Stanje na področju varnih generatorjev: povzetek poročila

Matjaž Depolli
E6, IJS

CRP projekt “Kriptografsko varen generator naključnih števil”
V1-2119, UVTP in ARRS

September 2024

Uvod

- Standardi na področju kriptografsko varnih generatorjev
- Stanje na trgu (vgrajeni generatorji ter samostojne naprave)
- Moderne grožnje (kvantni računalniki)

- Lastnosti kriptografsko varnih generatorjev
- Testiranja generatorjev
- Delitev generatorjev po principu delovanja
- Ozadje strojnega generiranja naključnih števil
- Niso vsa naključna števila enaka: kakšna je preferirana oblika za generiranje
- Kaj so naključna števila

Uporaba naključnih števil

- Simulacije in modeliranje
  - Monte Carlo simulacije
  - Stohastično modeliranje
  - Probabilistični algoritmi
  - Naključno vzorčenje
- Igre
  - Kot ključni element igre (kocke, mešanje kart, ipd)
  - Proceduralno generiranje
  - Loterija
- **Kriptografija**
  - Generiranje ključev oziroma sestavnih delov ključa
  - Avtentikacija
  - Nonce (števila za enkratno uporabo), soli, žetoni
  - Zapolnitev podatkovnih blokov do zahtevane dolžine
  - Dokazi z ničelnim znanjem
  - Generiranje izzivov v protokolu izziv-odziv, ki so izmenjani na odprtem kanalu

Naključna števila v kriptografiji

Ob poznavanju naključnih števil, ki so uporabljena v kriptografskem postopku, lahko nasprotnik popolnoma razvrednoti kriptografsko zaščito (ugane ključ).

Obstaja več zabeleženih varnostnih incidentov, kjer se je to dejansko zgodilo.

Zato uvedemo zahteve za kriptografsko **varne generatorje** naključnih števil

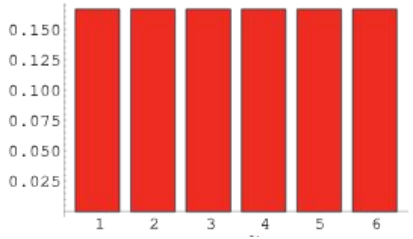
Naključna števila

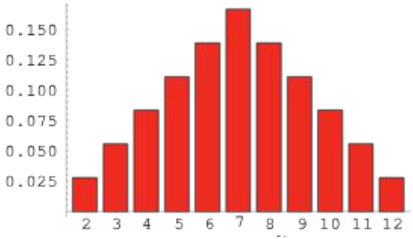
Kaj so naključna števila?

- Nizi števil, ki se jih ne da napovedati
  - Ob poljubno dolgi zgodovini niza ne moremo napovedati naslednje vrednosti v nizu
- Bistvene zahteve:
  - Poznana in nespremenljiva verjetnostna porazdelitev za zalogo vrednosti
  - Neodvisnost naslednje vrednosti v nizu od prejšnje (ni vzorcev)
  - Nespremenljivost v času
- Zahtevi, ki jamčita zasebnost
  - Nezmožnost napovedovanja prihodnosti na podlagi zgodovine
  - Nezmožnost napovedovanja zgodovine na podlagi znanega podniza

Naključni biti

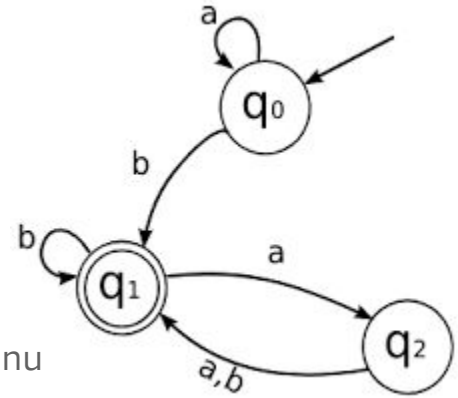
- Niz naključnih bitov je ekvivalenten nizu naključnih števil
- Zanimajo nas le generatorji naključnih bitov
- Iz naključnih bitov lahko generiramo naključna števila na poljubnem območju oziroma s poljubno porazdelitvijo
- Včasih smo delali tako: `m = rand() % 6;`
  Danes programski jeziki ponujajo boljše alternative



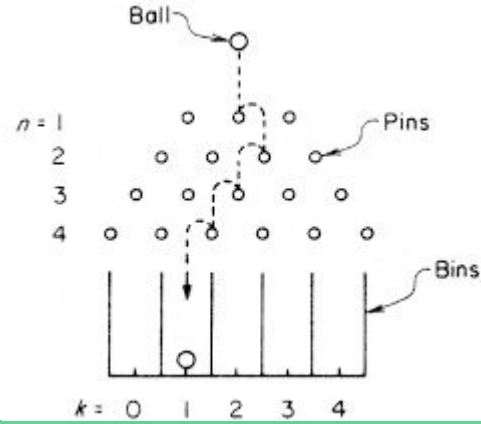


=

Kako generirati naključna števila



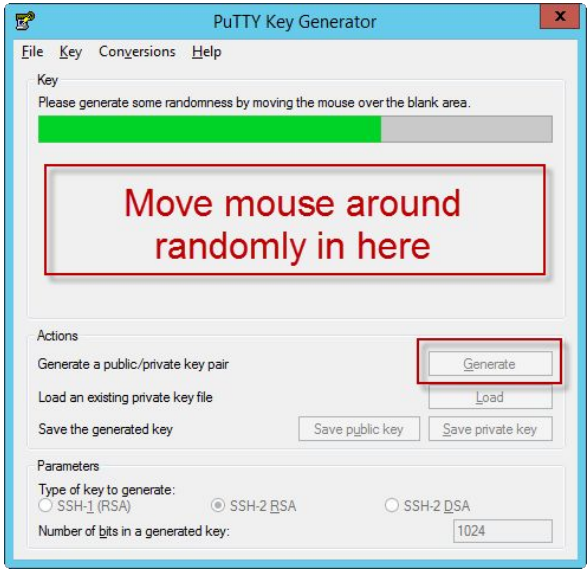
- Deterministično
  - Z algoritmom določimo naslednjo vrednost v nizu
    - Edini način, ki ga poznajo računalniki z arhitekturo po von Neumannu
  - Nizi so le videti naključni, imenujemo jih **psevdo-naključni**
  - Jedro generatorja je seme, ki se deterministično spremeni vsakič, ko generator generira eno število
  - Deterministično sta povezana tudi generirano število in seme
  - Ob poznavanju semena imamo torej zmožnost napovedovanja
- Nedeterministično
  - Generiramo **prava** naključna števila
    - Računalniki to zmorejo le v povezavi z zunanjimi enotami
- Kombiniramo deterministično in nedeterministično



- Želimo jih generirati hitro in veliko

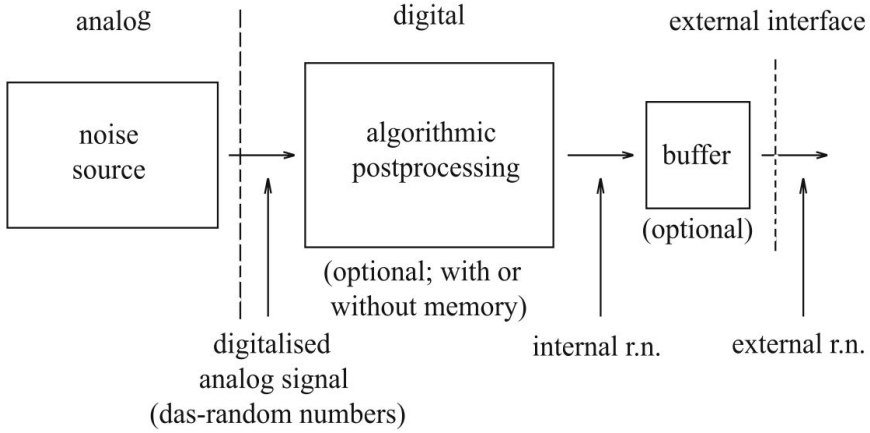
Generiranje pravih naključnih števil

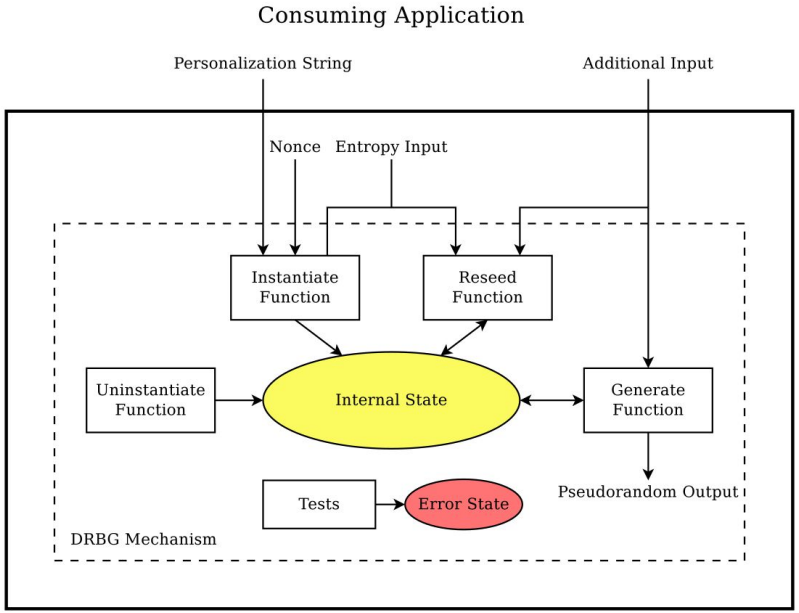
- Generatorji nimajo notranjega stanja, od katerega bi bil odvisen izhod
- Temeljijo na fizičnem viru entropije (naključnosti)
  - Kvantni viri
  - Viri šuma iz težko napovedljivih fizikalnih procesov
  - Viri šuma iz računalniških procesov povezanih z zunanjimi napravami
  - Viri šuma iz uporabnikovega vedenja in akcij
- Pomemben gradnik je ekstraktor naključnosti
  - Je deterministične (algoritem)
  - Poskrbi za enakomerno porazdelitev generiranih naključnih števil
  - Zgosti entropijo naključnega niza



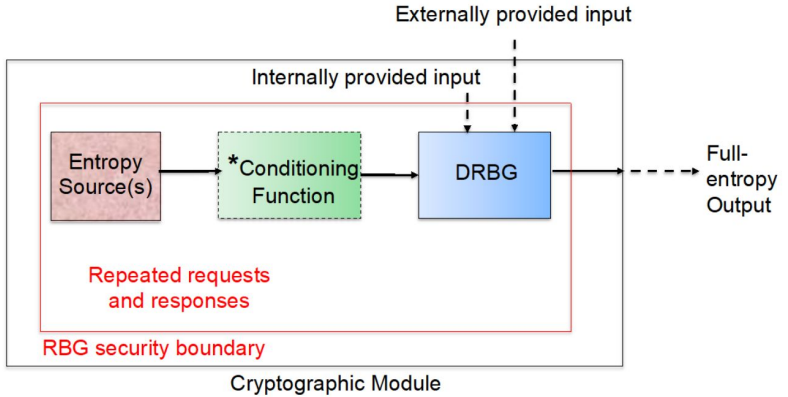
Standardna kriptografsko-varna načina generiranja

BSI





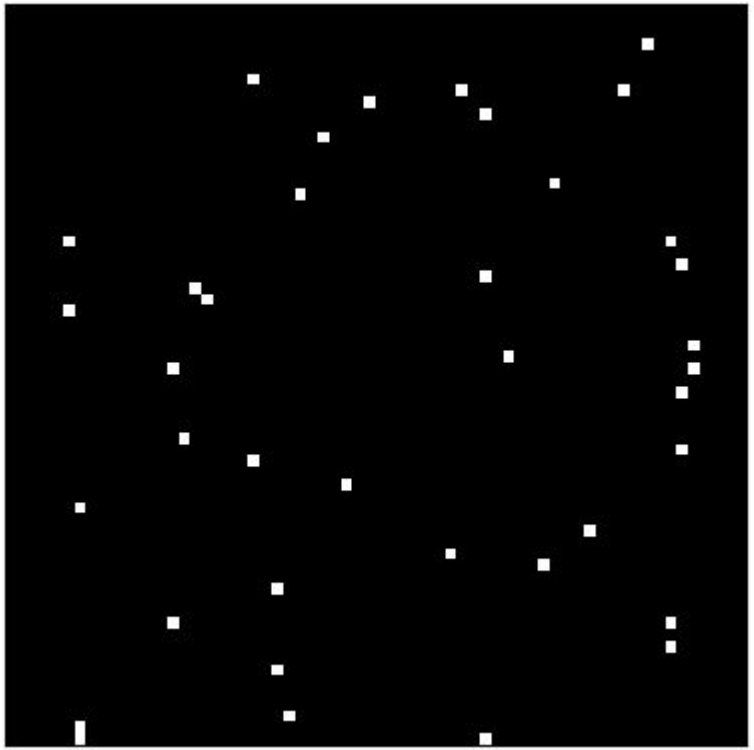
NIST

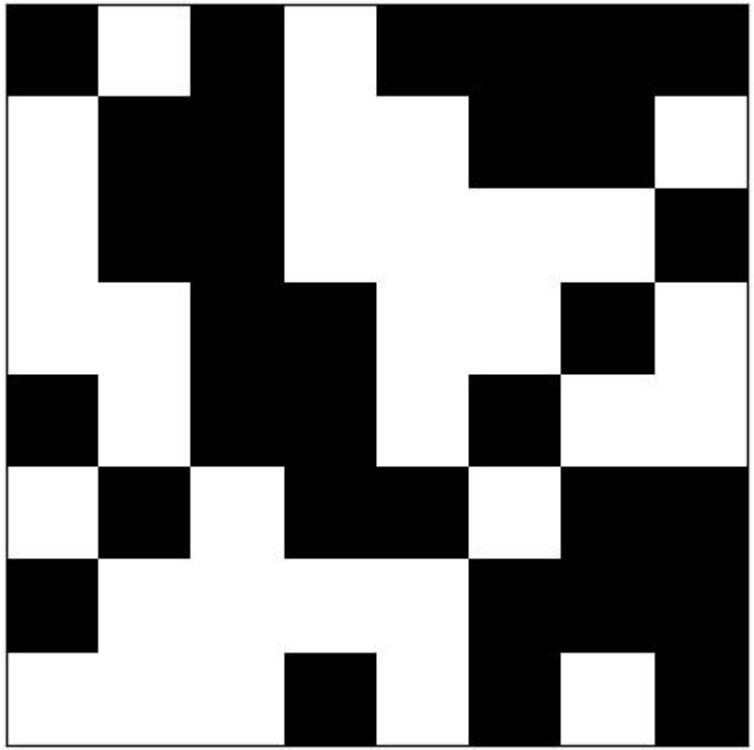


Ekstraktorji naključnosti

Iz strojnih generatorjev v splošnem dobimo medsebojno korelirana števila z neenakomerno porazdelitvijo

- Na osnovi leme o ostanku ob zgoščevanju lahko bitni niz dolžine *m*, ki vsebuje *n* bitov entropije, zgostimo v bitni niz dolžine *n* s (skoraj) polno entropijo
- Toeplitzev ekstraktor je primeren za FPGA vezja
- Na procesorjih običajno implementiramo ekstraktor na osnovi zgoščevalnih funkcij, na primer iz družine SHA-2





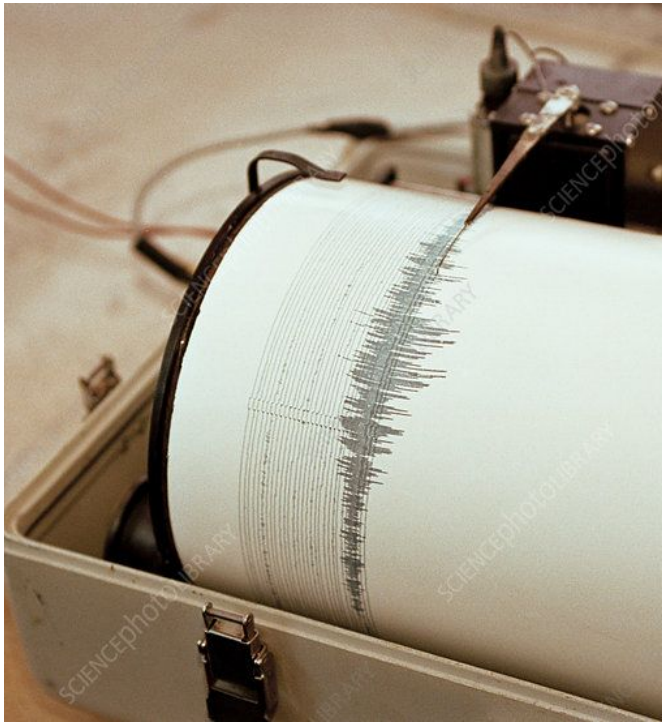
Šum

Šum je nezaželen del signala v fizikalni veličini

- Lahko je ambientalni (iz okolice), lahko izvira iz naprave ustvarjene za generiranje šuma.
- Šum v meritvi izvira iz načina merjenja. To je običajno izvedeno s pretvorbo merjene količine v električno napetost, le-to pa vzorči analogno-digitalni pretvornik (ADC).

Mehanizem šuma

- Kvantni šum (fizikalno nenapovedljivi pojavi)
- Ne-kvantni šum (pogosto izvira iz termičnega)



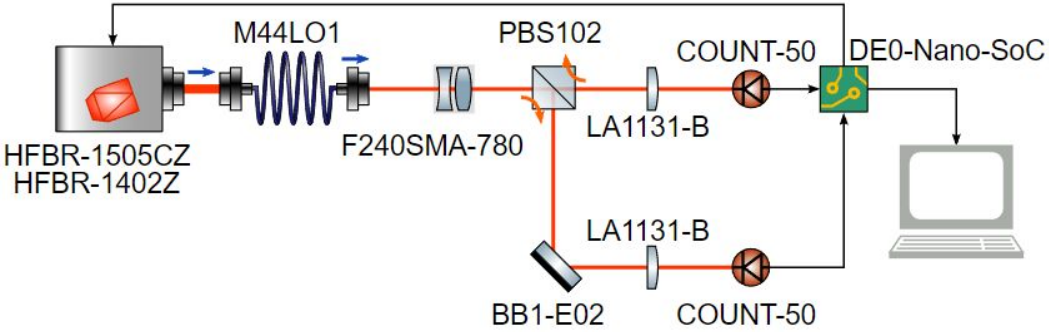
Strojni generatorji naključnih števil

Generatorji, ki temljijo na fizikalnih procesih ustvarjanja entropije

Želimo si

- Stabilnost vira entropije
- Neodvisnost od okolice
- Čim manj staranja
- Merljivost entropije

Kvantni generatorji



Nekaj izvorov kvantnega šuma:

- Radioaktivni razpad
- Optično:
  - Delilniki svetlobe (beam-splitters) - polarizacijski, zrcalni
  - Izvori fotonov, detekcija fotonov
- Stanja atomov (npr: kolektivni spinski šum)
- Kvantni računalniki

Bornovo načelo: “Izidov meritev opravljenih na kvantnomehanskih sistemih ne moremo napovedovati, lahko le določimo verjetnosti za možne izide.”

Stanje na trgu kvantnih generatorjev

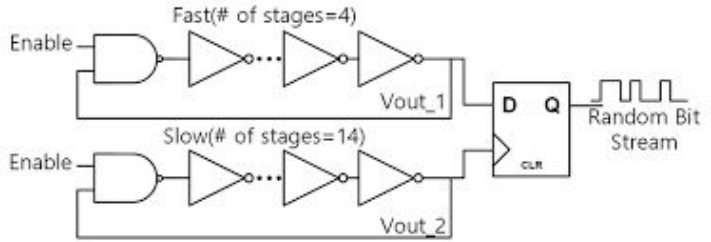
Ti generatorji že sodijo v zrele tehnologije

- V EU je uspešno podjetje ID Quantique, ki ponuja kvantne generatorje v obliki čipa
- Samsung ponuja že 5 generacijo pametnega telefona Samsung Galaxy Quantum. Namenjen je za Južno Korejski trg, kjer v sodelovanju s SK Telecom ponuja izboljšano varnost pri elektronskem poslovanju in avtentikaciji
- V tehnologijo vlaga bančni sektor
- Uporaba naraščа v spletnih igralnicah (PokerStars) in loterijah (francoska in švicarska)
- EU ima program Quantum Flagship, projekt QRANGE (2018-2022) je razvijal kvantni generator

Cene in zmogljivosti

- ID Quantique čipi, pod 10€, 1 Mbit/s
- Razširitvene kartice (PCIe), 1000€, 100 Mbit/s
- Samostojne naprave, 10.000€, 1000 Mbit/s

Ostali pravi naključni generatorji



- Vir entropije so težko napovedljivi fizikalni procesi
  - Lahko so deterministični a kaotični. Kaos: v praksi je nemogoče napovedati prihodnost procesa
  - Termični šum
  - Šum izpeljan iz kvantnih procesov
- Šum ima različne spektralne karakteristike
  - Za dokazovanje pravilnega delovanja generatorja je pomembno je poznati teoretični model šuma
- Zelo pogosti so oscilatorski viri entropije
  - Elektronsko vezje, ki oscilira; frekvenca navadno ni stabilna (jitter)
  - En oscilator (počasnejši) vzorči drugega (hitrejšega)
  - Implementacije so lahko tako v FPGA kot ASIC
- Stanje na trgu:
  - Integrirani so v praktično vse sodobne procesorje (AMD, Intel, ARM, Apple (secure enclave), RISC-V)
  - EU projekt HECTOR je imel cilj izdelati komponente generatorjev naključnih števil
  - Zunanji moduli izumirajo

Lastnosti kriptografsko varnih generatorjev

- **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.

- **fizična zaščita**
- **zaznavanje napak oziroma okvar**

Standardi za kriptografsko varne generatorje

Mednarodni ISO standard je zaenkrat preveč generičen

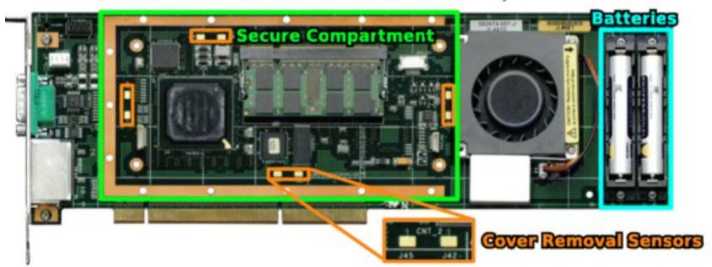
- ISO/IEC 18031:2011 Information technology — Security techniques — Random bit generation

Za kvalitetno implementacijo so bolj pomembni:

- BSI (Bundesamt für Sicherheit in der Informationstechnik / Nemški zvezni urad za varnost v informacijski tehnologiji)
  AIS (Anwendungshinweise und Interpretationen / opombe o uporabi in razlage):
  - **BSI AIS 20**: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators
  - **BSI AIS 31**: Functionality Classes and Evaluation Methodology for Physical Random Number Generators
- NIST (National Institute of Standards and Technology / Ameriški nacionalni inštitut za standarde in tehnologijo)
  - **Special publication 800-90A** Recommendation for Random Number Generation Using Deterministic Random Bit Generators
  - **Special publication 800-90B** Recommendation for the Entropy Sources Used for Random Bit Generation
  - **Special publication 800-90C** Recommendation for Random Bit Generator (RBG) Constructions
  - **Special publication 800-22** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

V okviru skupine QSG (Quantum Standards group) pri EITCI (European Information Technologies Certification Institute) potekajo priprava zahtev za kvantne generatorje

Fizična zaščita



- Kot za kriptografske module je tudi za kriptografsko-varne generatorje naključnih števil nujna fizična zaščita naprave, znotraj katere je generator izveden
- Glavne vrste zaščite:
  - Pred vplivi iz okolja
  - Pred emanacijami elektromagnetnega valovanja (IEC 61000)
  - Pred ustvarjanjem korelacij med generiranimi števili in merljivimi veličinami (napajalna napetost, čas za generiranje števila, ipd)
  - Pred nepooblaščenimi posegi v napravo (odpiranje ohišja, spreminjanje temperature, spreminjanje napajalne napetosti, spreminjanje programja na napravi)
- Uporabimo iste standarde kot za kriptografske module:
  FIPS 140-3, **ISO/IEC 19790**, **ISO/IEC 20543**, **ISO/IEC 15408**

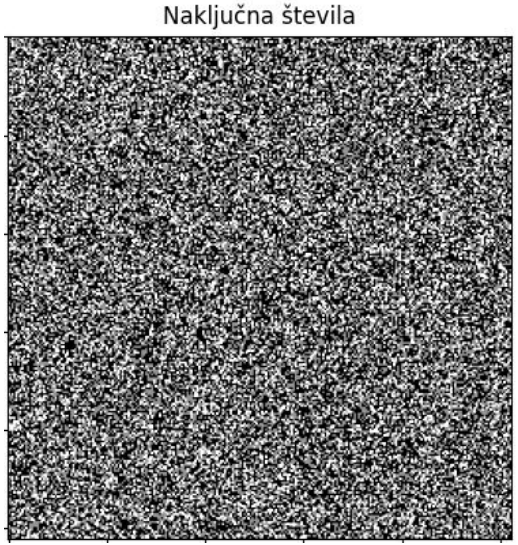
Testiranje

Namen testiranja:

- Preverjanje naključnosti, določanje entropije izhoda
- Kot del varnostnih ukrepov (tudi del NIST in BSI priporočil)
  - Testiranje vira entropije (pred ekstraktorjem naključnosti)
  - Sprotni testi za zaznavanje anomalij v realnem času
  - Zagonski testi

Testiranje naključnosti naj bo čim bližje viru entropije (preverjanje surovih meritev, na katerih vir bazira)

Testiranje celotne naprave oziroma vseh delov, ki jo sestavljajo.



Standardni testi

Obstaja množica obstoječih testov naključnosti, z dobro teoretično podlago:

- FIPS 140-2 vključuje svojo serijo testov naključnosti, za katero obstaja dokumentirana in vzdrževana izvedba *rngtest* (paket na linuxu)
- NIST SP 800 vključuje velik komplet testov skupaj z izvedbo, a njihova izvedba je relativno nerodna
- BSI AIS 31 podaja minimalno število testov skupaj z izvedbo
- Diehard in naslednik Dieharder sta računalniška programa z veliko zalogo testov (vključuje NIST teste) in enostavnim vmesnikom
- TestU01 je najnovejša programska zbirka zelo temeljitih in dobro opisanih testov, ki pridobiva citiranost

Kripto-varni generatorji na modernih napravah

- Windows: zaprtokodni sistem, na starih verzijah (Windows 2000) so bile zabeležene resne pomankljivosti
- Linux: odprtokoden a slabo dokumentiran. Entropijo pobira iz dogodkov na sistemu (premikanje miške, merjenje časa pri interakciji z napravami, merjenje časa pri servisih). Trenutno je v prenovi, sicer je bil v raziskavi leta 2006 označen za zadovoljivega
- iOS: zaprta programska koda in strojna oprema. Temelji na kriptografsko-varnih generatorjih vgrajenih v strojno opremo.
- Android: temelji na Javanski standardni knjižnici SecureRandom. Le-ta pa uporablja entropijo iz Linux sistema, ki je temelj Androida. Na starejši verziji SecureRandom je bila sicer odkrita in odpravljena resna pomanjkljivost.

Grožnja kvantnih računalnikov

- Kvantni računalniki postajajo resničnost
- So grožnja za obstoječe oblike šifriranja
- So potencialna grožnja determinističnim generatorjem
- So minimalna grožnja ne-kvantnim strojnim generatorjem
- Niso grožnja kvantnim strojnim generatorjem