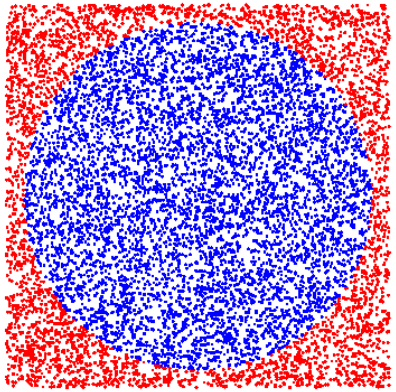
KVANTNA FIZIKA IN GENERIRANJE NAKLJUČNOSTI

Erik Zupanič
Odsek za fiziko trdne snovi (F5)
Institut “Jožef Stefan”

Delavnica v okviru CRP "Kriptografsko varen generator naključnih števil" (V1-2119, UVTP in ARRS), 11. september 2024

POMEN GENERIRANJA NAKLJUČNOSTI

- Zakaj potrebujemo (kvalitetna!) naključna števila?
  - Kriptografija (npr. AES)
  - Kvante komunikacije - QKD
  - Znanost (npr. Monte-Carlo simulacije)
  - Igre na srečo
  - …



POSLEDICE "SLABIH" GENERATORJEV NAKLJUČNIH ŠTEVIL

Man hacked random-number generator to rig lotteries, investigators say

New evidence shows lottery machines were rigged to produce predictable jackpot numbers on specific days of the year netting millions in winnings

'Computer whiz' rigged lott
times a year. Photograph: Brial

Meet Alex, the Russian Casino Hacker Who Makes Millions Targeting Slot Machines

A mathematician-turned-criminal unleashes his agents on casinos around the world. But there's money in the extortion racket, too.

But Alex couldn't just cash out as if he owned an ordinary startup because his business operates in murky legal terrain. The venture is built on Alex's talent for reverse engineering the algorithms—known as pseudorandom number generators, or PRNGs—that govern how slot machine games behave. Armed with this knowledge, he can predict when certain games are likeliest to spit out money—insight that he shares with a legion of field agents who do the organization's grunt work.

Prominent examples [edit]

Predictable Netscape seed [edit]

Early versions of Netscape's Secure Sockets Layer (SSL) encryption protocol used pseud
a PRNG seeded with three variable values: the time of day, the process ID, and the paren
often relatively predictable, and so have little entropy and are less than random, and so th
insecure as a result. The problem was reported to Netscape in 1994 by Phillip Hallam-Bak
CERN Web team, but was not fixed prior to release. The problem in the running code was
Goldberg and David Wagner,[4] who had to reverse engineer the object code because Net
details of its random number generation (security through obscurity). That RNG was fixed
higher) by more robust (i.e., more random and so higher entropy from an attacker's perspe

Microsoft Windows 2000/XP random number generator [edit]

Microsoft uses an unpublished algorithm to generate random values for its Windows opera
quantities are made available to users via the CryptGenRandom utility. In November 2007
Hebrew University of Jerusalem and University of Haifa published a paper titled *Cryptanal*
Generator of the Windows Operating System.[5] The paper presented serious weaknesses in Microsoft's approach at the time. The paper's conclusions were based on disassembly of the code in Windows 2000, but according to Microsoft applied to Windows XP as well.[6] Microsoft has stated that the problems described in the paper have been addressed in subsequent releases of Windows, which use a different RNG implementation.[6]

Possible backdoor in Elliptic Curve DRBG [edit]

The U.S. National Institute of Standards and Technology has published a collection of "deterministic random bit generators" it recommends as NIST Special Publication 800-90.[7] One of the generators, Dual_EC_DRBG, was favored by the National Security Agency.[8] Dual_EC_DRBG uses elliptic curve technology and includes a set of recommended constants. In August 2007, Dan Shumow and Niels Ferguson of Microsoft showed that the constants could be constructed in such a way ...graphic backdoor in the algorithm.[9] In September 2013 *The New York Times* wrote that "the N.S.A. ...door into a 2006 standard adopted by N.I.S.T... called the Dual EC DRBG standard",[10] thereby ... A carried out a malware attack against the American people. In December 2013, Reuters reported that ... by Edward Snowden indicated that the NSA had paid RSA Security $10 million to make ... default in their encryption software, and raised further concerns that the algorithm might contain a ...[11] Due to these concerns, in 2014, NIST withdrew Dual EC DRBG from its draft guidance on random ...ecommending "current users of Dual_EC_DRBG transition to one of the three remaining approved ... as possible."[12]

MIFARE Crypto-1 [edit]

Crypto-1 is a cryptosystem developed by NXP for use on MIFARE chips. The system is proprietary and originally the algorithm has not been published. Upon reverse engineering of the chip, researchers from the University of Virginia and the Chaos Computer Club found an attack on Crypto-1 exploiting a poorly initialized random number generator.[13]

Debian OpenSSL [edit]

In May 2008, security researcher Luciano Bello revealed his discovery that changes made in 2006 to the random number generator in the version of the OpenSSL package distributed with Debian Linux and other Debian-based distributions, such as Ubuntu, dramatically reduced the entropy of generated values and made a variety of security keys vulnerable to attack.[14][15] The security weakness was caused by changes made to the openssl code by a Debian developer in response to compiler warnings of apparently redundant code.[16] This caused a massive worldwide regeneration of keys, and despite all attention the issue got, it could be assumed many of these old keys are still in use. Key types affected include SSH keys, OpenVPN keys, DNSSEC keys, key material for use in X.509 certificates and session keys used in SSL/TLS connections. Keys generated with GnuPG or GNUTLS are not affected as these programs used different methods to generate random numbers. Keys generated by non-Debian-based Linux distributions are also unaffected. The weak-key-generation vulnerability was promptly patched after it was reported, but any services still using keys that were generated by the old code remain vulnerable. A number of software packages now contain checks against a weak key blacklist to attempt to prevent use of any of these remaining weak keys, but researchers continue to find weak key implementations.[17]

PlayStation 3 [edit]

In December 2010, a group calling itself *fail0verflow* announced recovery of the elliptic curve digital signature algorithm ...

VOLUME 69, NUMBER 23 PHYSICAL REVIEW LETTERS 7 DECEMBER 1992

Monte Carlo Simulations: Hidden Errors from "Good" Random Number Generators

Alan M. Ferrenberg and D. P. Landau
Center for Simulational Physics, The University of Georgia, Athens, Georgia 30602
Y. Joanna Wong
IBM Corporation, Supercomputing Systems, Kingston, New York 12401
(Received 29 July 1992)

The Wolff algorithm is now accepted as the best cluster-flipping Monte Carlo algorithm for beating "critical slowing down." We show how this method can yield *incorrect* answers due to subtle correlations in "high quality" random number generators.

PACS numbers: 75.40.Mg, 05.70.Jk, 64.60.Fr

ABSTRACT

The Wolff algorithm is now accepted as the best cluster-flipping Monte Carlo algorithm for beating "critical slowing down." We show how this method can yield *incorrect* answers due to subtle correlations in "high quality" random number generators.

You're Doing IoT RNG

By: Dan Petro, Senior Security Engineer & Allan Cecil, Bishop Fox Alumnus

There's a crack in the foundation of Internet of Things (IoT) security, one that affects **35 billion devices worldwide**. Basically, every IoT device with a hardware random number generator (RNG) contains a serious vulnerability whereby it fails to properly generate random numbers, which undermines security for any upstream use.

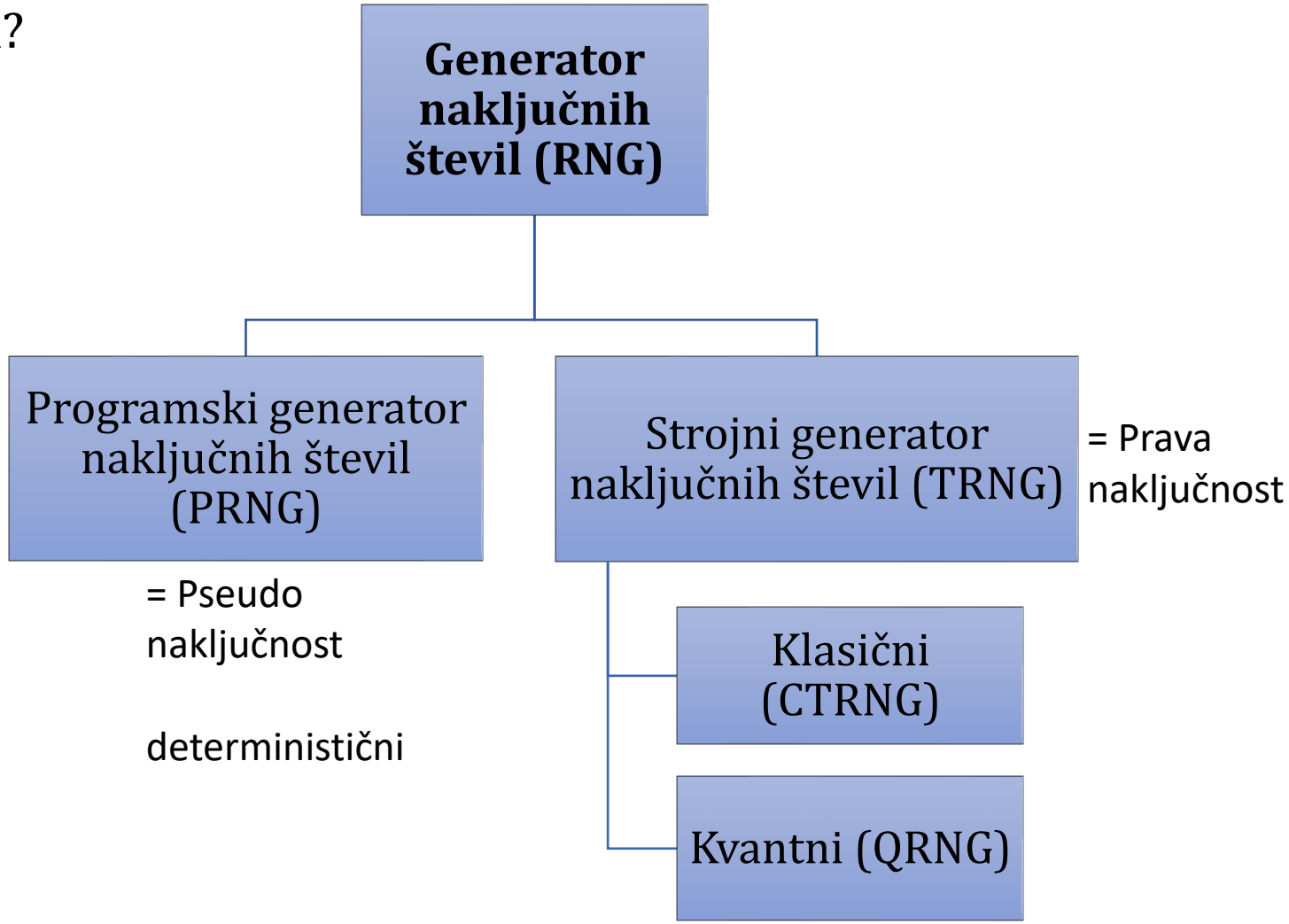
https://en.wikipedia.org/wiki/Random_number_generator_attack

GENERATORJI NAKLJUČNIH ŠTEVIL

- Kako generiramo naključna števila?

Naključna = ne sledijo vzorcu in so zato nepredvidljiva

Statistično testiranje
+
pomembno: zaupanje v RNG



KLASIČNA NAKLJUČNOST

- Primeri: met kovanca in kocke…

- Kaj je vzrok naključnosti? (posledica nezmožnosti poznavanja vseh začetnih pogojev sistema…), deterministični sistemi

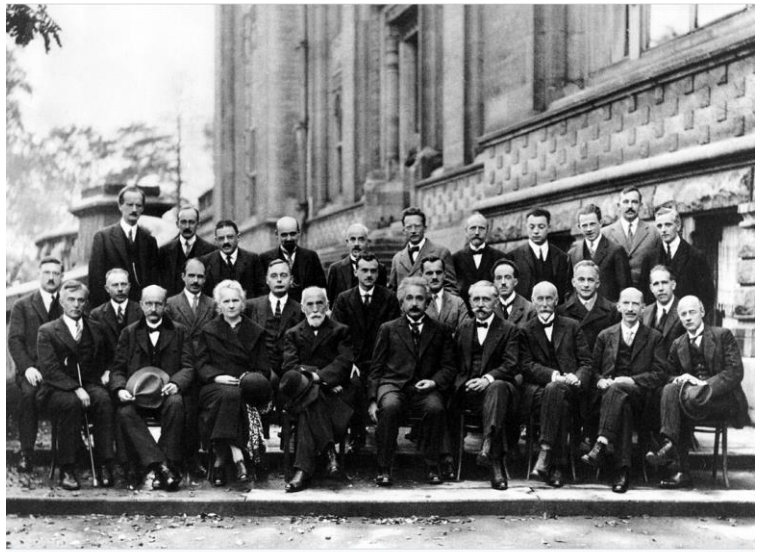
  - Procese je mogoče opisati klasično

  - Kompleksni sistemi

- Vplivanje na začetne pogoje oz. generator naključnosti?

KVANTNA MEHANIKA

- Razvoj v začetku prejšnjega stoletja



- Valovna funkcija opisuje kvantni sistem, ki vključuje vsa možna stanja oz. izide meritve in verjetnosti za posamezen izid

$$|\psi\rangle = \frac{1}{\sqrt{2}}|\,\text{kovanec}\,\rangle + \frac{1}{\sqrt{2}}|\,\text{kovanec}\,\rangle$$

- Koncepti nedoločenosti, superpozicije, prepletenost, …

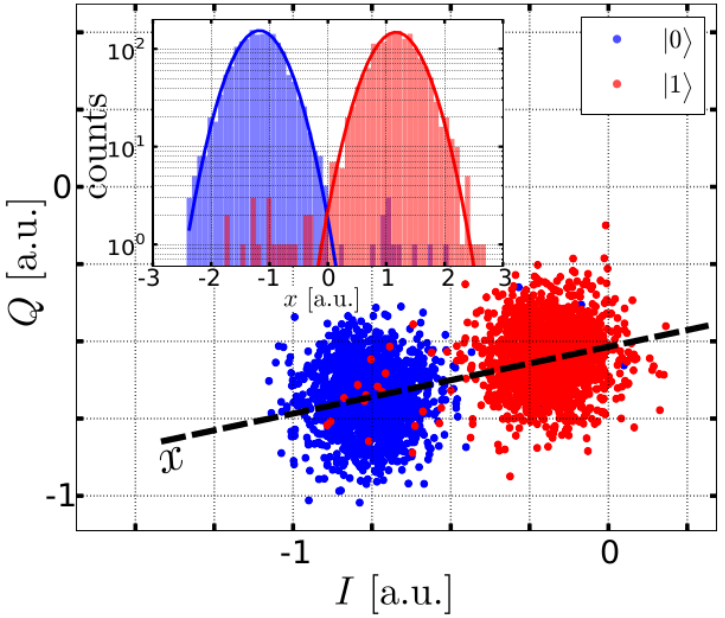
MERITVE NA KVANTNEM SISTEMU

- Superpozicija – sistem obstaja v več možnih stanjih, dokler niso izmerjeni

  -> kolaps kvantne valovne funkcije (verjetnost!)

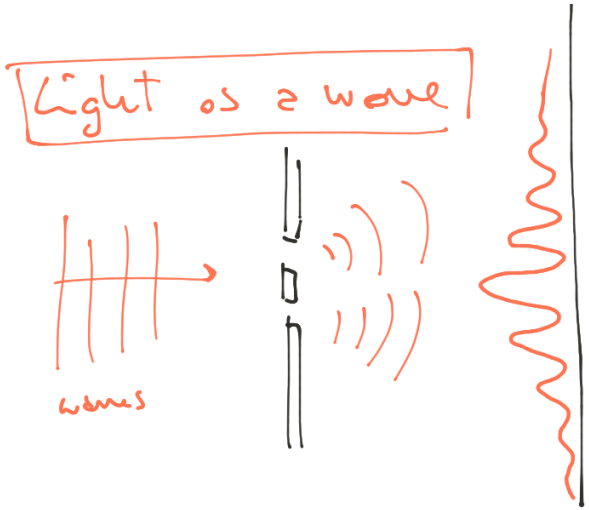
- Je zato kvantna mehanika neuporabna?

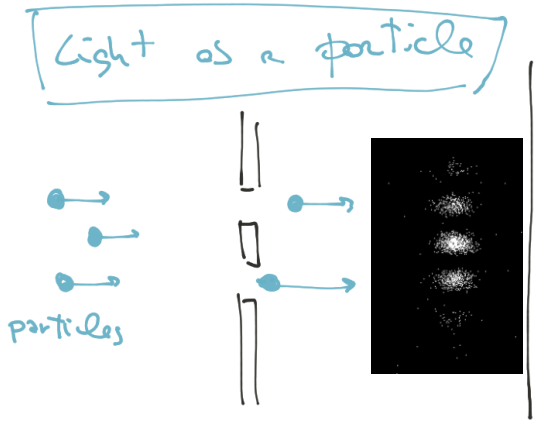
  - Kaj pa če imamo veliko delcev?

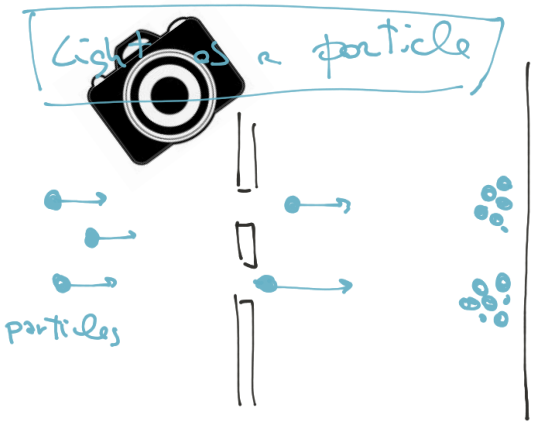


EKSPERIMENTI

- Eksperiment z dvojno režo (kolaps valovne funkcije)







- Eksperiment z EPR (Einstein-Podolsky-Rosen)-pari in Bellove neenakosti

BORNOVO PRAVILO

- Kvantna mehanika ne napoveduje rezultatov meritev ampak verjetnosti izidov meritev

$$P(x) = |\Psi(x)|^2$$

- Je temelj kvantne naključnosti – opisuje kako lahko kvantni sistem vodi do različnih rezultatov z določenimi verjetnostmi

- To fundamentalno naključnost uporabimo za vir entropije v QRNG

KVANTNI GENERATORJI NAKLJUČNOSTI

- Merjenje kvantnega sistema, ki je v superpoziciji, vedno daje naključen rezultat!

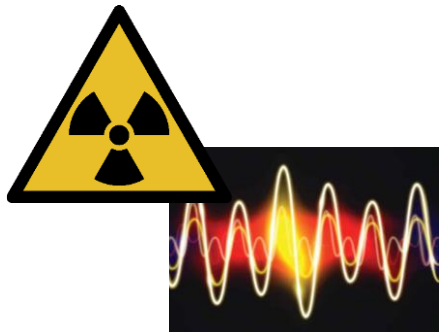
- Je neodvisen od začetnih pogojev in na njega ne moremo vplivati.

- Primeri oz. izvedbe QRNG:
    - optični oz. fotonski
    - elektronski (kvantni+termični šum)
    - radioaktivni razpad
    - …

OSNOVNI PRINCIP STROJNIH (Q)RNG

vir klasične entropije

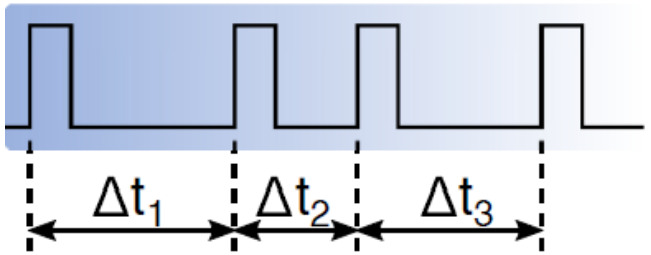
vir entropije → stanje → **merilni sistem (digitalizacija)** → n. bit → **post-procesiranje (ekstrakcija)**



niz stisnemo in zvišamo entropijo

- Statistično lahko ločimo klasični od kvantnega šuma…

DELOVANJE RADIOAKTIVNEGA QRNG



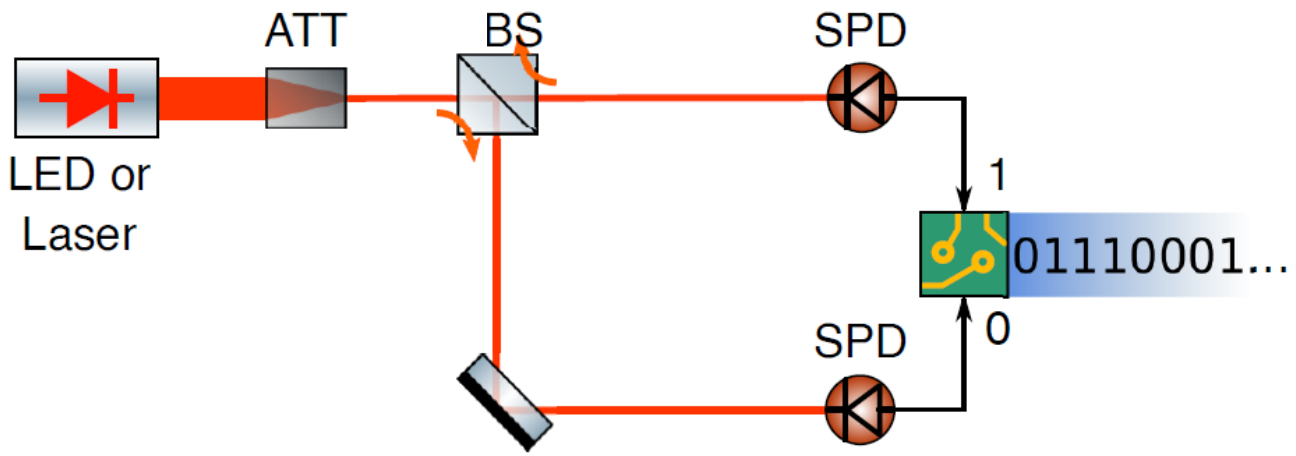
če $\Delta t_2 > \Delta t_1$ zapišemo 1
če $\Delta t_2 < \Delta t_1$ zapišemo 0
če $\Delta t_2 = \Delta t_1$ izpustimo

Razpolovna doba radioaktivnih izotopov je fundamentalna in nespremenljiva lastnost, na katero ni mogoče vplivati s spremembo zunanjih pogojev.

DELOVANJE OPTIČNEGA QRNG

- Vir entropije: superpozicija fotona

- Enostaven a učinkovit način za generiranje kvantne naključnosti



ATT – atenuator
BS – delilnik svetlobe 50:50
SPD – detektor posameznih fotonov
T – prepuščeno, R - odbito

PREDNOSTI (SLABOSTI) QRNG

Prednosti:

- Resnična naključnost (nepredvidljivost)
- Visoka entropija (kvalitetna naključnost)
- Odpornost vira entropije na napade in na zunanje dejavnike
- Zanesljivost

Slabosti:

- Nekatere izvedbe zapletene
- V splošnem počasnejši (kot npr. oscilatorski RNG)
- Dražji
- Tipično večji (možna minituarizacija kot npr. IDQuantiq)

STOPNJA NAKLJUČNOSTI

- Kaj pomeni, da vsa generirana naključna števila niso “enako kvalitetna”?

- Dobro merilo naključnosti je (Shannonova) entropija (merska enota za količino naključnosti)

- Statistični testi (Chi-square…) preverjajo porazdelitev

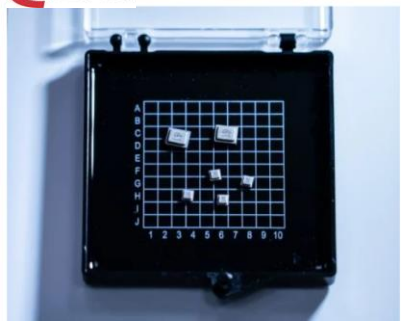
- Standardi (NIST testi, Diehard…) oz. skupine testov

- Ni dovolj dokazati na omejeno dolgem setu števil njihovo ustreznost, potrebno je poznati in modelirati napravo, ki jih generira -> stohastični model

Stohastični model je matematičen opis delovanja QRNG in opisuje vir naključnosti.

TRENUTNO STANJE IN RAZVOJ QRNG

IDQ



Quantis QRNG Chips

System-on-Chip for automotive, computing, critical infrastructure, IoT, mobile, space & security applications

- Six models for different use cases
- Highest security through local and private entropy
- Intrinsically and provably random
- Instant full entropy from the first bit
- Secured and controlled: low risk of silent "break"
- Certified robustness for automotive and space, NIST-compliant
- NIST Entropy Source Validation (ESV) certified on IID SP 800-90B

KETS

QUANTUM-SAFE SOLUTIONS USE CASES NEWS & INSIGHT ABOUT KETS

QUANTUM RANDOM NUMBER GENERATOR

QRNG (Quantum Random Number Generator) is a device that generates truly random numbers using the principles of quantum mechanics. The random numbers generated by QRNGs are truly unpredictable and cannot be replicated, making them valuable for applications that require high levels of randomness and security.

国盾量子 QuantumCTek

TROPOS (QRNG) by QNu Labs

Tropos is a quantum random number generator that extracts the randomness from an optical quantum process. It is based on the principle of time of arrival of photons. The implied scheme consists of continuously measuring the arrival time of photons and encoding the time interval between successive photon arrivals as random bits.

TRENUTNO STANJE IN RAZVOJ QRNG

- Komercialni sistemi na trgu: slabosti neznan “vmesni” del med kvantnim izvorom in izhodom, neznano post-procesiranje, možnost stranskih vrat itd…

ZAKLJUČEK

- kvantni generatorji naključnih števil so fundamentalno nepredvidljivi zaradi kvantne narave izvora entropije in zagotavljajo visoko kvalitetna naključna števila

- potrebno preverjanje in post-procesiranje, ki je v komercialnih sistemih lahko neznanka

- na kvaliteto generiranih števil ima vedno vpliv merilni sistem (klasičen šum, ...) ter post-procesiranje, ki entropijo poveča

Jožef Stefan Institute

Republika Slovenija
Urad Vlade RS za varovanje tajnih podatkov

arrs
JAVNA AGENCIJA ZA RAZISKOVALNO DEJAVNOST REPUBLIKE SLOVENIJE

NASLOV 1

- Vsebina1
- Vsebina 2
- …

VPLIV MERILNE NAPRAVE NA KVANTNI SISTEM

- Merilna naprava vpliva/interagira na sistem in je neodvisna od opazovalca
- Meritev v klasičnem sistemu ne nujno vpliva nanj (ga ne spremeni), v kvantnem pa neposredno spremeni sistem!

- Merilna naprava, kot je fotonski detektor ali prvotni detektor, zaznava specifična kvantna stanja (npr. prisotnost ali odsotnost fotona, polarizacijo fotona) in na podlagi te meritve generira izhodne podatke.

- Kakovost kvantnega generatorja naključnih števil je odvisna od natančnosti merilne naprave. Napake v detekciji, šum ali nepravilnosti v napravi lahko vplivajo na kakovost naključnih števil in posledično na varnost sistemov, ki jih uporabljajo.