDQuantique. Ti imajo trenutno hitrost okoli

1 Mbit/s in so v cenovnem razredu do 10 EUR. Podjetje Samsung jih vgrajuje v nekatere svoje mobilne naprave. Razširitvene kartice (PCIe) omogočajo večjo hitrost generiranja naključnih števil (preko 100 Mbits/s) in so zanimive za varen prenos podatkov na področju bančništva, zdravstva, državnih organov in telekomunikacij, kot tudi v igralništvu ter v raziskavah in razvoju (na primer Monte-Carlo simulacije). Njihova cena se giba med 1000 in 2000 EUR. Samostojne naprave so na voljo v cenovnem razredu preko 10.000 EUR in so primerne za podatkovne centre in podjetja, ki se ukvarjajo s storitvami v oblaku. Tukaj so gonilna sila ponudniki 5G omrežja (SK Telecom), kjer se QRNG na primer že uporablja za avtentikacijo naročnikov (zaenkrat predvsem v Južni Koreji).
Omenimo še nekatere glavne proizvajalce QRNG, večinoma gre za startupe, podjetja iz sektorja kvantnih komunikacij (QKD) in velika podjetja v sektorju IT in elektronike. Vodilno je že večkrat omenjeno švicarsko podjetje IDQuantique, ki izdeluje QRNG čipe za pametne telefone in QRNG naprave za uporabo v igralništvu, podatkovnih centrih in v telekomunikacijah. Njihovi izdelki so optični QRNG, ki temeljijo na CMOS detektorjih, na voljo so čipi z ali brez postprocesiranje (torej ali surova entropija ali pa celotna izvedna generatorja). Na voljo so evalvacijski kiti z različnimi čipi v obliki drobnih računalnikov (Raspberry Pi ali Odroid) z mrežno povezljivostjo (gigabitni Ethernet).
Pomemben igralec je tudi britanski Toshiba Europe, ki v sodelovanju z Univerzo v Cambridgu razvija QRNG in QKD opremo. Med startupi so bolj znani španski Quside (razvoj čipov), britanski Quantum Dice (spinout Univerze v Oxfordu) in avstralski QuintessenceLabs (razvija naprave za bančništvo, obrambo in storitve v oblaku v obliki PCIe kartic in 1U vgradnih enot, ki temeljijo na kvantnem tuneliranju). Med velikimi podjetji velja omeniti nemški Bosch, ki razvija QRNG za IoT in avtonomna vozila ter sodeluje z nemškim BSI pri pripravi standardov za certificiranje QRNG. Francoski Thales je nedavno začel vgrajevati QRNG v svoje kriptografske module (HMS).

Zaznaven trend je uporaba čedalje bolj prepustnih kanalov za prenašanje naključnih števil iz generatorja do uporabnika. Prvi moduli so uporabljali zaporedno vodilo USB2, danes so zelo pogoste razširitvene kartice PCIe, uveljavljati pa se začenjajo tudi samostojne naprave z mrežno povezljivostjo preko Etherneta. Hitrosti najbolj zmogljivih naprav presegajo Gbit/s.

3.2 Ostali strojni generatorji (TRNG)

Strojni generatorji TRNG, ki se ne uvrščajo v skupino QRNG, temeljijo na zelo različnih težko napovedljivih fizikalnih procesih, denimo na nedeterminističnih šumih ali na načeloma povsem determinističnih vendar kaotičnih procesih.
Šum je splošen izraz za običajno neželene signale, pogosto v kontekstu elektronskih naprav. Šumi so različnih vrst, zato jih delimo glede na njihov izvor in spektralne karakteristike. Nastanejo lahko znotraj naprave zaradi velikega števila gradnikov snovi, ki si med seboj pri končni temperaturi izmenjujejo energijo preko trkov (Johnson-Nyquistov termični šumi), zaradi diskretne narave elektronov (Poissonov šum, angl. shot noise), zaradi redkih dogodkov v snovi (šum 1/f) ter še nekaj drugih bolj eksotičnih mehanizmov. Izvirajo lahko tudi iz okolice naprave (elektromagnetne motnje, fluktuacije napajalne napetosti, preleti kozmičnih delcev). Pogosto je vir šuma načeloma celo kvantnomehanski, vendar proizvajalec ne želi ali ne more jamčiti, da je znatni del generirane entropije tovrstnega izvora. Tak primer so, denimo, zelo pogosto uporabljeni generatorji z Zenerjevi diodami, priključenimi v neprevodni smeri, v katerih prihaja do naključnih plazovnih prebojev toka zaradi kvantnomehanskega tunelskega pojava. Meja med kvantnimi in nekvantnimi generatorji

naključnih števil je zato v praksi nekoliko zabrisana. Generator, ki se prodaja kot kvantni, ni intrinzično boljši od podobnega "nekvantnega", ki uporablja praktično enak fizikalni proces.

Kaotični generatorji so povsem deterministični, vendar je zaradi nelinearnosti v praksi povsem nemogoče napovedati dolgoročno obnašanje naprave, četudi bi to načeloma bilo mogoče. V to skupino uvrščamo nekatere elektronske oscilatorje (Chuaovo vezje), ter naprave, ki naključnost zajemajo iz atmosferskih pojavov (denimo radiofrekvenčno elektromagnetno šumenje, ki je vir naključnosti na spletni strani random.org). Omeniti je treba, da je kaos pojav, ki se obravnava predvsem v kontekstu klasične fizike (koncept kaotičnosti v kvantni mehaniki je še predmet razprav).

3.2.1 Oscilatorski TRNG

V praksi se največ uporabljajo električni oscilatorji, katerih frekvenca ni nikoli idealno stabilna, temveč se trese, pojavu rečemo tudi trepetanje (angl. **jitter**). Tresenje nastane zaradi elektromagnetnih interferenc, fluktuacij napajalne napetosti zaradi preklopov tranzistorjev v integriranem vezju, termičnih fluktuacij in drugih težje določljivih prispevkov, in se lahko s časom znatno spreminja zaradi spreminjajočih se pogojev. Spremembe sicer niso pomembne, pomembno je le, da obstaja neka spodnja meja tresenja. Oscilatorje se uporabi kot vire entropije denimo tako, da en oscilator vzorči signal drugega. Frekvenca vzorčenja mora biti izbrana tako, da ob minimalni meri tresenja postane faza vzorčenega nihanja povsem nenapovedljiva. Najpreprostejši oscilatorji so **krožni oscilatorji** (angl. ring oscillator) iz verige lihega števila zaporedno vezanih logičnih inverterjev, sklenjenih v krog: takšno vezje je po definiciji nestabilno in niha s frekvenco, ki jo določata zakasnitev signala med vhodom in izhodom inverterja ter dolžina verige. Odličen vir entropije so oscilatorji izdelani v asinhroni logiki iz verige lihega števila Mullerjevih vrat; to so krožni oscilatorji z lastnim ritmom (angl. self-timed ring, STR). Potencialna pomanjkljivost generatorjev z oscilatorji je možnost, da se frekvenca nihanja stabilizira zaradi nenamerne fazne uskladitve (sinhronizacije) z drugimi deli vezja ali pa celo zaradi namernega vplivanja napadalca na napajalno napetost ali preko elektromagnetnega vzbujanja. V teh primerih bi tresenje lahko padlo pod mero, ki je potrebna za ustvarjanje zadostne količine entropije. Prednost oscilatorjev pa je, da se jih da zlahka implementirati v namenskih integriranih vezjih (ASIC), malo težje pa tudi v programabilni logiki (FPGA).

Tovrstni viri naključnih števil so vgrajeni v vse sodobne procesorje: v arhitekturi x86 imajo vsi novejši procesorji podjetij Intel in AMD na voljo strojna ukaza RDRAND in RDSEED, ki zajemata naključna števila iz strojnega generatorja, za ARM je na voljo TRNG v tehnologiji TrustZone, Applov procesor M1 ima TRNG vgrajen v "Apple Security Enclave", vir entropije je na voljo za RISC-V, itd. Tovrstni generatorji so zelo hitri in kvalitetni, zato jih je smiselno uporabljati v vseh primerih, ko za to ne obstajajo kakšni specifični varnostni pomisleki. Za vezja FPGA in ASIC je možno kupiti implementacije TRNG kot "intelektualno lastnino", torej v obliki rešitev, ki se jih preprosto integrira v vezje. Uporabljajo standardna vodila (denimo AMBA-AXI), so v skladu s poglavitnimi standardi in prestanejo pomembne sklope statističnih testov; pomanjkljivost je, da so dostavljena v obliki kriptiranih opisov vezja (angl. netlist) za točno določeno družino čipov, zato je nemogoče neodvisno preveriti pravilnost implementacije (omogočajo sicer neposreden dostop do surove sekvence iz vira entropije). Licenca kupcu dopušča neomejeno uporabo (primer TRNG-P100 IP Core podjetja Berten). Na voljo so tudi rešitve za implementacijo v CMOS tehnologiji v obliki GDSII (TRNG-Analog noise

source podjetja Thales). Razvoj strojnih komponent za generiranje naključnih števil je bil tudi cilj evropskega projekta HECTOR (Hardware enabled crypto and randomness, H2020, obdobje financiranja 2015-2018): nekatere komponente, ki so rezultat tega projekta, so prosto dostopne v obliki opisnih datotek za vezja VHDL v javnih repozitorijih, delovanje pa je dobro dokumentirano v javno objavljenih poročilih ter znanstvenih člankih.

3.2.2 Stanje na trgu TRNG

Generatorji v obliki zunanjih modulov, ki se jih na računalnik priključi preko zaporednega vmesnika (tipično USB), so postali redki. Na trgu je še nekaj ponudnikov, ki pa večinoma ponujajo starejše izdelke, ki po karakteristikah niso konkurenčni sodobnim rešitvam. Preprostost principa delovanja in implementacije je morda njihova največja prednost, saj je delovanje načeloma preverljivo zaradi neposrednega dostopa do elektronskega vezja. Pomanjkljivosti so potreba po gonilnikih za različne operacijske sistema (kar kaže na vprašljivo dolgoročno podporo), slaba fizična zaščita (plastična ohišja), slaba priložena dokumentacija ter slabo razmerje med ceno in zmogljivostjo. Splošni vtis je, da gre pogosto za nedodelane maloserijske rešitve. Opazili smo tudi težave z dobavljivostjo: številni proizvajalci imajo spletne kataloge s ceniki, izdelki pa dejansko niso na voljo.

Kar se tiče programskih rešitev za povezavo med generatorjem in odjemalcem, najdemo dva pristopa: neposredno uporabo generiranih števil preko vmesnika v obliki knjižnice ali pa dodajanje entropije v entropijski bazen jedra operacijskega sistema, tako da končni uporabnik naključna števila potem zajema preko standardnega vmesnika (denimo v obliki branja iz /dev/random v operacijskih sistemih iz družine Unix in izvedenk, kot je Linux).

Zaključimo lahko, da je trend na področju strojnih generatorjev, da je TRNG že vgrajen kot standardna komponenta v strojni varnostni modul (HSM, angl. hardware security module) ali v CPU, ki je v neposredni bližini računskega dela, kjer se naključna števila tudi "porabljajo". S tem se zmanjša razdalja potovanja in tako tudi možnost prisluškovanja, saj so možni samo morebitni napadi na stranski kanal na samem čipu. TRNG v obliki samostojnih naprav so postali redki. *Če se bodo uveljavili kvantni generatorji, lahko tudi za te dolgoročno pričakujemo integracijo v varnostne module in v procesorje.*

Na seznamu List of approved cyrptographic products (LAPC) za zaščito zaupnih informacij EU (EU classified information, EUCI) ni generatorjev naključnih števil kot samostojnih naprav (verzija 27 Oct 2021).

3.3 Ekstraktorji naključnosti

Naključna števila, ki jih ustvari primarni vir v fizikalnih generatorjih, praktično nikoli niso idealna v statističnem smislu, torej neodvisna (brez zaporednih korelacij v nizu) in enakomerno porazdeljena (enaka verjetnost za 0 in 1), zato jih je potrebno obdelati s t.i. **ekstraktorji naključnosti**. To so algoritmi, ki pretvorijo "šibko naključne" porazdelitve v skoraj enakomerne porazdelitve. Zgodovinsko pomemben je, denimo, von Neumannov ekstraktor iz leta 1951, ki iz zaporedja neodvisnih števil z neenakomerno (torej pristransko) porazdelitvijo generira povsem enakomerno (nepristransko) porazdelitev za ceno krajšega izhodnega niza (v najboljšem primeru pol krajšega). Odpravljanje korelacij je bolj zahtevno. Ideja v ozadju ekstraktorjev je lema o ostanku ob zgoščevanju (angl. leftover hash lemma), ki v grobem pravi, da lahko iz niza začetnih naključnih bitov z dano min-entropijo h izluščimo krajši končni niz skoraj enakomerno porazdeljenih števil.

V zadnjem obdobju se pogosto uporablja **Toeplitzev ekstraktor**, pri katerem se vektorje začetnih naključnih bitov dolžine n množi s Toeplitzevo matriko dimenzije m × n, rezultat pa so vektorji dolžine m končnih naključnih števil. Toeplitzeva matrika je povsem določena z njenimi elementi (binarnimi vrednostmi) v prvem stolpcu in prvi vrstici, ki se potem ponavljajo diagonalno desno navzdol; elementi so izključno izbrani (naključno seme) za dano implementacijo, vendar smejo biti fiksni in so lahko javno znani. Operacija množenja med elementi pri matričnem množenju je definirana kot logična konjunkcija (vrata AND), seštevanje pa kot izključna disjunkcija (vrata XOR) oz. seštevanje modulo 2. Dimenzije matrike se izbere tako, da je razmerje dimenzij prilagojeno entropiji vhodnih podatkov. Tako obdelano zaporedje naključnih števil prestane praktične statistične teste naključnosti. Toeplitzev ekstraktor je zelo primeren za implementacijo v programabilni logiki na vezjih FPGA zaradi možnosti visoke stopnje paralelizacije, zato je naravna izbira za postprocesiranje pri strojnih generatorjih na temelju FPGA, pogosto pa se uporablja tudi pri kvantnih generatorjih, kjer je vezje FPGA dokaj običajen sestavni del naprave in služi tudi drugim namenom. Manj primeren je ta ekstraktor za implementacijo na običajnih procesorjih zaradi skaliranja zahtevnosti z zmnožkom dimenzij, zato pri velikih parametrih n in m obdelava v realnem času ni mogoča in ekstrakcija predstavlja ozko grlo. Toeplitzev ekstraktor se pogosto uporablja tudi za ojačevanje zasebnosti (angl. privacy amplification) v protokolih za kvantno distribucijo ključev, kjer je cilj iz začetnega zaporedja pridobiti povsem naključen ključ za šifriranje ob znani verjetnosti, da ima napadalec možnost pridobiti (denimo s prisluškovanjem) delno informacijo o začetnem zaporedju.
Nekateri standardi za generatorje naključnosti (denimo NIST 800-90B) zahtevajo, da so generirani naključni biti pred izhodom iz naprave obdelani tudi s kriptografsko zgoščevalno funkcijo, denimo iz družine SHA. V bistvu gre tu za kombinacijo strojnega in programskega psevdo-naključnega generatorja, cilj pa je izboljšati robustnost, saj ob nepravilnem delovanju strojnega dela generatorja dobimo vsaj psevdo-naključna števila. Morebitna pomanjkljivost je nezmožnost preverjanja izhodnega niza, ki je vsaj psevdonaključen in zato prestane vse statistične teste, tudi če generator ne ustvarja prav nič entropije. Pri Toeplitzevem ekstraktorju težave s primarnim generatorjem s statističnimi testi lahko zaznamo. Ker so implementacije Toeplitzovega ekstraktorja v vezjih FPGA relativno "poceni", je smiselno uporabiti oboje, torej Toeplitzovo ekstrakcijo za pridobivanje visokoentropijskega niza, ki je lahko podvržen testiranju v realnem času, ter kriptografsko zgoščevanje tega niza pred izhodom iz generatorja kot dodatni zaščitni ukrep.

4 Ocena morebitne grožnje zaradi kvantnih računalnikov

Ker so kvantni računalniki (resda z majhnim številom kubitov) postali realnost, se zastavlja vprašanje, ali kvantni računalniki oz. kakšne druge kvantne naprave morebiti predstavljajo grožnjo za generatorje naključnih števil. Naj spomnimo, da so kvantni računalniki resna grožnja za asimetrično šifriranje z javnimi ključi (algoritme, kot je RSA), saj obstaja kvantni algoritem (Shorov algoritem), ki lahko eksponentno pohitri matematično operacijo določanja faktorjev velikih števil, kar je sicer računsko zelo zahtevno opravilo na klasičnih računalnikih. Zaradi tega se zdaj intenzivno razvijajo t.i. post-kvantni algoritmi. Po drugi strani je za simetrično šifriranje (algoritme, kot je AES) grožnja kvantnih računalnikov bistveno manjša, saj je mogoča samo kvadratična pohitritev (Groverjev algoritem), zato zadostuje podvojitev velikosti uporabljenih ključev.

4.1 Tveganja pri generatorjih psevdonaključnih števil

Pri generatorjih psevdonaključnih števil (PRNG) je tveganje majhno. Ogroženi so zgolj algoritmi, katerih varnost temelji na predpostavkah visoke računske zahtevnosti, ko sta Blum Micali in Blum Blum Shub, kjer varnost zagotavlja zahtevnost razstavljanja števil na prafaktorje oziroma računanja diskretnih logaritmov. Ti algoritmi se sicer zaradi zelo visoke računske zahtevnosti v praksi izjemno redko uporabljajo, ker so za večino praktičnih namenov prepočasni. Za druge PRNG je načeloma možna kvadratična pohitritev poskusov razbijanja, kar pa se lahko ponovno reši s podvojitvijo števila bitov v notranjem stanju generatorja. (Novejši predlogi standardov to že upoštevajo in zahtevajo uporabo generatorjem z večjim številom bitov notranjega stanja. Implementacija v skladu s temi novimi napotki je smiselna že zdaj, zelo priporočljiva pa v obdobju naslednjih desetih let.) V praksi so napadi na generatorje naključnih števil z grobo silo sicer malo verjetni.

4.2 Tveganja pri ne-kvantnih strojnih generatorjih naključnih števil

Tveganja pri ne-kvantnih strojnih generatorjih naključnih števil ocenjujemo kot izjemno majhna. Varnost tovrstnih generatorjev namreč temelji na naključnosti, ki izvira iz kompleksne dinamike fizikalnih sistemov (denimo iz kaotičnega odziva ali naključnih termičnih fluktuacij). Tudi če za opis le te zadošča klasična fizika, ki omogoča simulacije z zgolj polinomsko časovno zahtevnostjo (kar jih načeloma uvršča med "časovno učinkovite" simulacije), je praktično nemogoče simulirati te procese z zadostno numerično natančnostjo, da bi se dalo iz znanega trenutnega stanja generatorja sklepati na delovanje po zadosti dolgem času, v praksi že po nekaj nanosekundah. To niti ni odvisno od tipa uporabljenega računalnika: kvantni računalniki ne omogočajo prav nobene pohitritve pri simulaciji klasičnih fizikalnih sistemov. Kvalitetno izdelan strojni generator naključnih števil zato ni ranljiv niti na "klasične napade" niti na "kvantne napade" s simulacijami, ki bi omogočale napovedovanje izhodnih vrednosti iz generatorja.

4.3 Tveganja pri kvantnih strojnih generatorjih naključnih števil

Tveganja pri kvantnih strojnih generatorjih so nična pri idealnih generatorjih in izjemno majhna v dejanskih napravah. Procesi meritve v kvantni mehaniki so po trenutno znanih teorijah in v okviru najbolj sprejetih interpretacij povsem naključni. Tveganja lahko izvirajo samo iz napak v implementaciji naprave oziroma če ima napadalec dostop do naprave. Kvantni računalniki stopnje tveganja tako ne spremenijo.

5. Fizična zaščita strojnih generatorjev

Za strojne generatorje naključnih števil veljajo podobne zahteve kot za vse kriptografske module. Odporni morajo biti na vplive iz okolice (tako namerne kot nenamerne), predvsem pa na **napade z ustvarjanjem napak** (angl. fault attack), kjer skuša napadalec z vplivanjem na generator zmanjšati kvaliteto naključnih števil, ter na **napade s stranskimi kanali** (angl. side-channel attack), kjer skuša napadalec pridobiti informacijo o generiranih naključnih številih. Za oboje je potrebno ščitenje, tako ščitenje pred zunanjimi elektromagnetnimi (EM) valovanji, ki bi vplivala na generator, kot zmanjševanje elektromagnetnih emanacij, ki omogočajo prisluškovanje. V ta namen se uporablja kovinska ohišja in prevodne prevleke. Preverjanje odpornosti na zunanje sevanje (angl. radiation immunity) se lahko opravi na podobne načine, kot se preverja skladnost s standardi za elektromagnetno kompatibilnost (serija standardov IEC 61000), relevantni pa so tudi standardi

TEMPEST. Relevantno je tudi maskiranje, torej prikrivanje korelacij med generiranimi naključnimi števili ter fluktuacijami napajalne napetosti ali toka (zaščita pred napadi z analizo električne moči).
Pomembno je tudi napravo zavarovati pred nepooblaščenimi posegi (angl. tamper resistance). Poskuse posega je možno zaznati (odpiranje ohišja, spremembe napajalne napetosti, spremembe temperature) in generiranje naključnih števil v takem primeru ustaviti (ter izbrisati vse že generirane vrednosti v medpomnilnikih). Pri generatorjih na osnovi FPGA je smiselno generator zaščititi pred spremembami konfiguracije (opisa logičnega vezja) z uporabo kriptiranih bitstreamov v čipih, ki to podpirajo (Intelov Cyclone V ima podporo za 256-bitni AES, ključ je spravljen v čipu in ni berljiv preko nobenega vmesnika; ko je vključen "tamper bit", lahko FPGA konfiguriramo samo z bitstreami, ki so kriptirani prav s tem ključem). Tako zagotovimo integriteto vezja in preprečimo zlonamerne spremembe (spoofing, tampering).
Fizična varnost ter odpornost na različne napade kriptografskih modulov je specificirana v ameriškem standardu FIPS 140-3 (Security Requirements for Cryptographic Modules, posodobljen v letu 2019). Definiranih je več varnostnih nivojev in zahteve za različne nivoje in tipe modulov. Relevanten je tudi mednarodni standard ISO-IEC 19790:2012(E) "Information technology — Security techniques — Security requirements for cryptographic modules". Ta definira štiri varnostne nivoje za različne stopnje občutljivosti ter različna okolja uporabe (na primer varovani prostori, pisarna, prenosne naprave, povsem nevarovani kraji).
Druga priporočila so še:
• ISO/IEC 20543:2019: Information technology - Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408, oktober 2019
• ISO/IEC 15408-1:2022: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model, avgust 2022
• ISO/IEC 15408-2:2022: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components, avgust 2022
• ISO/IEC 15408-3:2022: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components, avgust 2022

6. Testiranje

6.1 Varnostni ukrepi pri strojnih generatorjih

Cilj varnostne evalvacije vira entropije je v okviru nekega (stohastičnega) modela preveriti spodnjo mejo ustvarjene entropije. Drugače povedano: bistvo dobrega strojnega generatorja je dobro določen fizikalni proces nastajanja entropije in poznavanje vseh dejavnikov, ki lahko na ta proces vplivajo. V tem primeru se zanesljivost in varnost naprave izboljša tako, da se možnost izvajanja teh vplivov kar se da zmanjša oziroma v idealnem primeru celo povsem izniči. Nevarnost je očitno predvsem v morebitnih neidentificiranih relevantnih dejavnikih ali v neizbežnih omejitvah pri zaščiti (vsaka naprava denimo potrebuje napajanje in električne povezave za prenos generiranih naključnih števil, kar predstavlja tveganje za vnos elektromagnetnega valovanja v notranjost naprave). Zaradi tega so pomembni tudi ukrepi, ki omogočajo zaznati anomalije v delovanju vira entropije v realnem času (angl. on-line test), predvsem če vir entropije povsem odpove (angl. total-failure test). Takšni testi morajo imeti hiter odziv in morajo biti prilagojeni specifičnemu viru, zato je potrebno vedeti, na kakšne načine lahko vir odpove. Primer so, denimo, različni viri na podlagi nestabilnih nihajnih vezij, kjer nevarnost predstavljata tako popolno prenehanje nihanja kot stabilizacija nihala. Na srečo je

oboje možno zaznati dokaj enostavno z računanjem povprečne vrednosti (test povprečja) in dolžine samih 0 oz. samih 1 (Wald-Wolfowitzev test ali angl. "runs test"). Prvi je dober test za prenehanje osciliranja (kar pokvari povprečje), drugi pa je dober test za stabilizacijo oscilatorja (ker meri statistično neodvisnost zaporedno generiranih vrednosti). V nekaterih generatorjih je možno celo neposredno preverjati količino, ki je osnova za opredelitev naključnosti, denimo stopnjo tresenja (angl. jitter). V ta namen se lahko v vezje FPGA implementira strojno izvedbo naprave za merjenje velikosti tresenja iz časovne sekvence surovih meritev izvedenih na samem oscilatorju. Smiselno je tudi računanje ocene min-entropije kot konservativne mere za naključnost niza bitov ter določiti prag dopustnega (torej minimalno min-entropijo, pri kateri lahko z ekstrakcijo naključnosti načeloma še pridobimo povsem naključna števila) z ustrezno varnostno rezervo.
Poleg samega vira entropije je potrebno preverjati tudi celotno delovanja naprave, vključno s postprocesiranjem in ekstrakcijo naključnosti, saj je tudi pri teh možna odpoved vezja (naključna ali namerno povzročena ob napadu). To je možno z izvajanjem bolj zahtevnih statističnih testov, ki lahko denimo tečejo v procesorskem delu strojnega generatorja (številni FPGA čipi vsebujejo tudi procesorje, na katerih lahko poganjamo tudi relativno zapleteno programsko opremo). Odzivni čas takšnih testov je seveda občutno daljši (časovna skala minut).
Cilj vseh varnostnih ukrepov je hitro zaznavanje napake, alarmiranje in takojšnja ustavitev posredovanja podatkov odjemalcem. Pomembni so tudi t.i. "start-up testi", v katerih preverjamo, ali so generirana števila sploh zadosti dobra za posredovanje odjemalcu. Z njimi preverimo, če se je strojna oprema pravilno inicializirala.

6.2 Standardi

Priporočila različnih standardizacijskih teles pokrivajo več vidikov testiranja. V grobem ločimo med testi pravilnosti delovanja in testi ovrednotenja kvalitete generatorja. Slednji vključujejo tako načine statističnega ovrednotenja količine entropije nedeterminističnih generatorjev kakor tudi nabor testov za preverjanje uniformnosti generiranih naključnih števil. Serija priporočil NIST SP 800 je z vidika testiranja najbolj temeljita, BSI AIS31 podaja le minimalno število testov. Testi se med priporočili v veliki meri prekrivajo, a se predpisani parametri in obseg testiranja razlikujejo.

6.2.1 Testi pravilnosti delovanja

V splošnem se v skupini testov pravilnega delovanja zahteva implementacijo zagonskih testov, testov popolne odpovedi, sprotnih (on-line) testov in testov na zahtevo. Za deterministične dele generatorjev se poleg omenjenih testov zahtevajo tudi testi z znanim odgovorom (angl. known-answer tests). Prav tako je priporočljiv test integritete celotne programske kode.
Testi pravilnosti delovanja se tipično izvajajo na zajetem šumu, redkeje po komponenti za postprocesiranje. Verjetnost napačnih pozitivnih rezultatov mora biti postavljena dovolj visoko. Pričakuje se napaka tipa I (zavrnitev ničelne hipoteze, kadar hipoteza drži), katere verjetnost je manjša ali enaka 10^{-4}. Sprejemljiva verjetnost zaznane napake v delovanju generatorja je ena napaka na 2^{20} zajetih vzorcev. Standard ISO nadalje predpiše največ trikratno ponovitev testa, preden se napaka javi uporabniku generatorja oziroma nastopi preventivni ukrep.
Zagonski testi standarda NIST imajo tri osnovne cilje. Prvi je preveriti, da je porazdelitvena funkcija začetnih bitov enaka porazdelitveni funkciji kasnejših bitov. Drugi cilj je preveriti neodvisnost porazdelitve bitov od njihove lokacije v začetnem zaporedju. Zaznavanje morebitne informacije v

predhodnih zagonskih sekvencah, ki bi lahko bila v pomoč pri napovedovanju zagonskih sekvenc v prihodnosti, je zadnji, tretji cilj zagonskih testov standarda NIST. Na drugi strani, BSI AIS31 vsebuje dva priporočena zagonska testa. Prvi test zazna 48 enakih zaporednih bitov v vmesniku FIFO dolžine 512 bitov. Test sicer ni primeren kot sprotni test, ker ne zazna očitnih statističnih pomanjkljivosti generiranega zaporedja, je pa primeren za testiranje popolne odpovedi. Drugi test je zasnovan kot test frekvenčne porazdelitve 128-tih 4-bitnih simbolov, ki se prevede na statistični test hipoteze s hi-kvadrat porazdeljeno testno statistiko. Test je primeren tudi v funkciji sprotnega testa.
NIST SP priporočila vsebujejo dva odobrena sprotna testa (Repetition Count Test, Adaptive Proportion Test), medtem ko priporočila BSI AIS31 nudijo primere sprotnih testov s testiranjem bitne porazdelitve. Predlagani enostavni testi so primerni le na digitaliziranem šumu, ker že enostavni ekstraktorji entropije preprečijo detekcijo statističnih anomalij. Pri uporabi lastnih sprotnih testov je v skladu z NIST SP potrebno zagotoviti, da (a) uporabljeni test z 99% verjetnostjo zazna ponovitev vrednosti v dolžini 100/H, kjer H predstavlja min-entropijo, in (b) test s 50% verjetnostjo na 50000 zaporednih vrednostih zazna, da se je verjetnost pojavitve poljubne vrednosti povečala z 2^{-H} na $2^{-H/2}$.

6.2.2 Ocena vsebovane entropije

Pred statistično oceno entropije se zahteva definicija stohastičnega modela vira in na podlagi tega tudi ocena teoretične entropije. Definiranje modela je naloga snovalca. Snovalec izhaja iz fizikalnega modela šumnega procesa, ki mora za postopek certificiranja biti ustrezno podprt z argumenti in matematičnimi dokazi.
V naslednjem koraku se izračuna praktična entropija. Račun je odvisen od tega, ali je vir neodvisna in enakomerno porazdeljena naključna spremenljivka (angl. IID - Independent and Identically Distributed) ali ne (npr. ergodična homogena Markova veriga). Lastnost IID bi morala biti razvidna že iz teoretičnega stohastičnega modela. NIST SP 800-90B vsebuje številne statistične teste za preverjanje lastnosti IID, medtem ko BSI AIS31 v ta namen specificira le test T8.
Ničelna hipoteza med ugotavljanjem lastnosti IID je, da ima testno zaporedje lastnost IID. Predpisana je stopnja tveganja 0.001. Zavrnitev ničelne hipoteze z vsaj enim testom pomeni privzeto lastnost ne-IID. Nekateri izmed testov zahtevajo pretvorbo binarnih zaporedij v zaporedja simbolov. Tudi za ta korak sta predpisana dva postopka: (a) simbol je število enic v zaporednih blokih osmih bitov ali (b) zaporedje osmih bitov se interpretira kot osem-bitno število. Za testiranje lastnosti IID NIST SP predpisuje 11 testov mešanja, 4 teste hi-kvadrat in test z dolžino najdaljšega ponovljenega niza. Testi mešanja so: statistika testa odstopanja (Excursion Test Statistic), število urejenih nizov (Number of Directional Runs), najdaljši urejeni niz (Length of Directional Runs), število naraščanj in padanj (Number of Increases and Decreases), število sekvenc na osnovi mediane (Number of Runs Based on the Median), najdaljša sekvenca na osnovi mediane (Length of Runs Based on Median), test povprečja trkov (Average Collision Test Statistic), test maksimuma trkov (Maximum Collision Test Statistic), statistika testa periodičnosti (Periodicity Test Statistic), statistika testa kovariance (Covariance Test Statistic) in statistika testa stisljivosti (Compression Test Statistic). Hi-kvadrat testi so definirani za binarna in ne-binarna zaporedja ter ločeno za preverjanje neodvisnosti in enakosti porazdelitve. V primeru IID vira je za statistično oceno entropije dovolj ocena najbolj pogoste vrednosti (Most Common Value).

NIST za bolj verjeten primer ne-IID vira definira 9 ocen min-entropije. Končna ocena je minimum vseh praktičnih entropij in začetne teoretične entropije. Predpisani postopki za ne-IID vire so: ocena kolizije (Collision Estimate), ocena Markova (The Markov Estimate), ocena kompresije (The Compression Estimate), ocena t-terke (t-Tuple Estimate), ocena najdaljšega ponovljenega niza (Longest Repeated Substring Estimate), ocena večkratne napovedi najbolj pogoste vrednosti v oknu (Multi Most Common in Window Prediction Estimate), ocena napovedi zamika (The Lag Prediction Estimate), ocena napovedi MultiMMC (The Multi MMC Prediction Estimate) in ocena napovedi LZ78Y (The LZ78Y Prediction Estimate).

6.2.3 Testiranje uniformnosti naključnih števil

Ničelna hipoteza, ki jo testiramo, je, da je zajeta sekvenca bitov generirana z idealnim naključnim generatorjem oziroma da je slučajna spremenljivka, ki predstavlja izhod generatorja, neodvisna in enakomerno porazdeljena (IID). Ob tej predpostavki izračunamo porazdelitve različnih statističnih količin, nato pa na generiranih bitih preverjamo skladnost s pričakovanji. Možnosti je neskončno in testi so lahko poljubno zapleteni. Deterministični generatorji (PRNG) po definiciji ne morejo zadostiti poljubno zapletenim testom, zato preverjamo samo smiselne lastnosti (kaj je smiselno, pa je odvisno od načina uporabe generiranih naključnih števil). Prava naključna števila iz strojnih generatorjev (TRNG) bi morala zadostiti prav vsem statističnim testom, tudi poljubno zapletenim. Ta lastnost je pomembna za aplikacije v preizkusih osnovnih fizikalnih zakonov (denimo Bellovi testi v kvantni mehaniki) in v kriptografiji pri najvišjih stopnjah varnosti. V praksi so seveda testi omejeni z računsko močjo in pomnilniškimi kapacitetami.

BSI AIS31 predpisuje 8 testov, od katerih se testi T6, T7 in T8 opravijo neposredno na zajetem šumu. Predpisani testi so: T0: nepovezanost (Disjointness test), T1: monobitnost (Monobit test), T2: poker (Poker test), T3: sekvence enakih vrednosti (Run test), T4: dolge sekvence (Long run test), T5: avtokorelacija (Autocorrelation test), T6: enakomerna porazdelitev (Uniform distribution test), T7: multinomska porazdelitev (Comparative test for multinomial distributions) in T8: entropija (Entropy test).

Standard ISO/IEC 18031:2011 predpisuje teste T1 do T4 tudi kot sprotne teste pravilnosti delovanja. Obširno in bolj temeljito testiranje je priporočeno v NIST SP 800-22. Poleg osnovnih testov ničelne hipoteze, ki vsebujejo tudi različice AIS31 testov pri širšem razponu vhodnih parametrov, se zahteva statistično ovrednotenje zanesljivosti posameznega testa. To dosežemo z večkratno ponovitvijo testa na različnih zaporedjih (vsaj 1000-krat), pri čemer posamezno testno zaporedje vsebuje od 10^3 do 10^7 bitov (spodnja meja se ne priporoča). Delež primerov, ko ničelne hipoteze ne moremo zavreči, se mora nahajati v 99% intervalu zaupanja. Dodatno je potrebno preveriti uniformnost distribucije P-vrednosti posameznih testov, za kar je predviden test enakosti porazdelitev (Goodness-of-Fit Distributional Test) pri stopnji tveganja 0.0001. Predvideni minimalni osnovni testi ničelne hipoteze so: test monobitnosti (The Frequency or Monobit Test), blokovni frekvenčni test (Frequency Test within a Block), test sekvenc (Runs test), test najdaljše sekvence enic v bloku (Test for the longest run of ones in a block), test binarnega matričnega ranga (Binary matrix rank test), test z diskretno Fourierjevo transformacijo (Discrete Fourier transform test), test predlog brez prekrivanja (Non-overlapping template matching test), test predlog s prekrivanjem (Overlapping template matching test), Maurerjev univerzalni statistični test (Maurer's "universal statistical" test), test linearne zahtevnosti (Linear complexity test), zaporedni test (Serial test), približni entropijski test

(Approximate entropy test), test tekoče vsote (Cumulative sums test), test naključnosti ciklov (Random excursions test) in alternativni test naključnosti ciklov (Random excursions variant test).

6.3 Računalniški programi

Testiranje generatorjev naključnih števil zahteva implementacijo statističnih testov v računalniški kodi. V izogib napačnim interpretacijam in programskim napakam tako BSI kot NIST nudita referenčne implementacije zgoraj opisanih testov. Poleg teh testnih zbirk je na voljo vrsta specializiranih statističnih testov naključnih števil, ki so pridobila široko podporo strokovne javnosti. Ti testi pogosto vsebujejo standardne teste kot podmnožico, predvsem pa so zasnovani za preverjanje statistične naključnosti z alternativnimi prijemi.
Zbirka testov AIS_31_testsuit je implementacija statističnih testov v Javi, ki so opisani v predlogu funkcionalnih razredov generatorjev naključnih števil iz leta 2011. Testi T1 - T8 so relevantni za priporočila AIS20 in AIS31.

SP800-90B_EntropyAssessment je zbirka testov kvalitete vira entropije v skladu s priporočili NIST SP800-90B sekcija 3.1. Za zbirko je na voljo krajši priročnik [McKay 2016]. Avtor izvorne kode je Chris Ceil (NIST). Zbirka vsebuje teste IID, ustrezno ovrednotenje min-entropije, zagonske teste in program za izračun entropije po komponenti za ekstrakcijo.

NIST SP 800-22rev1a je zbirka statističnih testov iz leta 2010 za validacijo deterministčnih in nedeterminističnih generatorjev naključnih števil po priporočilih NIST SP 800. Za osnovnih 15 testov se preverja tudi statistična zanesljivost samega testiranja.

Dieharder verzija 3.31.1 je zbirka 61 testov naključnih števil, katere avtorji so Robert Brown, Dirk Eddelbuettel in David Bauer. Zbirka je naslednik starejše Diehard verzije z razširjenim naborom parametrov. Vključena je tudi zbirka testov NIST. Prednost te implementacije testov je podpora za zelo dolga zaporedja, ki presegajo priporočeno zgornjo mejo, ki jo podaja NIST, to je 10^7 vzorcev.

Poleg standardiziranih testov je priporočljiv preizkus naključnosti generiranih zaporedij z orodji, kot so:

- TestU01, zbirka generičnih statističnih testov uniformnosti naključnih števil avtorja Pierra L'Ecuyera iz Univerze v Montrealu;
- Projekt R, programsko okolje za statistično računanje, ki sta ga sprva razvila Robert Gentleman in Ross Ihaka z Oddelka za statistiko Univerze v Aucklandu in je kasneje prerasel v projekt na osnovi licence GNU;
- rngtest, paket za FIPS 140-2 testiranje naključnih števil;
- PractRand, C++ knjižnica psevdonaključnih generatorjev in statističnih testov;
- gjrand, visoko ocenjen generator psevdonaključnih števil in zbirka testov naključnih števil.

Pred leti je nabor dieharder veljal za najbolj popoln nabor statističnih testov, danes pa ga nekateri smatrajo za zastarelega. Dobro se je uveljavil nabor **TestU01**, ki je dobro dokumentiran v objavljenih člankih in v navodilih za uporabo. Vsebuje nekaj sklopov testov (SmallCrush, Crush, BigCrush), ki se pogosto uporabljajo. PractRand se odlikuje po možnosti testiranja poljubno izjemno dolgih sekvenc.

6.4 Certificirano kvantno generiranje naključnih števil

V zadnjih letih se je močno uveljavilo preverjanje ustreznosti virov entropije, ki temelji na modeliranju delovanja naprave in empiričnem določanju parametrov tega modela. Tu se zastavlja vprašanje veljavnosti predpostavk, na katerih temelji model (denimo zaradi neznanih oz. neupoštevanih dejavnikov vpliva, zaradi zlonamernega delovanja, ali pa zaradi staranja naprave, ki lahko spremeni vrednosti parametrov), zato vedno obstaja nevarnost, da naprava dejansko generira manj entropije, kot pričakuje uporabnik, on-line testi pa tega ne zaznajo, če gre za nepravilnost, katere posledice niso enostavno merljive. Izkaže se, da kvantna fizika omogoča preverjanje delovanja generatorja na empiričen način, pri čemer niso potrebne prav nobene predpostavke o delovanju naprave (razen privzete veljavnosti kvantne mehanike same) [Acin2016], zato ta pristop imenujemo tudi "od naprave neodvisno" generiranje naključnosti (angl. device-independent randomness generation). Entropijo naključnih števil, generiranih z nekaterimi tipi kvantnih generatorjev, je namreč možno certificirati s protokolom, ki izrablja enega izmed najbolj nenavadnih kvantnih pojavov, kvantno prepletenost. Prepletenost je lastnost sestavljenih kvantnih sistemov, pri katerih so rezultati meritev, opravljenih na posameznih sestavnih delih sistema, med seboj korelirani močneje, kot bi bilo to možno v okviru klasične fizike pod predpostavko t. i. lokalnega realizma (lokalnost pomeni, da informacije potujejo z omejeno hitrostjo, realizem pomeni, da so rezultati meritev vnaprej določeni, meritev jih le razkrije). Obstoj kvantne prepletenosti je bil neizpodbitno potrjen v poskusih kršenja Bellove neenakosti v dvojicah kvantnih naprav.

Protokol omogoča stalen nadzor nad kvantno entropijo, ki jo proizvaja sistem, in tako certificira pravo naključnost v realnem času. V kvantnih generatorjih, ki so povsem neodvisni od naprave (angl. device independent, DI), je certificiranje možno brez privzetkov o načinu delovanja ali implementaciji naprave. To pomeni, da model vira entropije sploh ni potreben, prav tako nas ne rabijo skrbeti nasprotniki. Poudariti je treba, da s tem protokolom ne certificiramo samo naključnosti z vidika uporabnika, temveč tudi zasebnost naključnih števil. To sledi iz fizikalnega dejstva, da kršitev Bellove neenačbe uporabniku pove, da je kvantno stanje v paru naprav čisto in prepleteno, kar implicira, da ne more biti korelirano z okolico oz. morebitnim tretjim opazovalcem. Stopnja kršitve Bellove neenačbe omogoča to maksimalno stopnjo korelacije z okolico kvantificirati. Za preizkus Bellove neenačbe ni potrebno vedeti nič o delovanju naprave, izmeriti moramo le statistične lastnosti rezultatov meritev.

Generatorji DI so žal izjemno počasni (velikostni red bitov na sekundo) in so še vedno na stopnji demonstracijskih naprav (proof of concept). Obstajajo bolj praktične rešitve (delna neodvisnost od naprave, angl. semi-device-independent), kjer je potrebno nekaj predpostavk o delovanju naprave, ki pa so preprosto preverljive. Eden izmed ciljev evropskega projekta QRANGE (projekt H2020, 2018-2021) je tudi razvoj tovrstnega generatorja s samo-testiranjem (angl. self-testing QRNG).

6.5 Standardi za kvantne generatorji

V okviru skupine QSG (Quantum Standards group) pri EITCI (European Information Technologies Certification Institute) trenutno potekajo prizadevanja za pripravo zahtev in standardov za kvantne generatorje naključnih števil, in sicer ločeno za generatorje, ki uporabljajo kvantno prepletenost in tiste, ki jo ne.

7. Generatorji naključnih števil za kvantno distribucijo ključev

Kvantni generatorji naključnih števil se pogosto omenjajo kot ključni sestavni del sistemov za kvantno distribucijo ključev (angl. quantum key distribution, QKD). To je smiselno, če so pri tem mišljeni certificirani kvantni generatorji na osnovi kvantne prepletenosti, ki jamčijo tako naključnost kot zasebnost, žal pa ti generatorji trenutno še niso zadosti zrela tehnologija. Kvantni generatorji, ki ne temeljijo na prepletenosti, nimajo bistvene *konceptualne* prednosti pred kvalitetnimi nekvantnimi strojnimi generatorji. Trenutno torej ni dobrih argumentov, da bi današnji sistemi za QKD morali nujno uporabljati QRNG, kvaliteten klasičen TRNG je tudi ustrezen.

8. Zaključek

Povzemimo glavna opažanja:

1. Naključna števila so ključen vir v kriptografiji. Dokumentirani so številni primeri slabih implementacij ali namerno kompromitiranih generatorjev. Implementacija mora zagotavljati varnost, za kar obstaja nabor dobrih praks in formalnih zahtev (opisujejo jih strokovna priporočila in standardi različnih teles).
2. Kvantni generatorji naključnih števil (QRNG) so **zrela tehnologija**, ki je na voljo v obliki čipov, razširitvenih kartic in samostojnih naprav. Na trgu najdemo rešitve na osnovi optičnih pojavov, kvantnega tuneliranja in radioaktivnih razpadov. Razvoj gre v smeri poceni virov za naprave IoT, zelo hitrih generatorjev ter certificiranih kvantnih generatorjev, ki poleg naključnosti garantirajo tudi popolno zasebnost števil in so tako odporni tudi na grožnje, ki jih sploh še ne poznamo. Varnost je posledica osnovnih načel kvantne mehanike in v znanstveni skupnosti velja širok konsenz, da je kvantna mehanika pravilen opis sveta.
3. Kvalitetni strojni generatorji pravih naključnih števil (TRNG) so postali **standardna komponenta** sodobnih mikroprocesorjev in kriptografskih modulov. Kot vir entropije se danes največ uporablja oscilatorje in metastabilna digitalna vezja, v prihodnje lahko pričakujemo prehod na kvantne generatorje. Pomembne so tudi pravilne izvedbe ekstraktorjev entropije.
4. Razvoj generatorjev psevdonaključnih števil gre v smeri robustnih rešitev, ki so **odporne** na delno kompromitirane vire entropije za semena (denimo algoritmi iz družine Fortuna). Smiselno je v entropijski bazen (angl. entropy pool) vnašati entropijo iz čim več različnih virov.
5. Trenutno potekajo revizije nacionalnih standardov za generatorje naključnih števil in pričakovati je **konsolidacijo** terminologije in priporočil.
6. Kvantni računalniki **ne predstavljajo resnega tveganja** za generiranje naključnih števil. (Morda velja celo nasprotno: ena izmed možnih uporab kvantnih računalnikov v prihodnosti je certificirano in od naprave neodvisno generiranje naključnih števil.)
7. Kljub temu je pri programskih generatorjih psevdo-naključnih števil **smiselno povečati velikost notranjega stanja** (podvojitev dolžine povsem izniči prednost, ki bi jo predstavljal kvantni računalnik, ki lahko izvaja Groverjev algoritem). Iz previdnosti je smiselno s prehodom na generatorje z ustrezno dolgim notranjem stanjem začeti že danes, saj obstaja možnost, da bi se v kakšnem desetletju ali dveh pojavili kriptografsko relevantni kvantni računalniki.

Dodatki

Terminologija

Na področju generatorjev naključnih števil ni poenotene terminologije. Različni standardi v klasifikacijah denimo različno poimenujejo zelo podobne tipe generatorjev. Dodaten izziv je prevajanje teh izrazov v slovenščino. V nadaljevanju je zbranih nekaj opomb o izrazju, ki ga uporabljamo v tem poročilu.

Generatorje lahko v grobem delimo na strojne in programske, podobno kot ločimo strojno in programsko opremo v računalništvu. **Strojne** imenujemo tudi **fizični** generatorji, kadar želimo poudariti, da gre za nekaj oprijemljivega (naprave), in **fizikalni** generatorji, kadar želimo poudariti, da kot vir entropije uporabljamo nek fizikalni proces. Možen izraz je tudi generator pravih naključnih števil, za katerega uporabljamo angleško okrajšavo **TRNG** (angl. true random number generator). Te štiri izraze (strojni, fizični, fizikalni, TRNG) lahko v večini primerov smatramo kot sinonime. **Programske** generatorje imenujemo tudi generatorji psevdonaključnih števil in uporabljamo angleško okrajšavo **PRNG** (pseudo-random number generator).

Nekoga, pred katerim se želimo zaščititi z uporabo kriptografskih tehnik, imenujemo **nasprotnik**, v določenih kontekstih pa tudi napadalec, zlonamernež ali sovražnik, zlasti kadar imamo v mislih aktivne napade na delovanje generatorja naključnih števil.

Pogojevanje (signala), **ekstrakcija entropije** in **post-procesiranje** so zelo sorodni pojmi. Cilj je vselej izboljšati statistične lastnosti niza vrednosti. Pogojevanje (kondicioniranje) se običajno nanaša na zgodnje faze izboljševanja signala, včasih celo v analognem delu naprave. Ekstrakcija entropije je bolj specifičen izraz in opisuje vse postopke, ki povečajo entropijo zaporedja vrednost. Post-procesiranje se običajno nanaša na pozne faze izboljševanja toka podatkov, kar pogosto vključuje uporabo kriptografskih zgoščevalnih funkcij.

"Nezmožnost napovedovanja **za naprej**" in "nezmožnost napovedovanja **za nazaj**" sta prevoda angleških izrazov "forward unpredictability" in "backward unpredictability", ki opisujeta dve lastnosti generatorjev naključnih števil, ki sta kritično pomembni za njihovo uporabo v kriptografiji in se nanašata na odpornost generatorja ob razkritju, ki zadeva nadaljevanje zaporedja (za naprej) oz. pretekle vrednosti (za nazaj). Gre za izraza, tvorjena po analogiji z "zaupnost za naprej" in "zaupnost za nazaj", iz angleških izrazov "forward secrecy" in "backward secrecy", ki se ju v številnih jezikih niti ne prevaja (v francoščini včasih za prvega sicer uporabljajo "confidentialité persistante", v nemščini pa "vorwärts gerichtete Geheimhaltung"). Obstaja več takšnih parov izrazov, ki se nanašajo na zaupnost, napovedljivost, varnost, ipd.

Literatura

A. Acín, L. Masanes: Certified randomness in quantum physics, Nature **540**, 213 (2016).

E. Barker, J. Kelsey: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication (NIST SP) 800-90A revision 1, National Institute of Standards and Technology (2015).

L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Spec. Publ. 800-22 rev 1a, (2010).

L. Dorrendorf, Z. Gutterman, and B. Pinkas. Cryptanalysis of the Windows Random Number Generator. Proc. ACM CCS 2007, ACM Press, pp. 476-485, New York (2007).

P. L'Ecuyer and R. Simard. TestU01: A C Library for Empirical Testing of Random Number Generators. ACM Transactions on Mathematical Software **33**, 4, 22 (2007).

N. Ferguson, B. Schneier, T. Kohno, Cryptography engineering: Design principles and practical applications, Wiley (2010).

M. Herrero-Collantes, J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

J. E. Jacak, W. A. Jacak, W. A. Donderowicz, et al. Quantum random number generators with entanglement for public randomness testing. Sci Rep **10**, 164 (2020).

D. Johnston, Random number generators--Principles and practices, DE-G Press (2018). **Knjiga s praktičnimi nasveti za snovalce strojnih generatorjev naključnih števil.**

G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis, Quantum random number generator based on spin noise, Phys. Rev. A **77**, 054101 (2008).

W. Killmann, W. Schindler, A Proposal for Functionality Classes for Random Number Generators, verzija 2.0 (2011).

R. T. Kneusel, Random numbers and computers, Springer (2018).

C. K. Koç (urednik): Cryptographic engineering, Springer, Berlin (2009).

C. Kollmitzer, S. Schauer, S. Rasss, B. Rainer (uredniki), Quantum random number generation, Springer (2020). **Pregled stanja na področju QRNG.**

Y. Li, Y. Fei, W. Wang, et al., Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol., Sci Rep **11**, 23873 (2021).

K. McKay, User's Guide to Running the Draft NIST SP 800-90B Entropy Estimation Suite (2016).

M. Mosca, M. Piani, Quantum threat timeline report 2020, Global risk institute (2020).

C. Paar, J. Pelzl, Understanding cryptography, Springer (2010).

M. Peter, W. Schindler, A Proposal for Functionality Classes for Random Number Generators, verzija 2.35 – DRAFT (2022).

M. Petrov, I. Radcheko, D. Steiger, R. Renner, M. Troyer, V. Makarov, Independent quality assessment of a commercial quantum random number generator, EPJ Quantum Technology **9**, 17 (2022).

O. Petura, U. Mureddu, N. Bochard, V. Fischer, L. Bossuet: A Survey of AIS-20/31 Compliant TRNG Cores Suitable for FPGA Devices (2016).

M. Piani, M. Mosca, B. Neill, Quantum Random-Number Generators: Practical Considerations and Use Cases, evolutionQ Inc. (2021).

B. Sanguinetti, A. Martin, H. Zbinden, N. Gisin, Quantum Random Number Generation on a Mobile Phone, Phys. Rev. X **4**, 031056 (2014).

W. Schindler (BSI): Security evaluation of Physical RNGs, Workshop on randomness and Arithmetics for Cryptograph on Hardware, Roscoff (2019).

L. Sleem, R. Couturier. TestU01 and Practrand: Tools for a randomness evaluation for famous multimedia ciphers. Multimedia Tools and Applications, Springer Verlag, **79** (33-34), 24075 (2020).

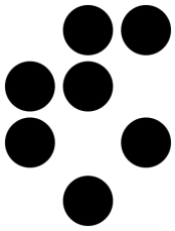
M. Stipčević, Ç. K. Koç, True Random Number Generators, poglavje v knjigi Open Problems in Mathematics and Computational Science, Springer (2014).

M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, M. Boyle: Recommendation for the Entropy Sources Used for Random Bit Generation, (Second DRAFT) NIST Special Publication 800–90B (2018).

B. Yang: True random number generators for FPGAs, doktorska disertacija, KU Leuven (2018).

IQT-QRNG-0121, Quantum Random Number Generators: A Ten-year Market Assessment, Inside Quantum Technologies report, https://www.insidequantumtechnology.com/product/quantum-random-number-generators-a-ten-year-market-assessment/ (2021).

Poročilo IJS-CRP-V1-2119-P1
Verzija 1.0
18. oktober 2022



Institut "Jožef Stefan"
Jamova 39
SI-1000 Ljubljana
https://www.ijs.si/

Avtorji:
Matjaž Depolli
Peter Jeglič
Roman Novak
Erik Zupanič
Rok Žitko

Kontaktna oseba: Rok Žitko, rok.zitko@ijs.si

ROK ŽITKO Digitally signed by ROK ŽITKO
Date: 2022.11.26 19:07:26 +01'00'