



Kvantni generatorji naključnih števil

Avtor: Gašper Harej

Mentor: dr. Peter Jeglič

Somentor: prof. dr. Rok Žitko

Uvod

Naključna števila so osnovni gradnik sodobnih tehnologij:

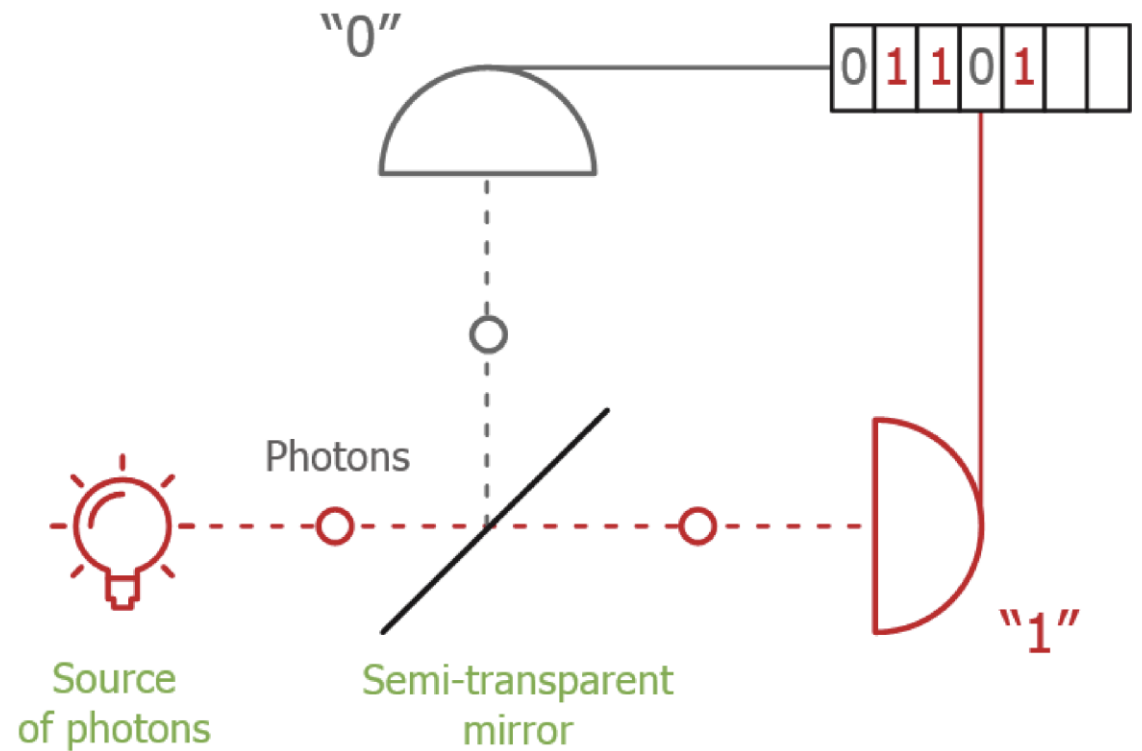
- kriptografija – npr. za varno generiranje ključev
- znanost – npr. simulacije, statistično vzorčenje

Generatorje delimo v tri skupine:

- Psevdonaključni generatorji
- Generatorji pravih naključnih števil
- Kvantni generatorji naključnih števil

Kvantni principi

- Superpozicija: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Bornovo pravilo: $|\alpha|^2 = \text{verjetnost}$
- Kvantna meritev



Izzivi QRNG

V praksi izhodni podatki niso idealni:

Mrtvi časi
detektorjev

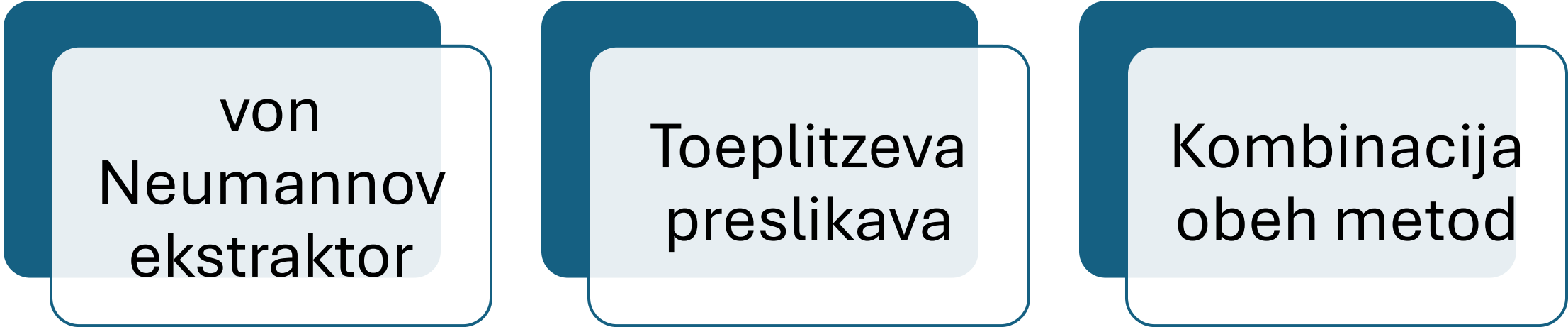
Dvojni
zadetki

Pristranskost



ekstraktorji entropije

Ekstraktorji entropije



von
Neumannov
ekstraktor

Toeplitzeva
preslikava

Kombinacija
obeh metod

Eksperimentalna postavitev

- Qocka:
 - delitev fotonov na delilniku žarka
- PRNG SHA-256 v števnem načinu:
 - Zgoščevalna funkcija
 - Ob znanem semenu je brez entropije



Ocena entropije

- Shannonova entropija:

$$H(X) = - \sum p_i \log_2 p_i$$

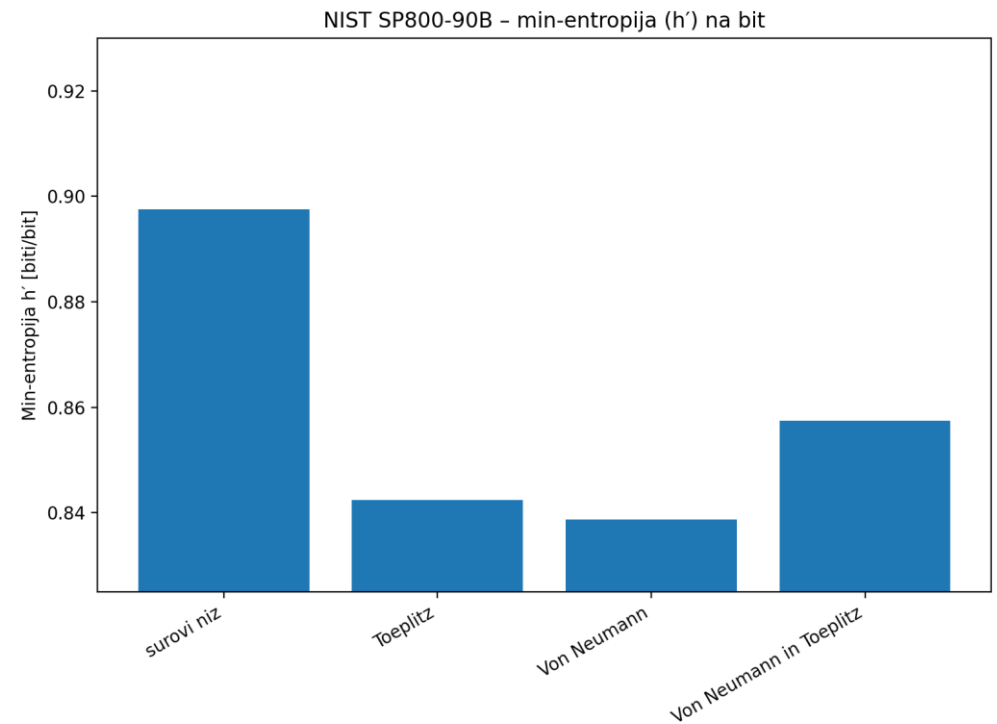
- povprečna količina informacije v izidu

- Min entropija:

$$H_{\infty}(X) = - \log_2 p_{\max}$$

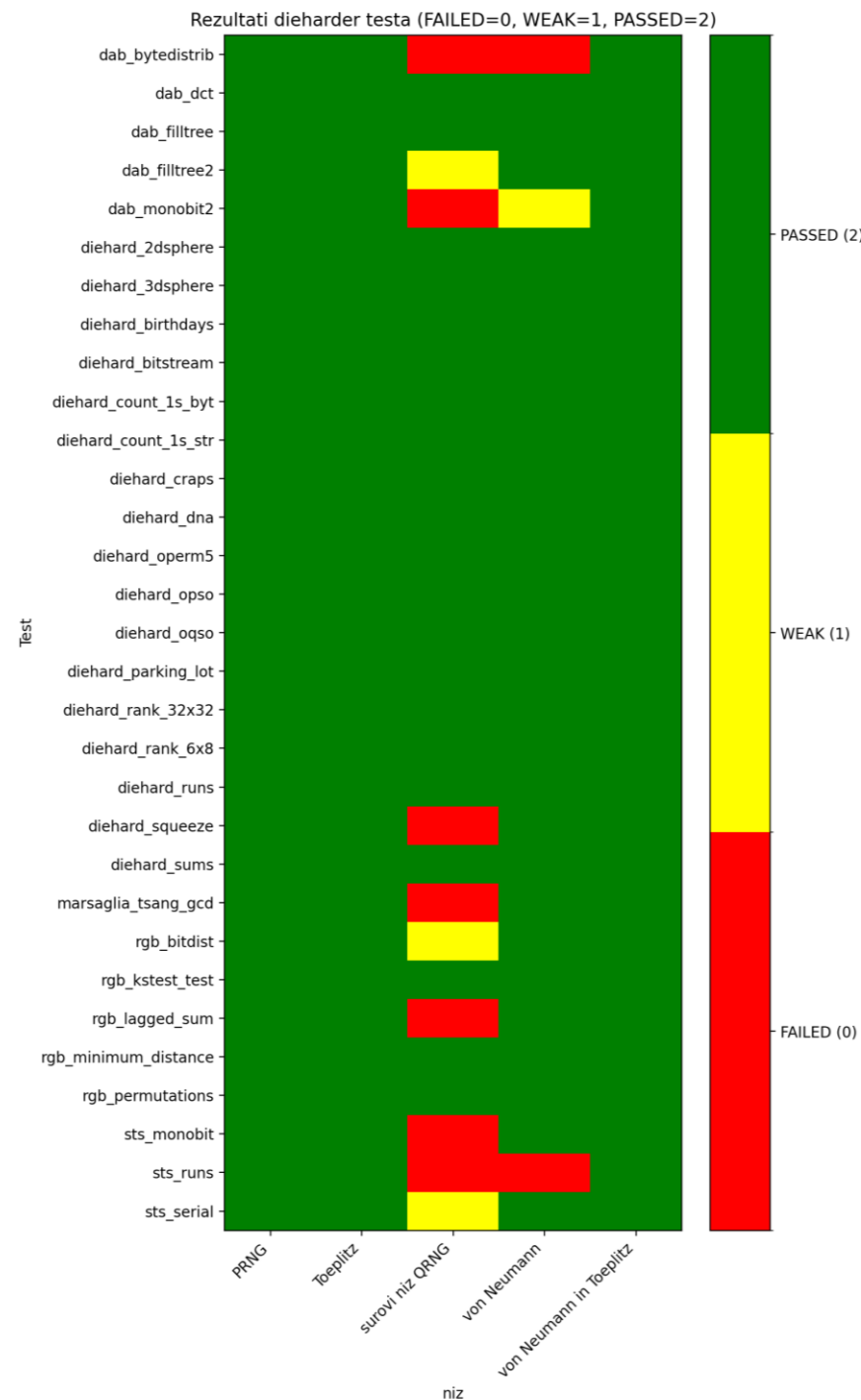
- kako nepredvidljiv je najverjetnejši izid

- NIST SP 800-90B: minimum več ocen
- estimatorji so konzervativni in pogosto podcenijo entropijo



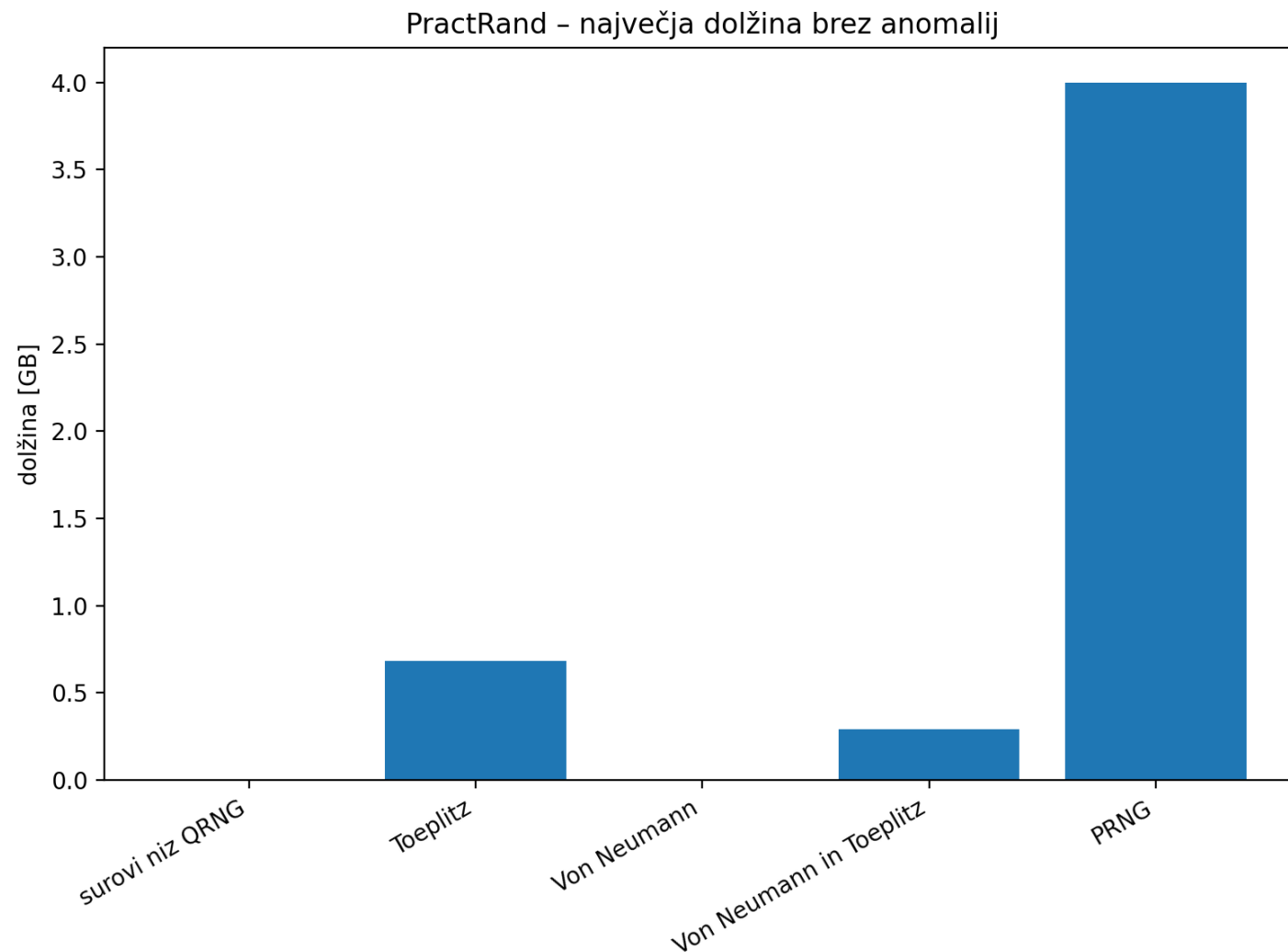
Dieharder

- Zbirka statističnih testov
- Ključni:
 - monobit test: preverja delež ničel in enic
 - runs test: analizira dolžino zaporedij istih bitov
 - itd.



PractRand

- sodobnejši nabor testov
- Preverja lastnosti zelo dolgih zaporedjih
- Uspeh na testih = odsotnost očitnih struktur



Zaključek

Rezultati raziskave:

- ocena entropije in statistični testi ne merijo istega
- obdelava podatkov je nujna
- statistični testi sami po sebi niso dokaz entropije

Za zanesljivo varnostno validacijo QRNG:

- modeliranje vira
- konzervativna ocena entropije
- statistično testiranje

Glavni prispevek:

- eksperimentalna potrditev, da statistični testi sami ne zadostujejo za dokaz resnične entropije