Priporočila za izdelavo varnih generatorjev naključnih števil

Rok Žitko
F1, Institut "Jožef Stefan"
FMF, Univerza v Ljubljani

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

Cilj: kriptografska varnost

- "kvalitetna" naključnost se približuje *idealni naključnosti*
  = neodvisnost + enakomerna porazdelitev
  = nenapovedljivost
  ("polna entropija", $H_{min}>1-2^{-32}$)
- nasprotnik nima dostopa do generiranih števil
- nasprotnik ne more vplivati na generator

ABSOLUTNA VS. RELATIVNA NENAPOVEDLJIVOST

relativna entropija = v kolikšni meri generator ustvarja števila, ki jih ne morejo napovedati dejanski ali potencialni opazovalci s svojimi omejenimi tehničnimi sposobnostmi

Tuji standardi in smernice

- ameriški NIST SP 800-90 A/B/C
- nemški BSI AIS-20/31
- ISO/IEC 18031:2011

Proces uniformizacije standardov je v teku

programski, deterministični — psevdonaključnost

PRNG = pseudo random **number** generator
DRBG = deterministic random **bit** generator

fizični, strojni, nedeterministični — prava naključnost

TRNG = true random number generator
NRBG = nondeterministic random bit generator

PRNG

- varnost temelji na kompleksnosti računov
- primerna izbira algoritma
  (lahko iz standarda, e.g. Hash_DRBG po NIST SP800A)
- pravilnost implementacije
  (known-answer test)
- seme iz TRNG, obnavljanje semena

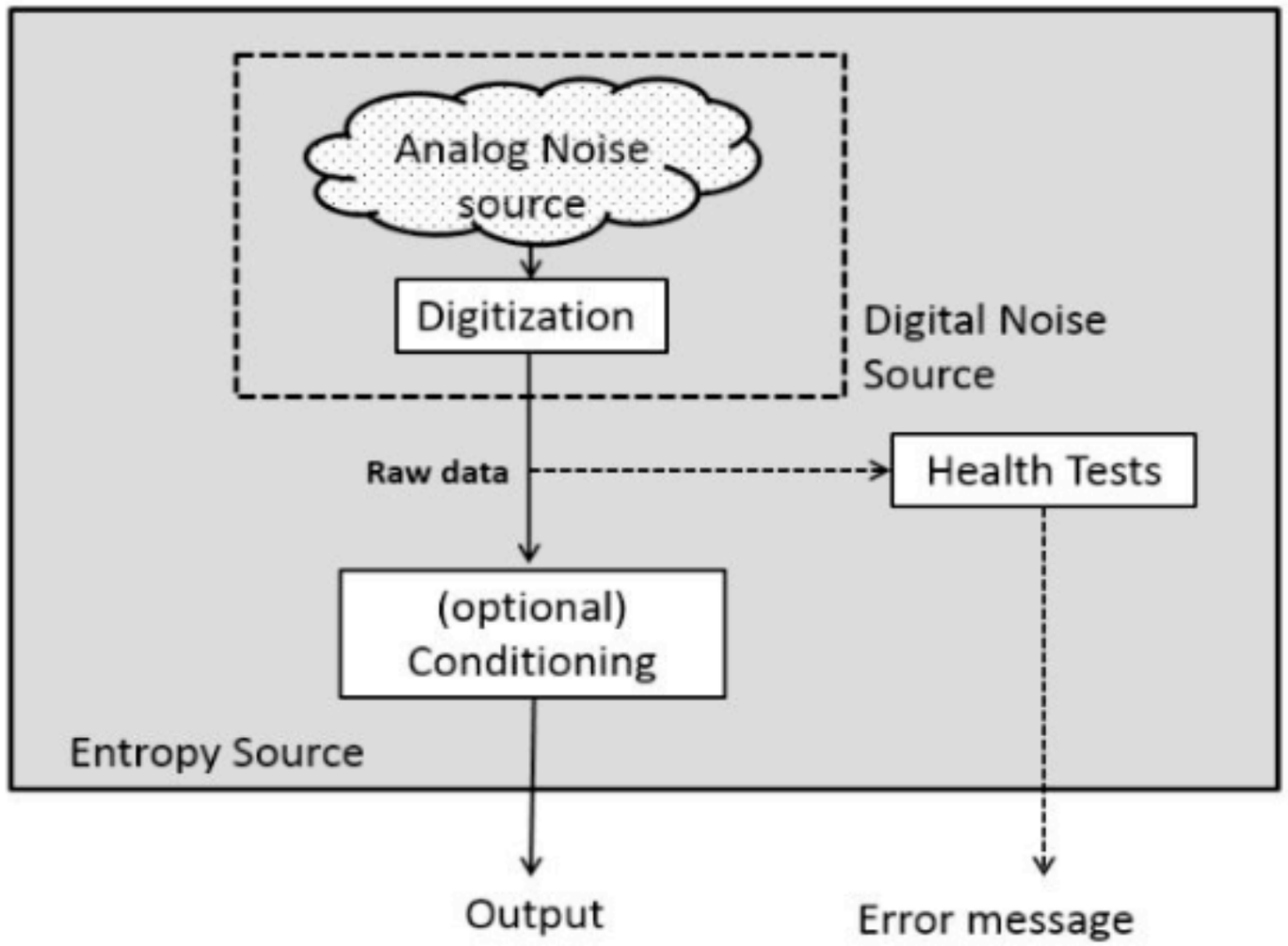
TRNG

- varnost temelji na fizikalnem procesu, ki ustvarja entropijo
- veliko možnih izvedb in tehnologij, zato standardi predpisujejo zgolj zahteve, ne pa konkretnih implementacij
- previlnost delovanja se preverja s testi (ob zagonu, sprotnimi testi, testi na zahtevo...)

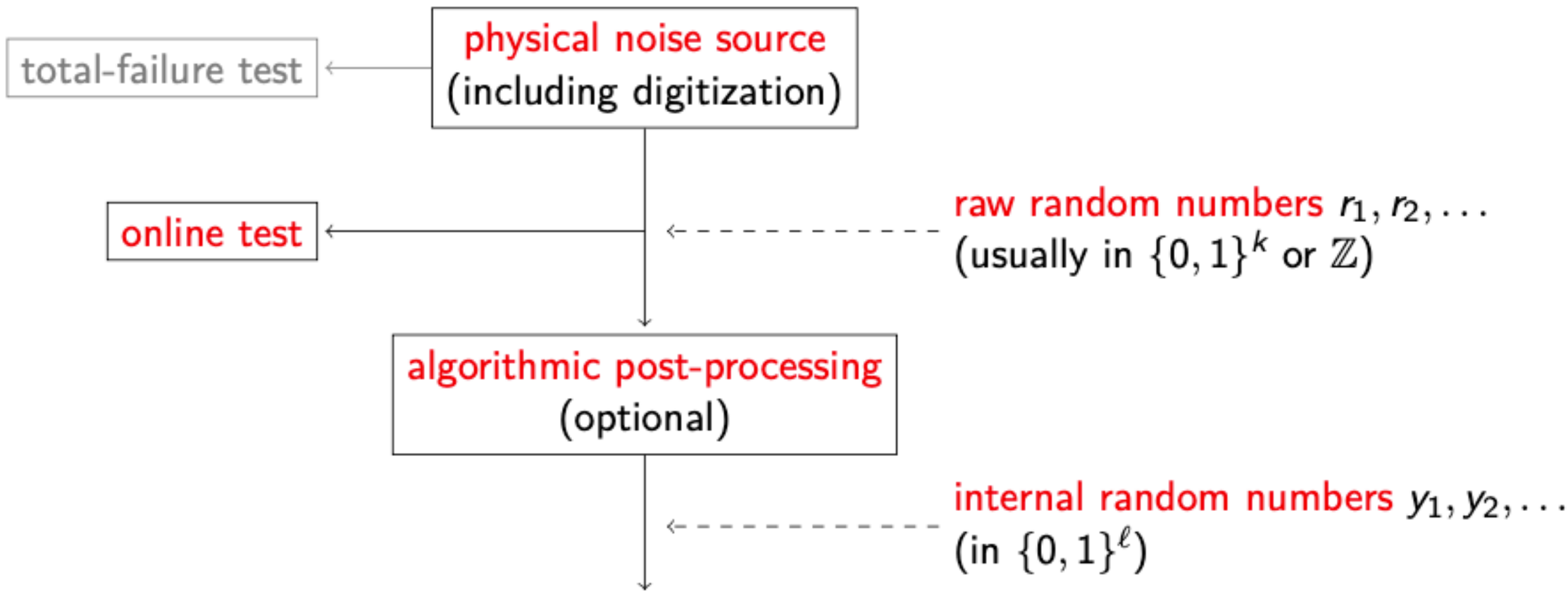
SPROTNI TESTI

2.2 The Entropy Source Model

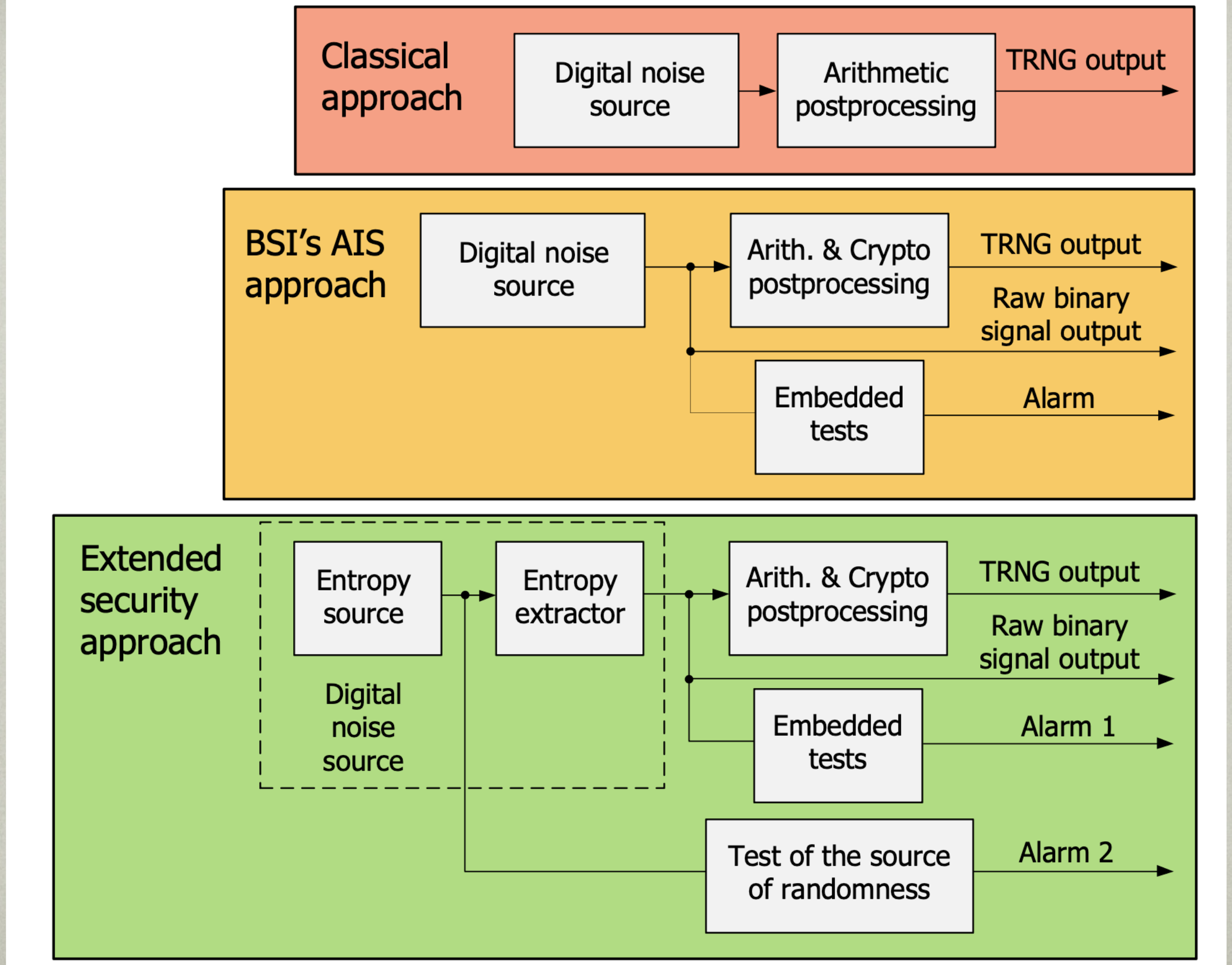
This section describes the entropy source model in detail. Figure 1 illustrates the model that this Recommendation uses to describe an entropy source and its components, which consist of a noise source, an optional conditioning component and a health testing component.



Schematic diagram of a PTG.2 generator



Vir: J. Mittmann, BSI, "Stochastic models and online tests", AIS 20/31 Workshop (2023)

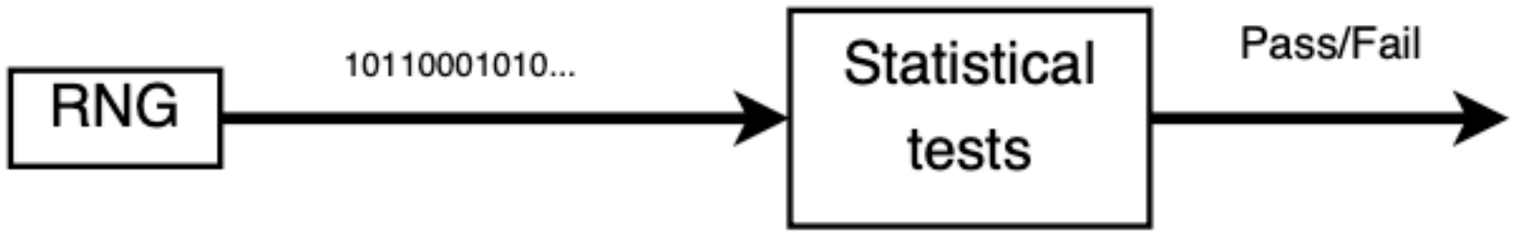


Vir slike: V. Fischer, prosojnice s predavanja

STOHASTIČNI MODEL

- podaja matematični opis izvora šuma (entropije) z naključnimi spremenljivkami
- ima obliko stohastične diferencialne enačbe ali porazdelitvene funkcije
- omogoča preveriti spodnjo mejo entropije izhodnih vrednosti
- temelji na razumevanju delovanja izvora šuma

Obsolete method:



Modern method:

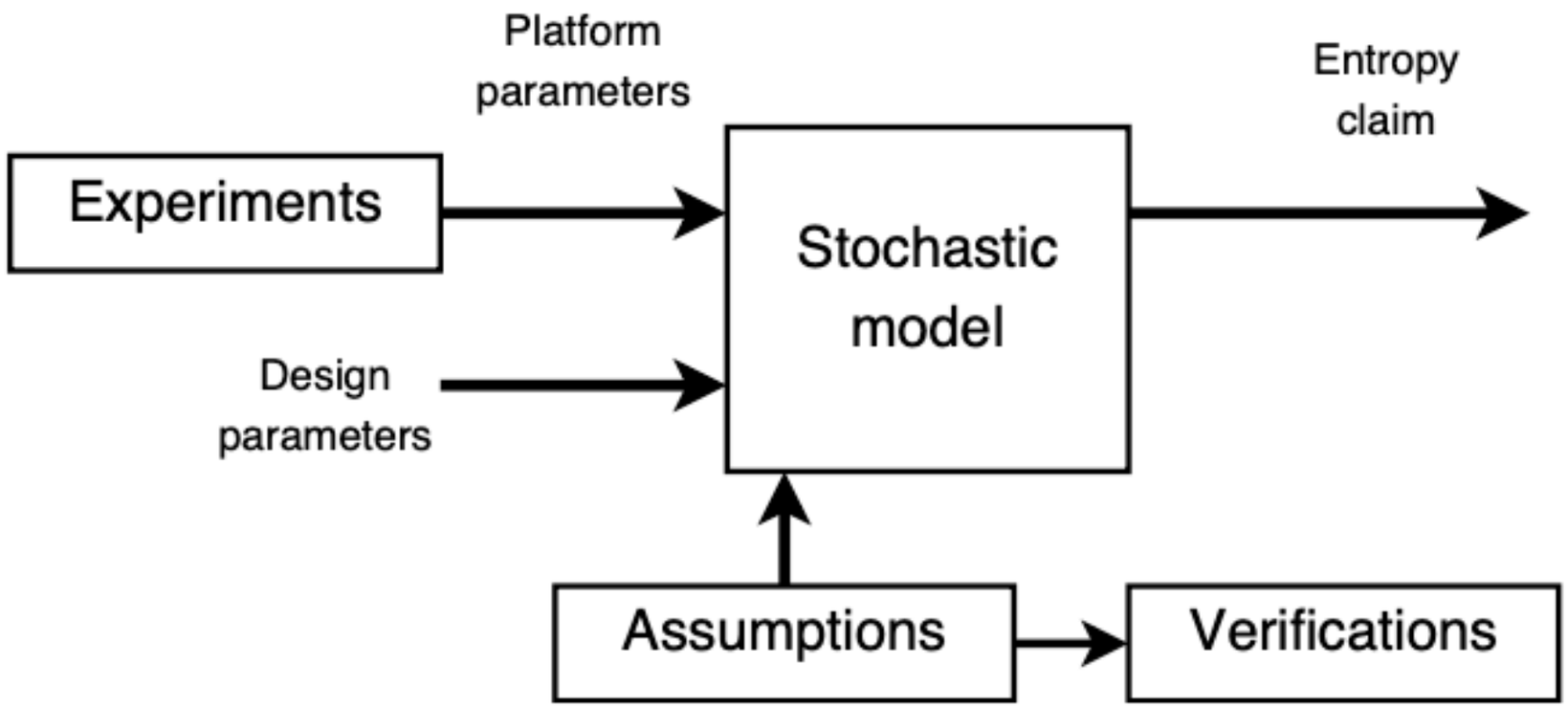


Figure 2.2: TRNG Design methods.

Vir slike: B. Yang, doktorska teza (2018)

SPLOSNA PRIPOROČILA

Previden pristop

- upoštevanje najboljših dokumentiranih in preverjenih praks
- konservativne izbire in izogibanje nepreizkušenim idejam
- uporaba standardnih in dobro poznanih tehnologij, kjer te obstajajo

Transparentnost

- vsi deli naprave so lahko podvrženi testiranju
- testni vs. običajni način delovanja

uporaba vgrajenih TRNG (v procesorjih in modulih)

- če lahko zaupamo proizvajalcu in celotni dobavni verigi
- če lahko neodvisno preverimo pravilnost implementacije

lasten TRNG

- enostavnost: vir entropije čim preprostejši z dobro razumljenimi osnovnimi lastnostmi, ki se jih lahko modelira;
  pomembno je identificirati in kvantificirati parametre, ki lahko vplivajo na vir
- majhnost: čim manj mest, kjer je možen napad na vir;
  čim krajše povezave med komponentami;
  čim manjša potreba po postprocesiranju

Sprotni testi

- čim bližje osnovnemu viru entropije
- enostavna in kompaktna implementacija
- nizka latenca (hitrost odziva)
- visoka sposobnost zaznave aktivnega napada
- nizka stopnja lažnih alarmov

Pristop "underpromise-overdeliver"

- sprotni test mora zaznati nedopustno slabo naključnost zadosti hitro
- visoka razpoložljivost (izogibanje lažnim alarmom)
- mora biti prilagojen stohastičnemu modelu

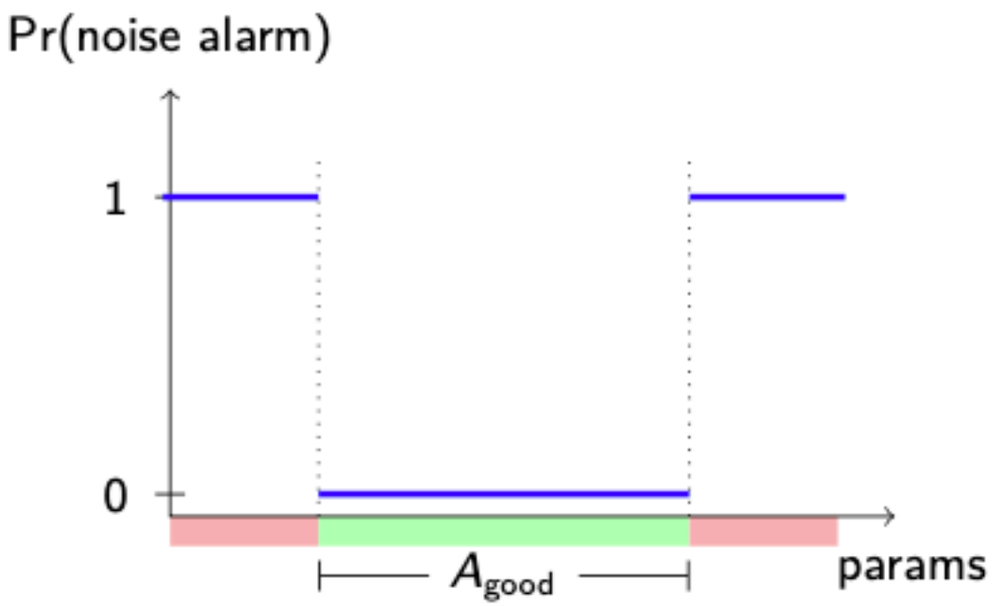


Figure: Ideal online test

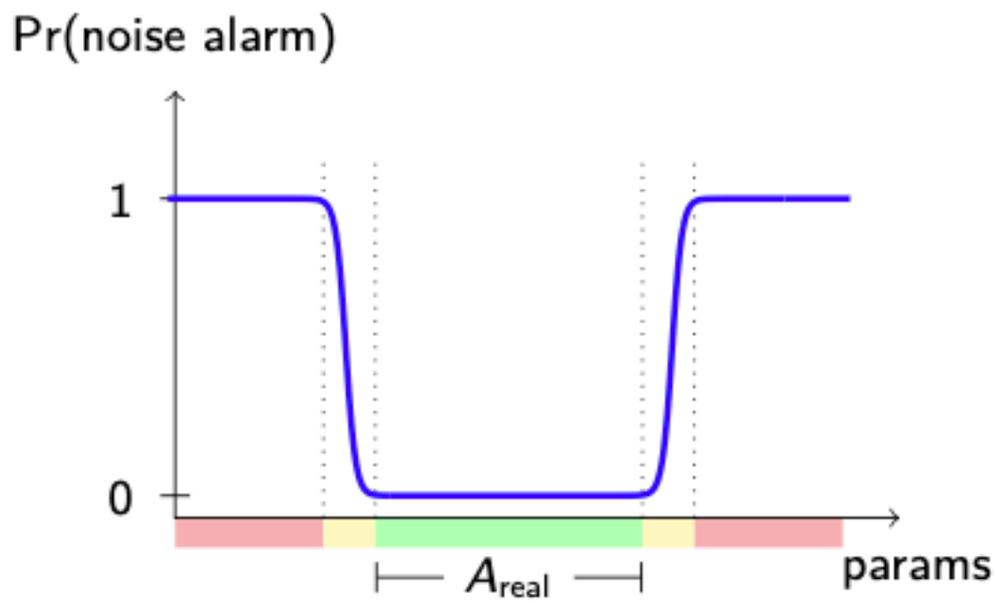


Figure: Realistic online test

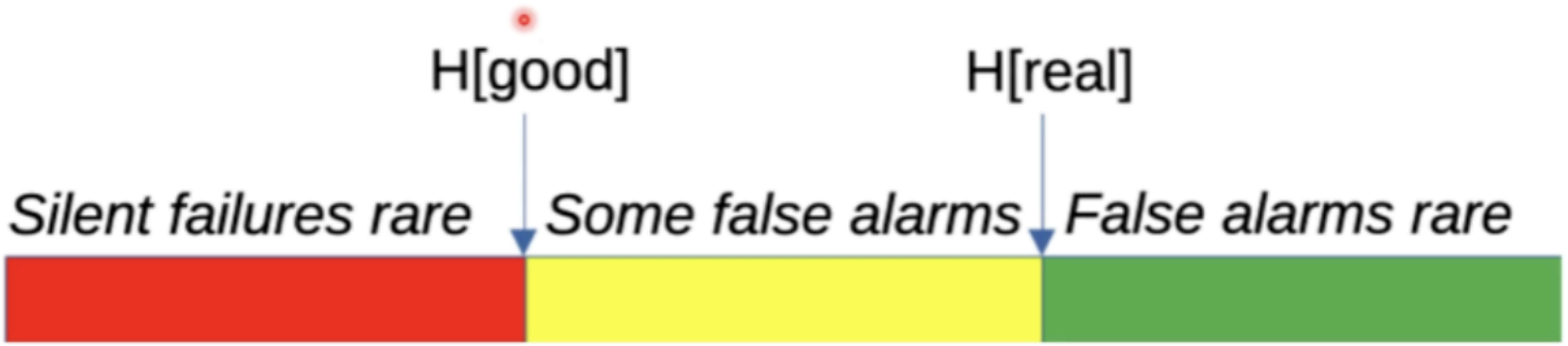
Vir: J. Mittmann, BSI, "Stochastic models and online tests", AIS 20/31 Workshop (2023)

Strategy: under promise, over deliver

- H[real] = lowest expected entropy/bit of source
- H[good] = lowest acceptable entropy/bit of source

- Design source so H[real] > H[good]

- Health tests detect error when entropy < H[good]



Vir: John Kelsey, NIST workshop 2023

KOMBINIRANI (REDUNDANTNI) VIRI ZA VISOKE STOPNJE VARNOSTI

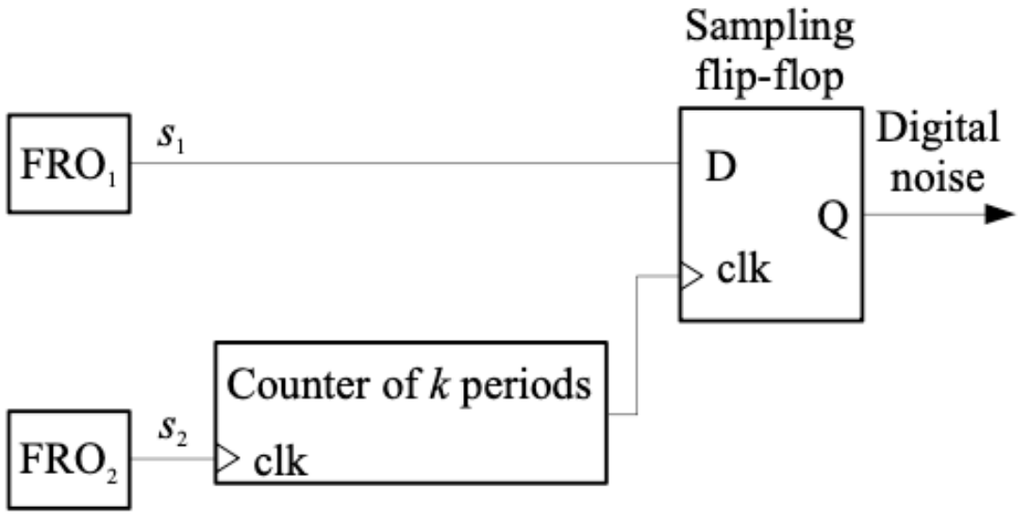
- več zelo različnih virov (e.g. oscilatorski na osnovi jitterja in optični kvantni)
- zmanjša možnost napada, saj je potrebno vplivati za zelo različne fizikalne procese
- kombiniranje z seštevanjem modulo 2 (XOR) ali z uporabo zgoščevalnih (hash) funkcij

SPECIFIČNA PRIPOROČILA ZA TRNG NA OSNOVI LOGIČNIH VEZIJ

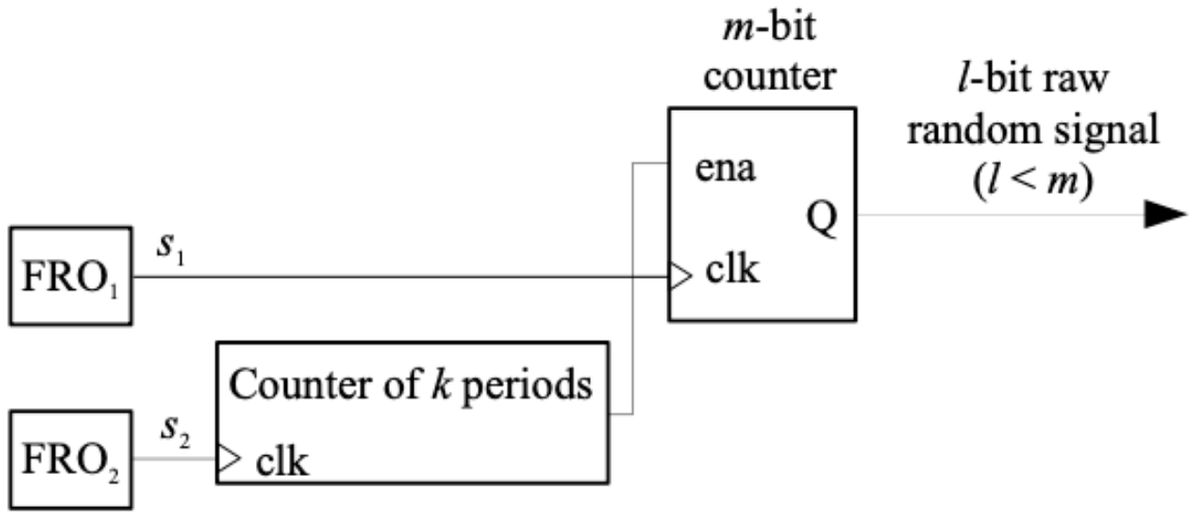
- uporaba zgolj lokalnega nedeterminističnega tresenja z uporabo diferencialne postavitve
- uporaba starejših procesnih tehnologij, ki bolj šumijo

IZVEDBE OSCILATORSKIH TRNG

način vzorčenja



način štetja



omogoča računanje
variance v realnem času!

SPECIFIČNA PRIPOROČILA ZA QRNG

- osnovna načela jasna (Bornovo pravilo o rezultatih meritev v kvantni mehaniki), zato varnost vprašanje uporabljenih komponent in njihovih karakteristik (neidealnosti) ter pravilnosti implementacije
- priporočila ITU-T X.1702, zelo sumarno napisano

Klasifikacija TRNG po BSI

- PTG.2: fizičen vir, dobro definiran, stohastičen model. Shannonova entropija večja od 0.997. Test popolne odpovedi in sprotni test.
- PTG.3: PTG.2 + kriptografsko postprocesiranje. Pravilnost implementacije postprocesiranja z known-answer testom ob zagonu in restartu.

Postprocesiranje

- algoritmično je namenjeno izboljševanju statističnih lastnosti (dvig entropije na blizu 1 bit na bit)
- kriptografsko je namenjeno zagotavljanju varnosti;
  za ohranjanje nenapovedljivosti, če vir odpove na tak način, da tega sprotni test ne zazna

SPECIFIČNA PRIPOROČILA ZA PRNG

- uporaba dobro poznanih, temeljito raziskanih in dobro dokumentiranih kriptografskih generatorjev
- uporaba algoritmov, za katere obstaja dokaz varnosti oz. vsaj odsotnost dvomov o varnosti
- semena iz TRNG ali iz nefizikalnih virov; uporaba kvalitetnih konstrukcij za zbiranje entropije (Yarrow, Fortuna)
- /dev/random v jedru Linux je OK (obstaja varnostna evalvacija od BSI, ki se redno osvežuje)
- podvojitev dolžine semen zaradi groženj kvantnih računalnikov (v obdobju 10 let, e.g. prehod z SHA2-256 na SHA2-512);
  že predvideno v posodobitvah standardov BSI AIS20/31 in NIST SP-800

SPLOŠNO

- dokumentacija vmesnika (API)
- upravljanje vsebine pomnilnika

Življenski cikel (tehnologij)

- dobavljivost komponent
- izvor in formalne zahteve po poreklu iz EU27
- nova spoznanja o stopnji varnosti
- spremembe standardov in področne zakonodaje

kriptografska agilnost: enostavno zamenjevanje kriptografskih komponent

METODOLOGIJA PREVERJANJA

- Metodologija za evalvacijo po BSI AIS 20 (za deterministične) oz. AIS 31 (za fizikalne generatorje)
- Skladnost z zahtevami
  - analiza dokumentacije
  - analiza kode oz. strojne implementacije
- Učinkovitost izvedbe
  - testiranje delovanja
  - poskusi napadov
  - spremembe okoljskih parametrov
  - statistični testi

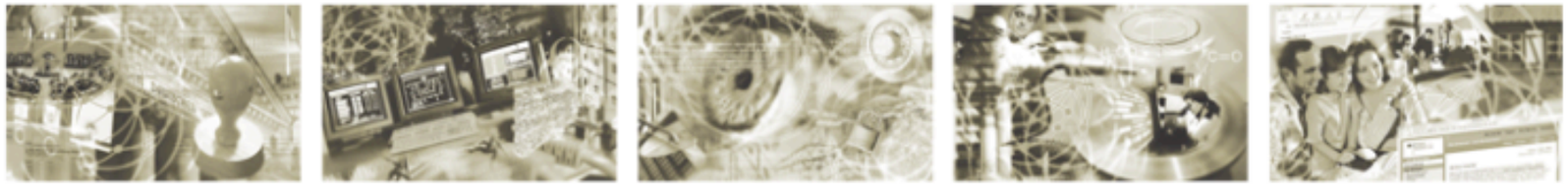
- Preverja se
  - vse elemente v verigi (vir, digitizacija, sprotni testi, postprocesiranje)
  - testi ob zagonu
  - pravilnost sporočanja alarmov in ustavitve
  - učinkovitost vseh testov
  - ustreznost in pravilnost kriptografskega postprocesrianja
  - robustnost in odpornost na poskuse manipuliranja ter prisotnost protiukrepov
  - odsotnost zadnjih vrat (back door)
  - pravilnost implementacije testnega načina

- Pri TRNG je glavni cilj preveriti, ali se vir entropije obnaša v skladu s stohastičnim modelom.

- Sekvence za testiranje mora pridobiti evalvator sam. Testirati je treba več naprav istega tipa.

- Pri FPGA: če se spremeni bitstream, se to smatra kot nova naprava, ki mora biti ponovno varnostno evalvirana.

Bundesamt
für Sicherheit in der
Informationstechnik



Evaluation of random number generators

Version 0.10

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Developer evidence for the evaluation of a physical true random number generator

Version:	**[Version]**
Date:	**[Datum]**
Evaluation Procedure:	**[BSI-DSZ-CC-xxxx]**

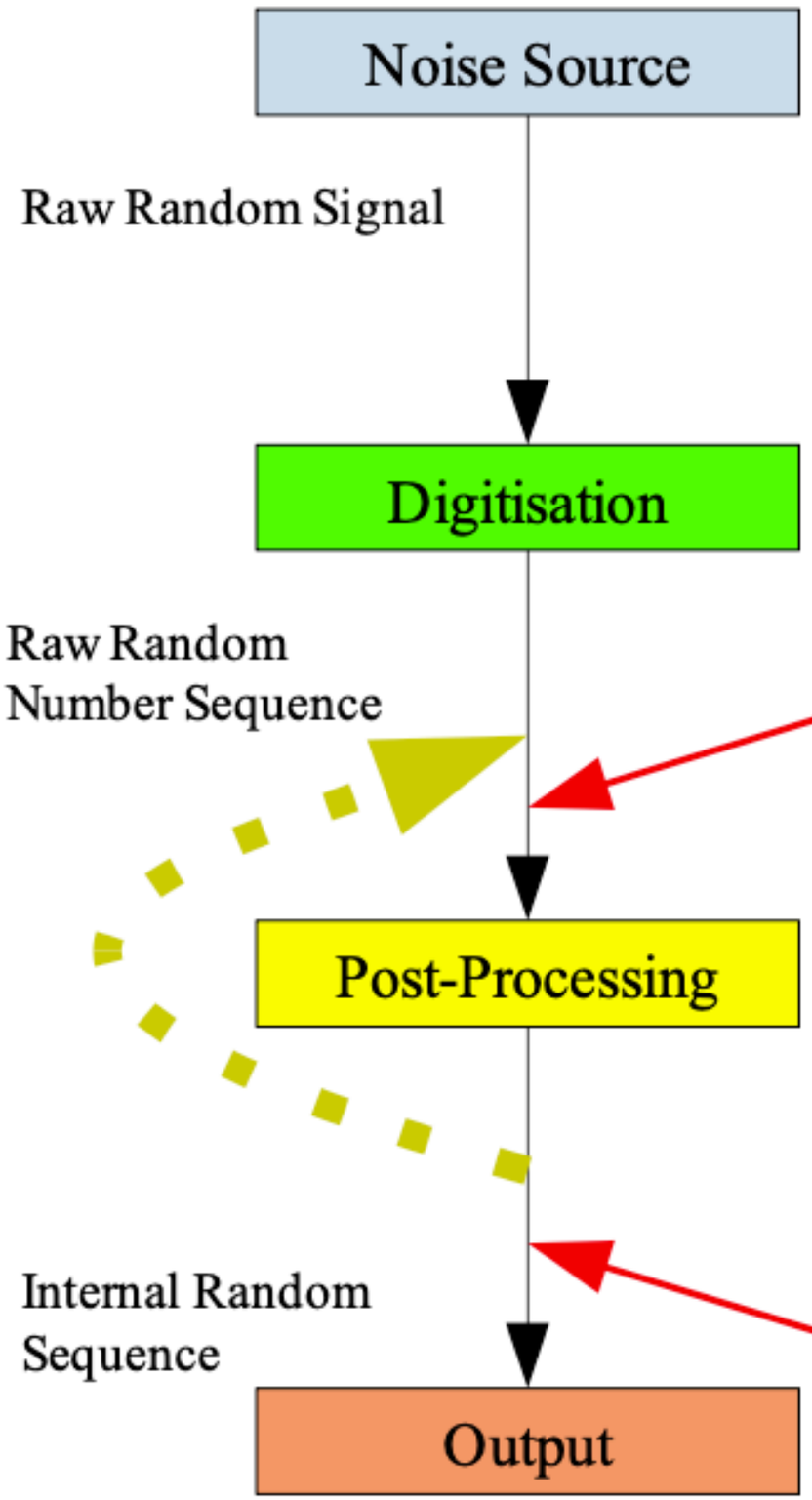
Author:	**[Name(n)]**
Quality Assurance:	**[Name(n)]**

Developer's evidence:

	Developer	Remarks
P.1	Description of the intended use of PTRNG.	• The generation of random numbers may be provided as a security service for the user or for internal use only.

P.2	Description of the PTRNG in terms of the internal entropy source that generates raw random signals.	• The description *shall* describe
		  • the power supply of the PTRNG, if relevant for the critical parts of the PTRNG, e.g. power supply might be filtered, stabilized or otherwise prepared for PTRNG use in order to ensure that power consumption by other entities does not affect the entropy source or the digitization of the analogue raw random signal,
		  • any control of the entropy source, e.g. activating or deactivating the entropy source, operational modes related to power saving.
		• Typical examples of the physical effects generating noise as an entropy source are: resistor noise, thermal noise, flicker noise, and radioactive decay. Typical examples of entropy sources are: free running oscillators varying randomly in their frequency, Zener diodes producing noise voltage, and radioactive material sending particles at random times. Each entropy source requires specific operational conditions in order to work correctly, for example, a correctly-working power supply or clock. The raw random signal and the digitization of the raw random signal might be affected by operational conditions, for example, glitches in the power supply.

P.3	Description of the PTRNG in terms of the digitization mechanism of the raw random signal into the raw random number sequence.	• The description *shall* describe the signals and any controls that are used and possibly might affect the digitization of the raw random signal, e.g., the clock used as time scale for digitization of the entropy source.



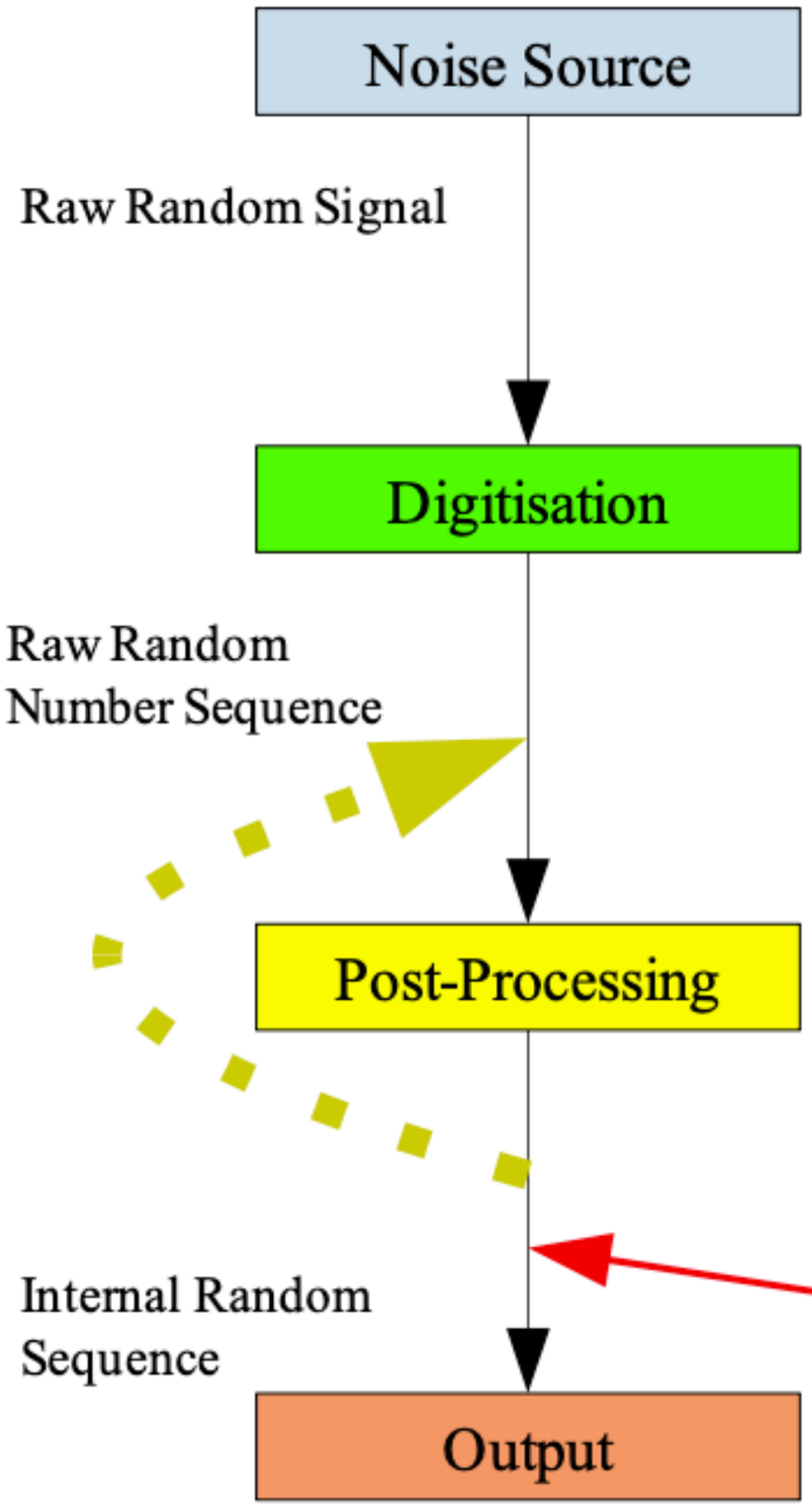
Method A

A.1 On the basis of the stochastic model, the developer shows that the raw random numbers are stationary distributed, and that there are no significant (long-step) dependencies, which are not covered by the statistical tests from test procedure B.

A.2 The raw random numbers pass the statistical test procedure B under all relevant environmental conditions

A.3 The developer verifies that the post-processing algorithm does not reduce the entropy per bit. Alternatively, the developer provides evidence that the average entropy per internal random number remains sufficiently large

A.4 The internal random numbers pass the statistical test procedure A (and other statistical standard test suites if applied) under all relevant environmental conditions.



Method B

B.1 On the basis of the stochastic model, the developer shows that the raw random numbers are stationary distributed, and that there are no significant (long-step) dependencies that are not covered by the statistical tests from test procedure B.

B.2 The developer verifies on the basis of the stochastic model that due to the post-processing algorithm the entropy per internal random number is sufficiently large. Under suitable conditions test procedure B might support this goal.

B.3 The internal random numbers pass the statistical test procedures A (and other statistical standard test suites if applied) and test procedures B under all relevant environmental conditions.

Statistični testi

- SP800-22 STS (statistical test suite): zastarelo, NIST pripravlja reimplementacijo
- dieharder: širok nabor, testi drugega reda (preverja uniformnost porazdelitve p-vrednosti ponovljenih izvedb istega testa)
- TestU01: nima težav z lažnimi pozitivnimi izzidi
- PractRand: novi testi (večja pokritost), testiranje zelo dolgih sekvenc

Priporočilo: TestU01 in PractRand

KLJUČNE MISLI

- generatorji z visoko entropičnimi vir, za katere obstajajo stohastični modeli
- sprotno preverjanje entropije vira
- enostavnost, transparentnost, možnost neodvisnega preverjanja
- evalvacija po metodi BSI AIS 20/31