# SP 800-22 and GM/T 0005-2012

## Clearly Obsolete, Possibly Harmful

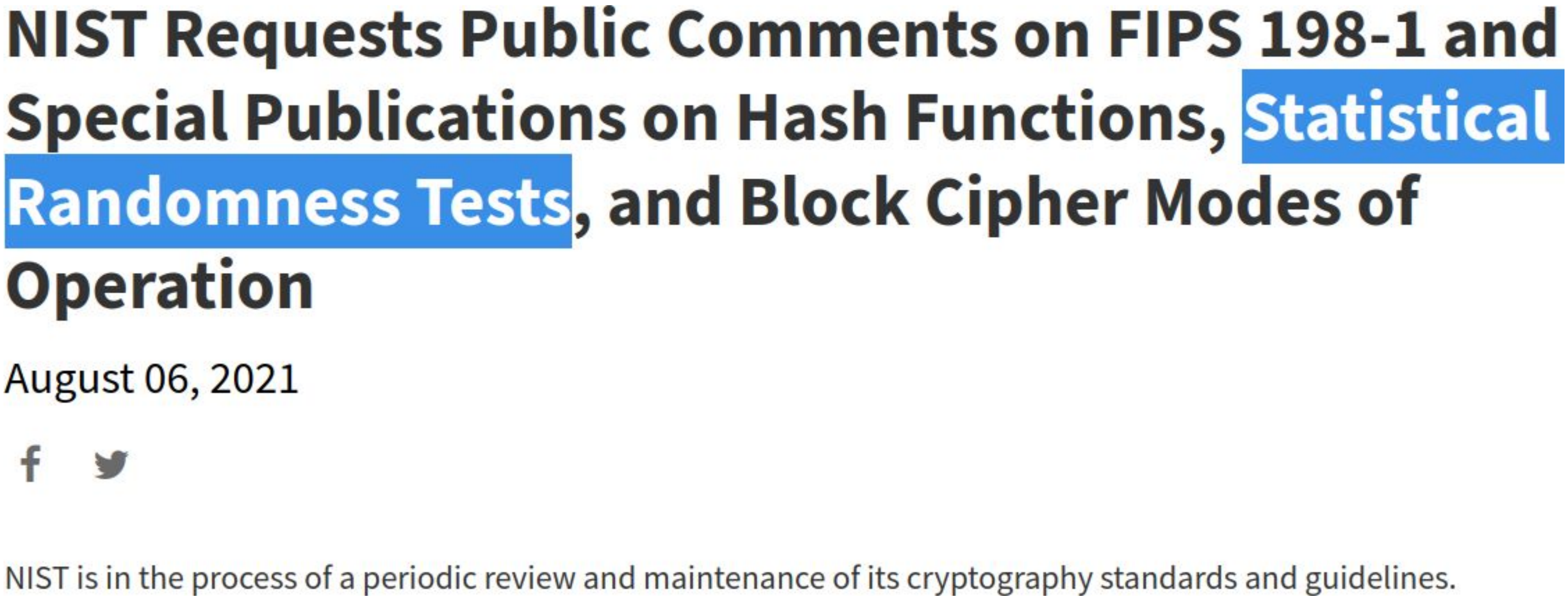
Think openly, build securely

*7th Security Standards Research (SSR)*
*June 6, 2022 – Genoa, Italy.*

**Dr. Markku-Juhani O. Saarinen**
Senior Cryptography Architect, PQShield Ltd.

# a.k.a. Periodic review is a good thing

## Last summer..



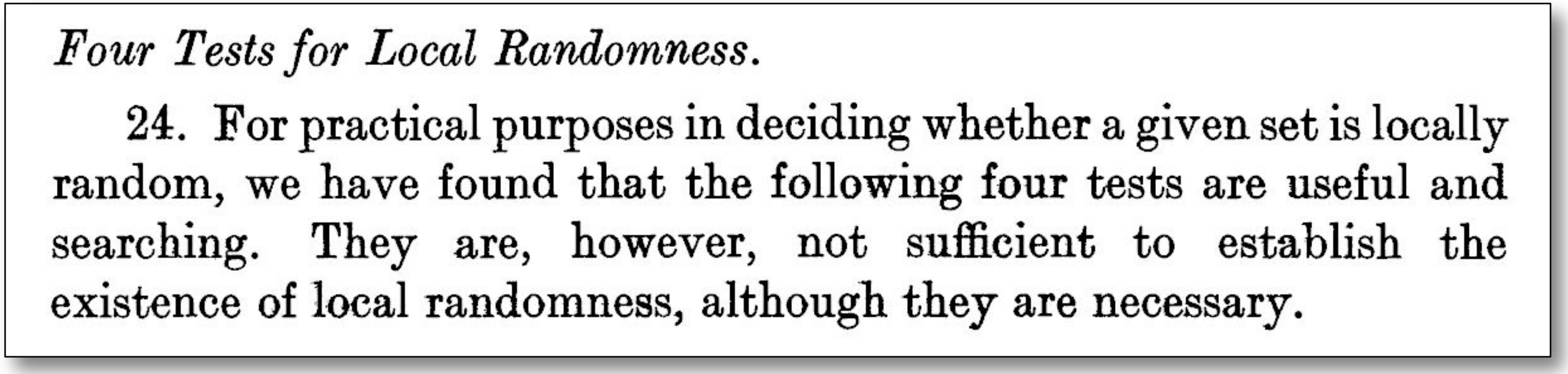
NIST Requests Public Comments on FIPS 198-1 and Special Publications on Hash Functions, Statistical Randomness Tests, and Block Cipher Modes of Operation

August 06, 2021

NIST is in the process of a periodic review and maintenance of its cryptography standards and guidelines.

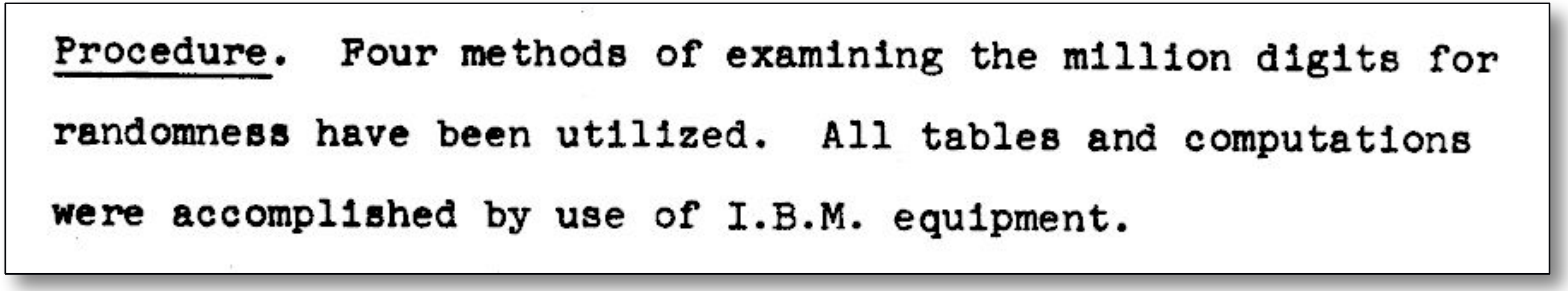
# Randomness Before Information Theory

## Computation was manual (1938), punch card (1948)

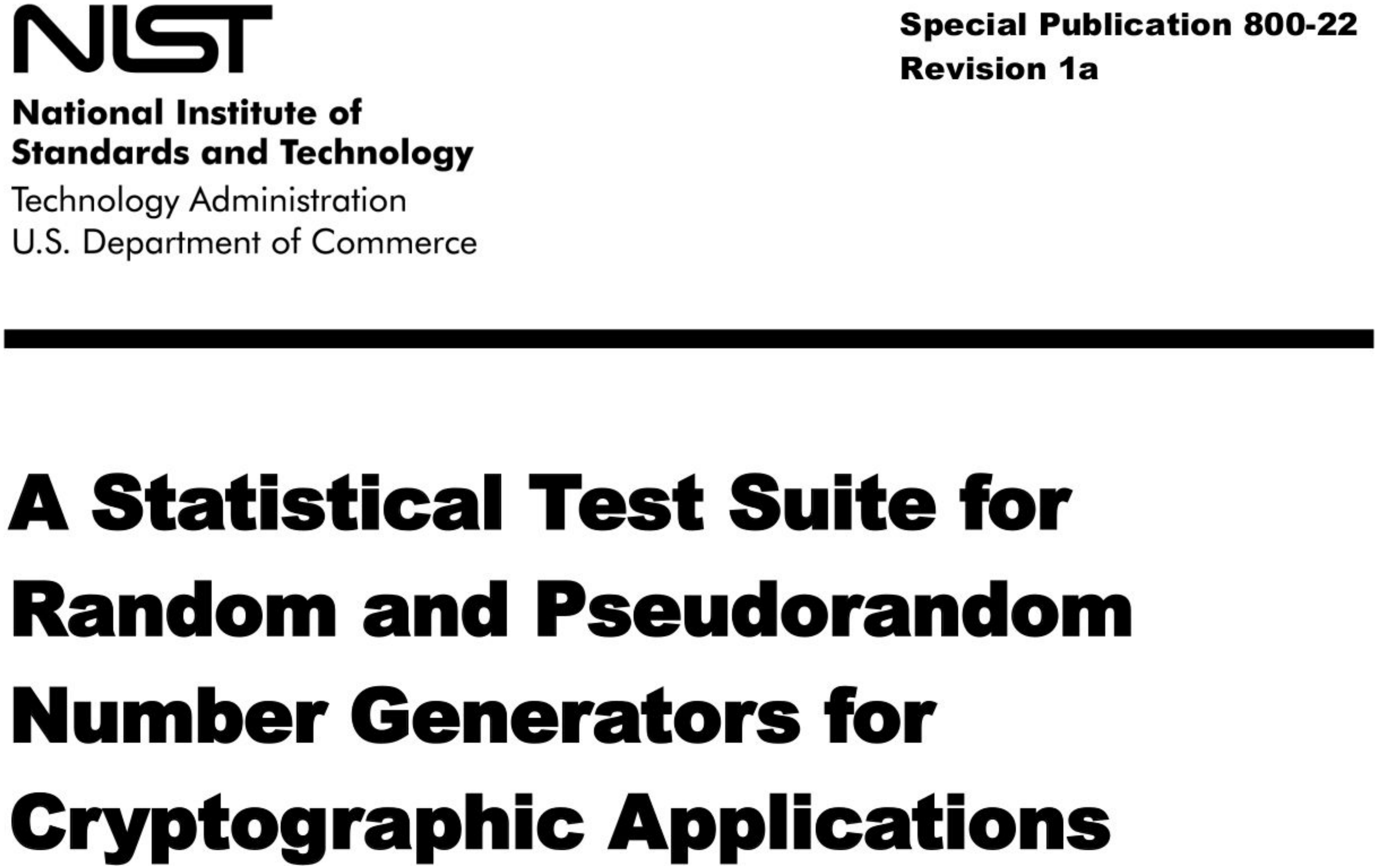


*Four Tests for Local Randomness.*

24. For practical purposes in deciding whether a given set is locally random, we have found that the following four tests are useful and searching. They are, however, not sufficient to establish the existence of local randomness, although they are necessary.



Procedure. Four methods of examining the million digits for randomness have been utilized. All tables and computations were accomplished by use of I.B.M. equipment.

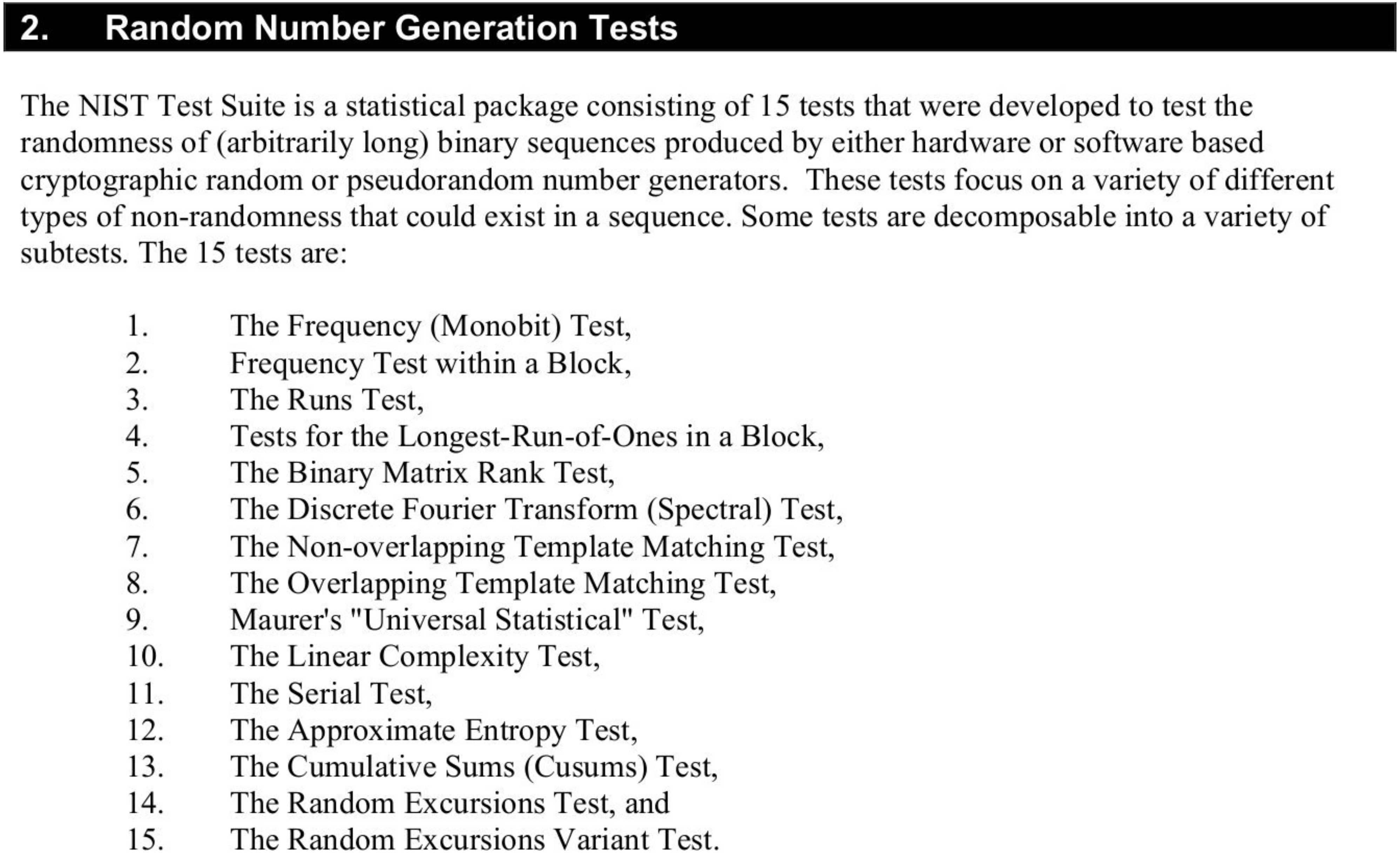


NIST

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-22
Revision 1a

# A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications



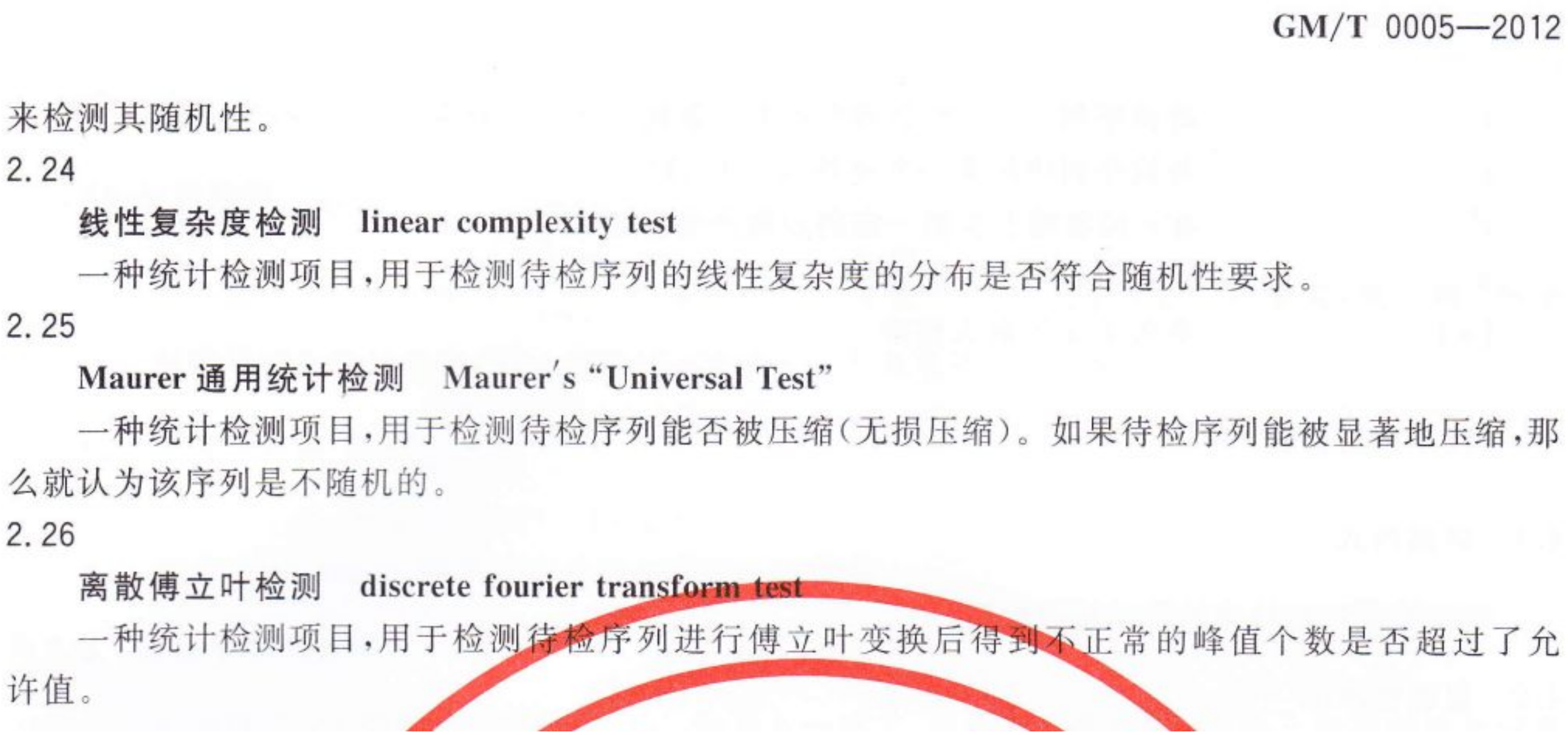
## 2. Random Number Generation Tests

The NIST Test Suite is a statistical package consisting of 15 tests that were developed to test the randomness of (arbitrarily long) binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. The 15 tests are:

1. The Frequency (Monobit) Test,
2. Frequency Test within a Block,
3. The Runs Test,
4. Tests for the Longest-Run-of-Ones in a Block,
5. The Binary Matrix Rank Test,
6. The Discrete Fourier Transform (Spectral) Test,
7. The Non-overlapping Template Matching Test,
8. The Overlapping Template Matching Test,
9. Maurer's "Universal Statistical" Test,
10. The Linear Complexity Test,
11. The Serial Test,
12. The Approximate Entropy Test,
13. The Cumulative Sums (Cusums) Test,
14. The Random Excursions Test, and
15. The Random Excursions Variant Test.

# GM/T 0005-2012 “Randomness Test”

## Chinese Standard: Many similar tests to SP 800-22



GM/T 0005—2012

来检测其随机性。

2.24

**线性复杂度检测　linear complexity test**

一种统计检测项目,用于检测待检序列的线性复杂度的分布是否符合随机性要求。

2.25

**Maurer通用统计检测　Maurer′s “Universal Test”**

一种统计检测项目,用于检测待检序列能否被压缩(无损压缩)。如果待检序列能被显著地压缩,那么就认为该序列是不随机的。

2.26

**离散傅立叶检测　discrete fourier transform test**

一种统计检测项目,用于检测待检序列进行傅立叶变换后得到不正常的峰值个数是否超过了允许值。

# SP 800-22

## Systemic Problem: Statistics != Security

- **Random and pseudorandom generators.** No distinction is made between, say, hash function output and a ring oscillator.

- From cryptographers viewpoint these randomness tests can be characterized as **low-complexity black-box distinguishers**.

- **Has no role in security certification** (except indirectly in China)
  - **FIPS 140-3** requires SP 800-90B entropy sources and SP 800-90A DRBGs.
  - **Common Criteria** protection profiles often use BSI AIS-20/AIS-31.

# SP 800-22: Cryptanalysis in a Box?

## Systemic Problem: Statistics != Security

- In such “black-box” statistical testing for randomness, the **process** and **security** of random number generation is ignored.

- In actual random number generator evaluation**:**
  - **Entropy sources**: Entropy analysis, physical, and stochastic models.
  - **Pseudorandom generators**: Evaluation is a *cryptanalytic* task. Computational distinguishability is assessed (e.g. $2^{128}$ or $2^{256}$ effort).
  - **Correctness** of generators: test vectors, formal models, physical tests.

- Pure statistical testing is perhaps useful for non-cryptographic random generators. (But SP 800-22 says it is explicitly for crypto.)

# + All the bad “Reference Generators”

- Appendix D of SP 800-22 describes nine “**reference generators**”.

- In the paper I discuss how basically none of these are secure. Many do not even try to separate internal state from output.

- Even the 32-bit Linear Congruential Generator passes the tests.

- Why did the document describe such a *completely flawed* evaluation process? Was this a prelude to **Dual_EC_DRBG** ?

*… wait, it’s still a valid doc. Who uses it?*

# Lava Lamp Security Inc

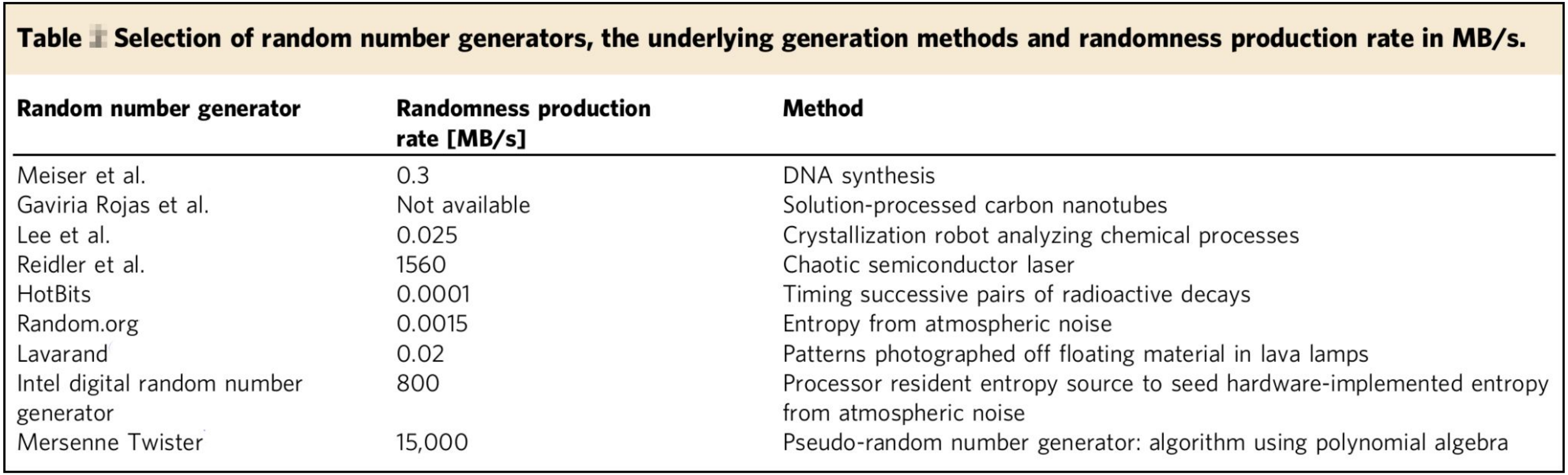


**Table [redacted] Selection of random number generators, the underlying generation methods and randomness production rate in MB/s.**

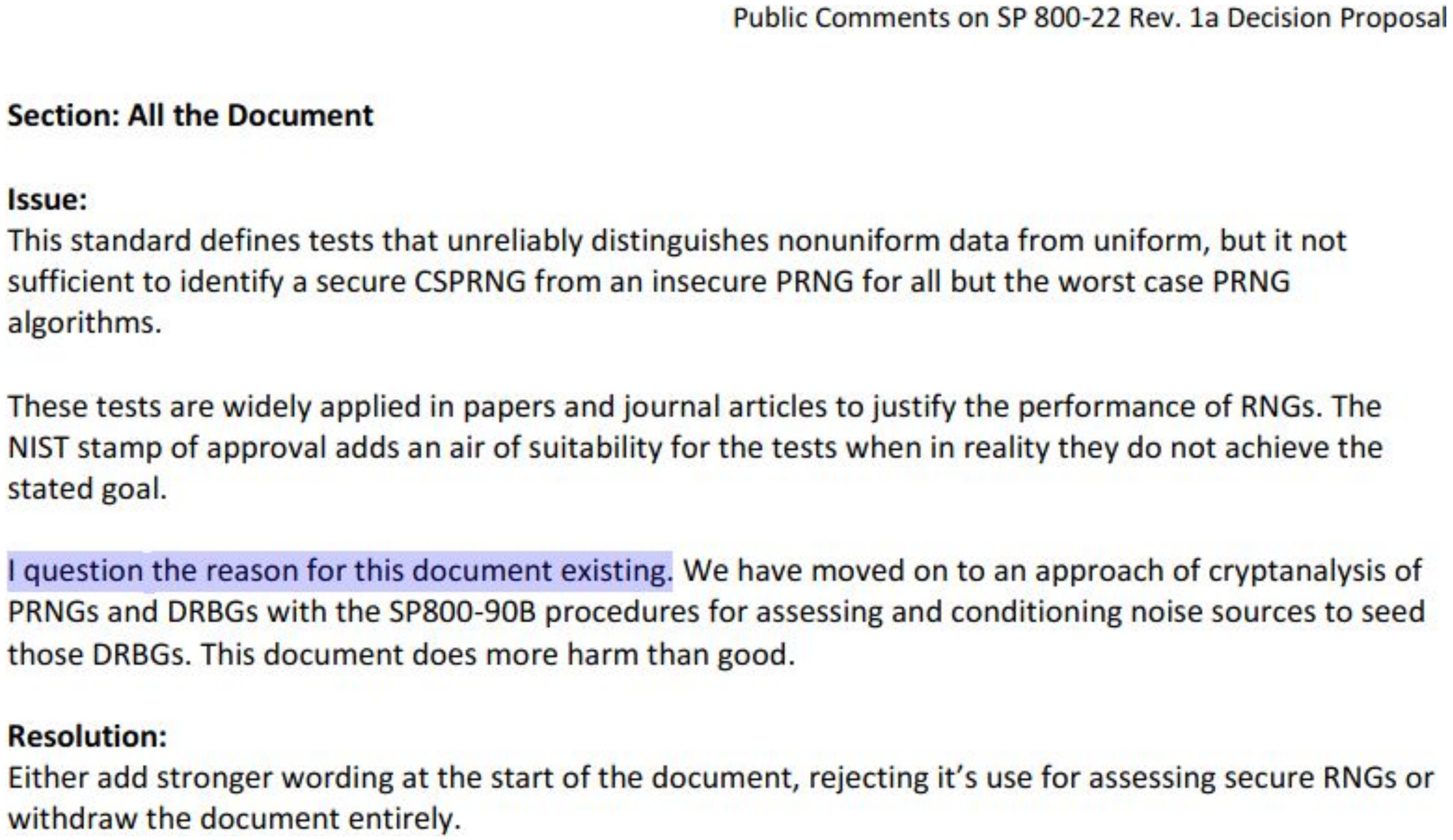
| Random number generator | Randomness production rate [MB/s] | Method |
|---|---|---|
| Meiser et al. | 0.3 | DNA synthesis |
| Gaviria Rojas et al. | Not available | Solution-processed carbon nanotubes |
| Lee et al. | 0.025 | Crystallization robot analyzing chemical processes |
| Reidler et al. | 1560 | Chaotic semiconductor laser |
| HotBits | 0.0001 | Timing successive pairs of radioactive decays |
| Random.org | 0.0015 | Entropy from atmospheric noise |
| Lavarand | 0.02 | Patterns photographed off floating material in lava lamps |
| Intel digital random number generator | 800 | Processor resident entropy source to seed hardware-implemented entropy from atmospheric noise |
| Mersenne Twister | 15,000 | Pseudo-random number generator: algorithm using polynomial algebra |

- Colorful "parallel universe" from non-cryptographer inventors.
- Rarely any security evaluation, just statistical testing.

*( Intel above is of course an exception. )*

# Official comments: David Johnston, Intel

## “I question the reason for this document existing.”



Public Comments on SP 800-22 Rev. 1a Decision Proposal

**Section: All the Document**

**Issue:**
This standard defines tests that unreliably distinguishes nonuniform data from uniform, but it not sufficient to identify a secure CSPRNG from an insecure PRNG for all but the worst case PRNG algorithms.

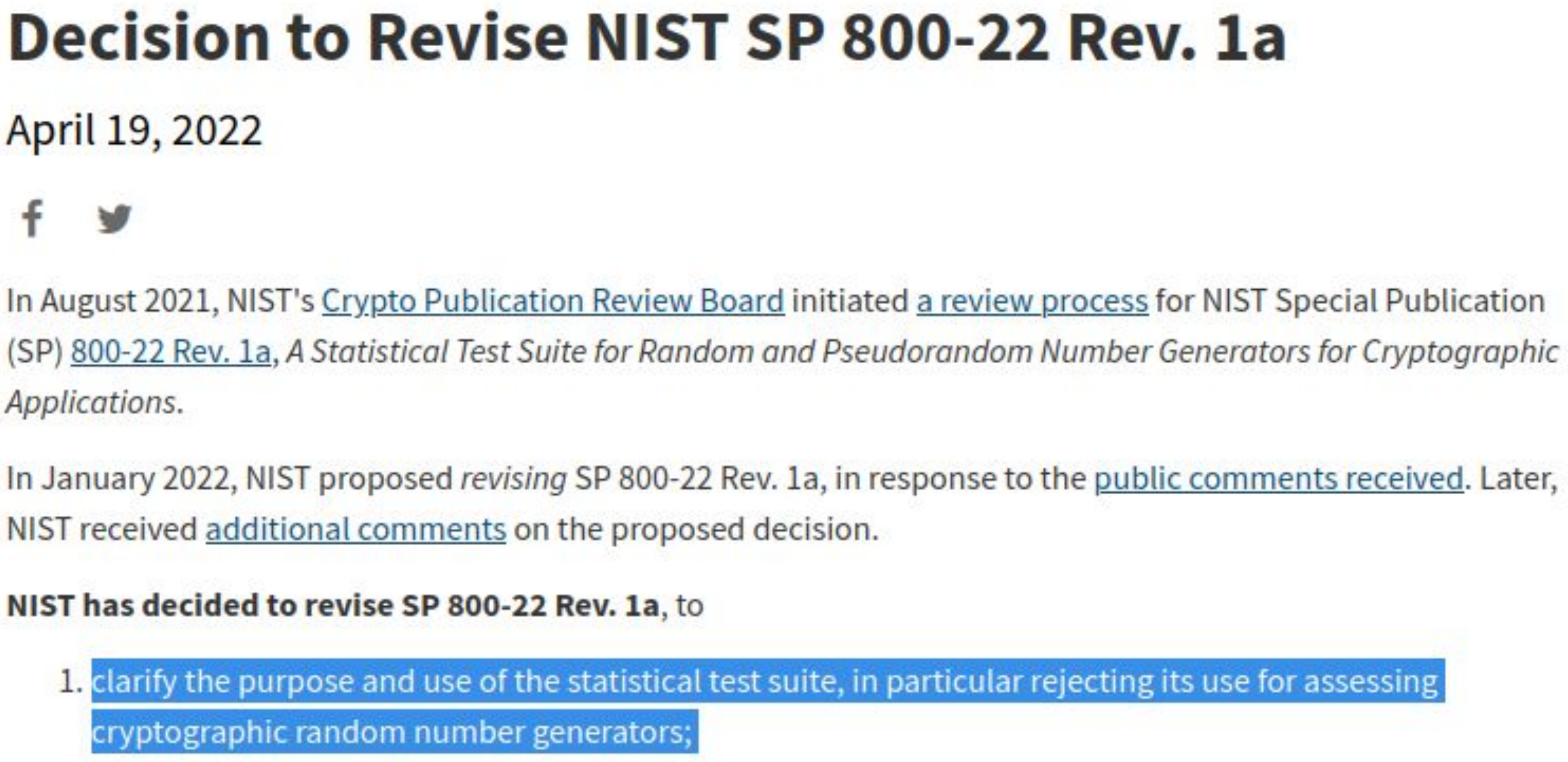
These tests are widely applied in papers and journal articles to justify the performance of RNGs. The NIST stamp of approval adds an air of suitability for the tests when in reality they do not achieve the stated goal.

I question the reason for this document existing. We have moved on to an approach of cryptanalysis of PRNGs and DRBGs with the SP800-90B procedures for assessing and conditioning noise sources to seed those DRBGs. This document does more harm than good.

**Resolution:**
Either add stronger wording at the start of the document, rejecting it’s use for assessing secure RNGs or withdraw the document entirely.

# Victory! Status: “Don’t use for crypto.”

## This SSR 22 paper was also a NIST public comment.



### Decision to Revise NIST SP 800-22 Rev. 1a

April 19, 2022

In August 2021, NIST's Crypto Publication Review Board initiated a review process for NIST Special Publication (SP) 800-22 Rev. 1a, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*.

In January 2022, NIST proposed *revising* SP 800-22 Rev. 1a, in response to the public comments received. Later, NIST received additional comments on the proposed decision.

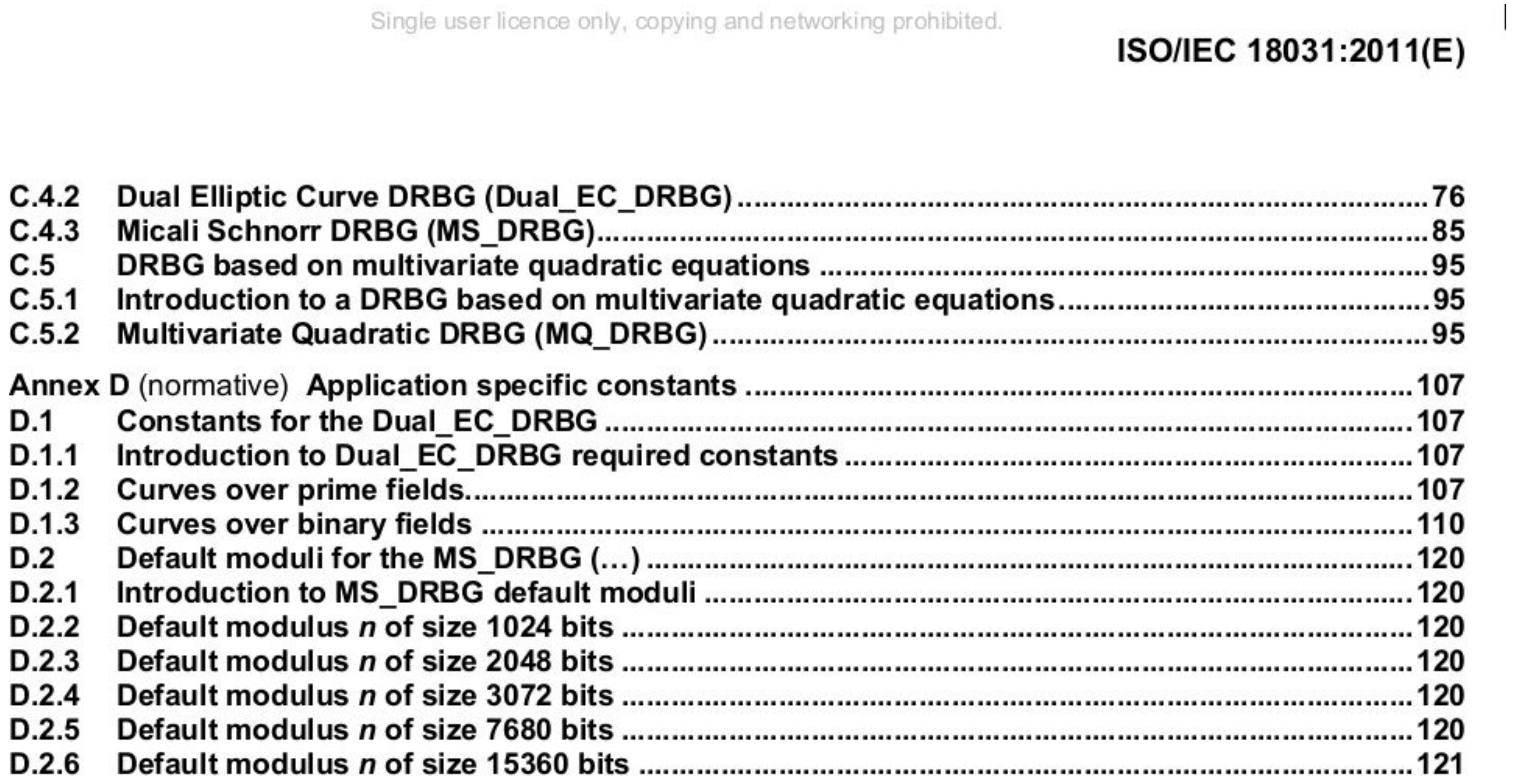
**NIST has decided to revise SP 800-22 Rev. 1a**, to

1. clarify the purpose and use of the statistical test suite, in particular rejecting its use for assessing cryptographic random number generators;

https://csrc.nist.gov/news/2022/decision-to-revise-nist-sp-800-22-rev-1a

# Postscript: ISO 18031 & RBG Backdoors

## Still valid: “Reviewed and confirmed in 2017”

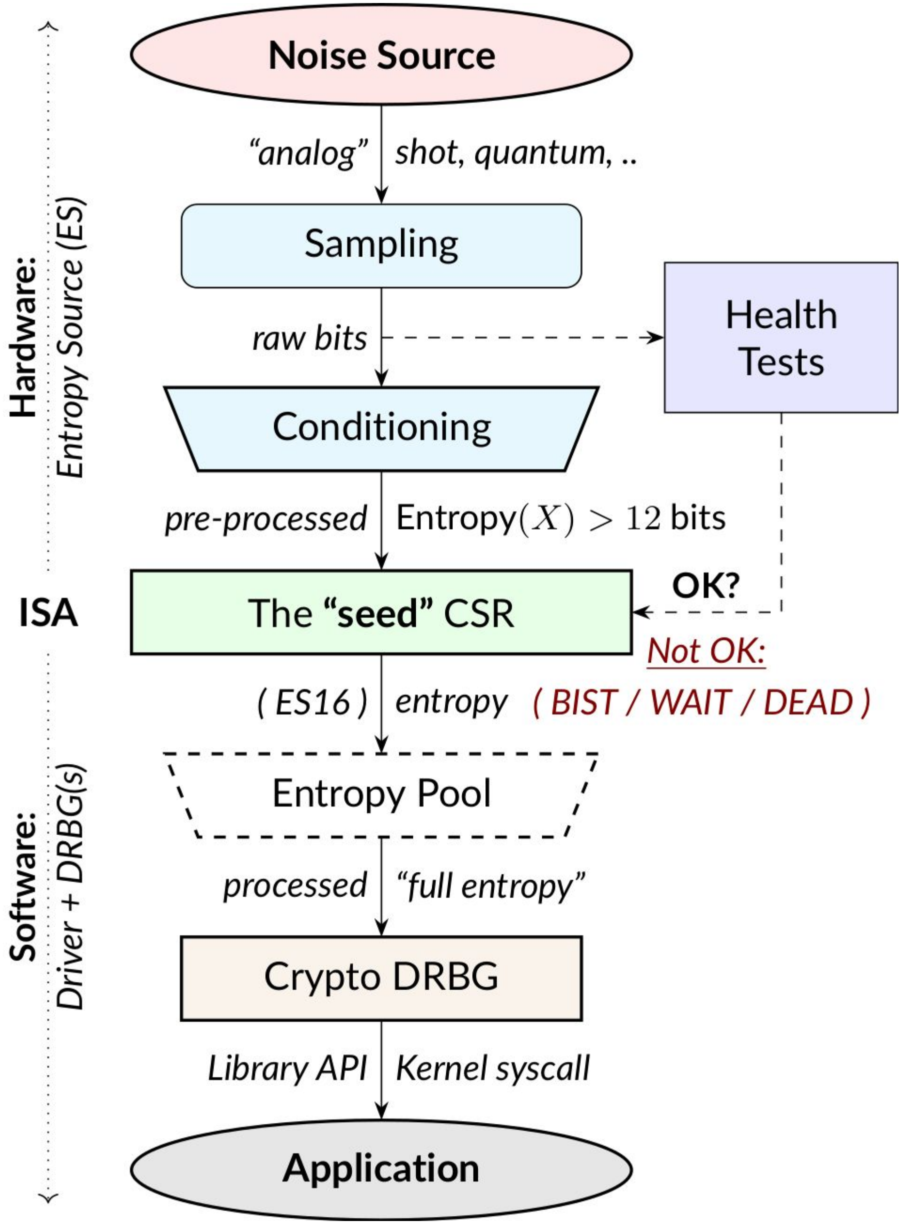


# Extra Slides on Actual RNG Evaluation.

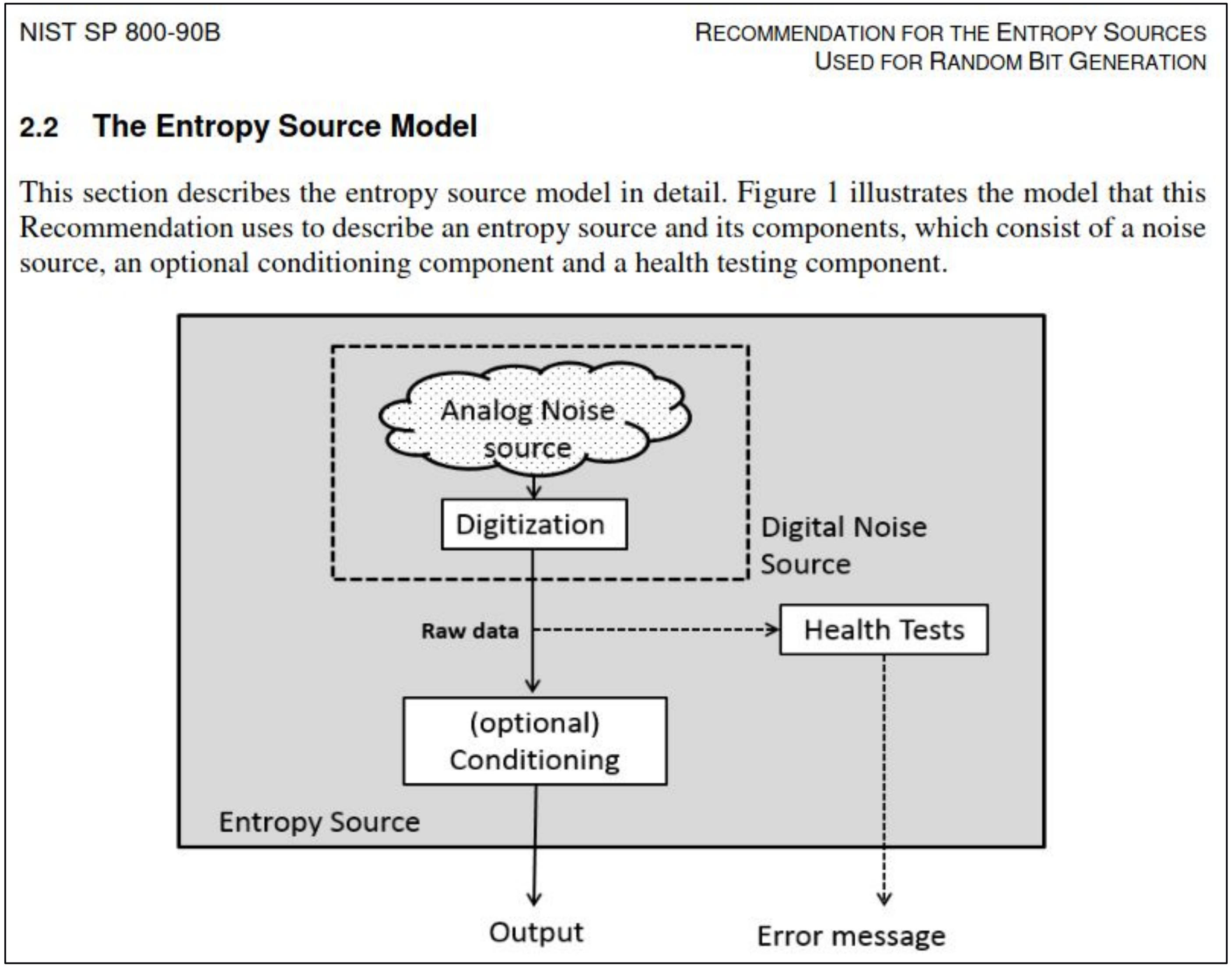
# How do HW RNGs work?

## SP 800-90A/90B/90C

- **Noise Source** is based on explainable (usually physical) phenomena.
- **Health tests** monitor noise quality and detect faults, even attacks.
- **Conditioning** with a cryptographic hash condenses entropy to keymat.
- **DRBG** uses secure cryptography (be.g. AES-256) to generate output.



# What is a “90B” Entropy Source? (USA)



NIST SP 800-90B

RECOMMENDATION FOR THE ENTROPY SOURCES
USED FOR RANDOM BIT GENERATION

### 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.

Entropy Source contains a well-understood **Noise Source**.

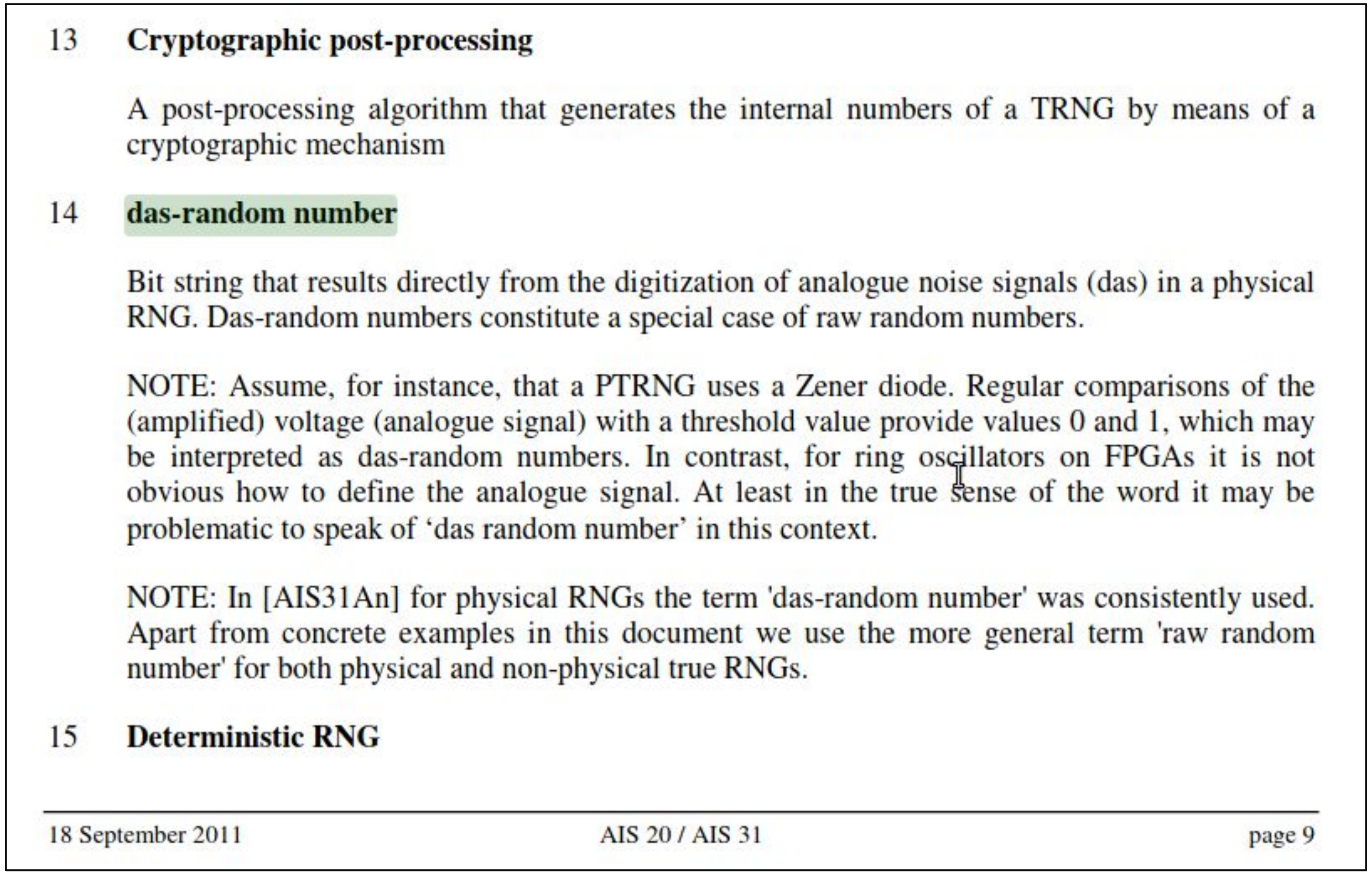
**Health tests** are a **mandatory** part of an entropy source.

**Conditioning** is optional but can be inside the box.

Output distribution has *known lower bound on entropy rate.*

# AIS 20 / AIS 31 (German BSI, CC)

## Little bit different from SP 800-90 A/B/C



13 **Cryptographic post-processing**

A post-processing algorithm that generates the internal numbers of a TRNG by means of a cryptographic mechanism

14 **das-random number**

Bit string that results directly from the digitization of analogue noise signals (das) in a physical RNG. Das-random numbers constitute a special case of raw random numbers.

NOTE: Assume, for instance, that a PTRNG uses a Zener diode. Regular comparisons of the (amplified) voltage (analogue signal) with a threshold value provide values 0 and 1, which may be interpreted as das-random numbers. In contrast, for ring oscillators on FPGAs it is not obvious how to define the analogue signal. At least in the true sense of the word it may be problematic to speak of ‘das random number’ in this context.

NOTE: In [AIS31An] for physical RNGs the term 'das-random number' was consistently used. Apart from concrete examples in this document we use the more general term 'raw random number' for both physical and non-physical true RNGs.

15 **Deterministic RNG**

18 September 2011 AIS 20 / AIS 31 page 9

AIS 31 is used in intl. Common Criteria certifications; was clearly better than FIPS evaluation until FIPS 140-3 & SP 800-90B (2018).

**AIS 31** says **Post-processing** when FIPS/90B says **Conditioning.**

**Das-random** or **raw random** are used for noise source output..

Uses TRNG / PTRNG acronyms.

# AIS 20 / AIS 31 (German BSI, CC)

## Even translated to Russian and published by TK26 ..

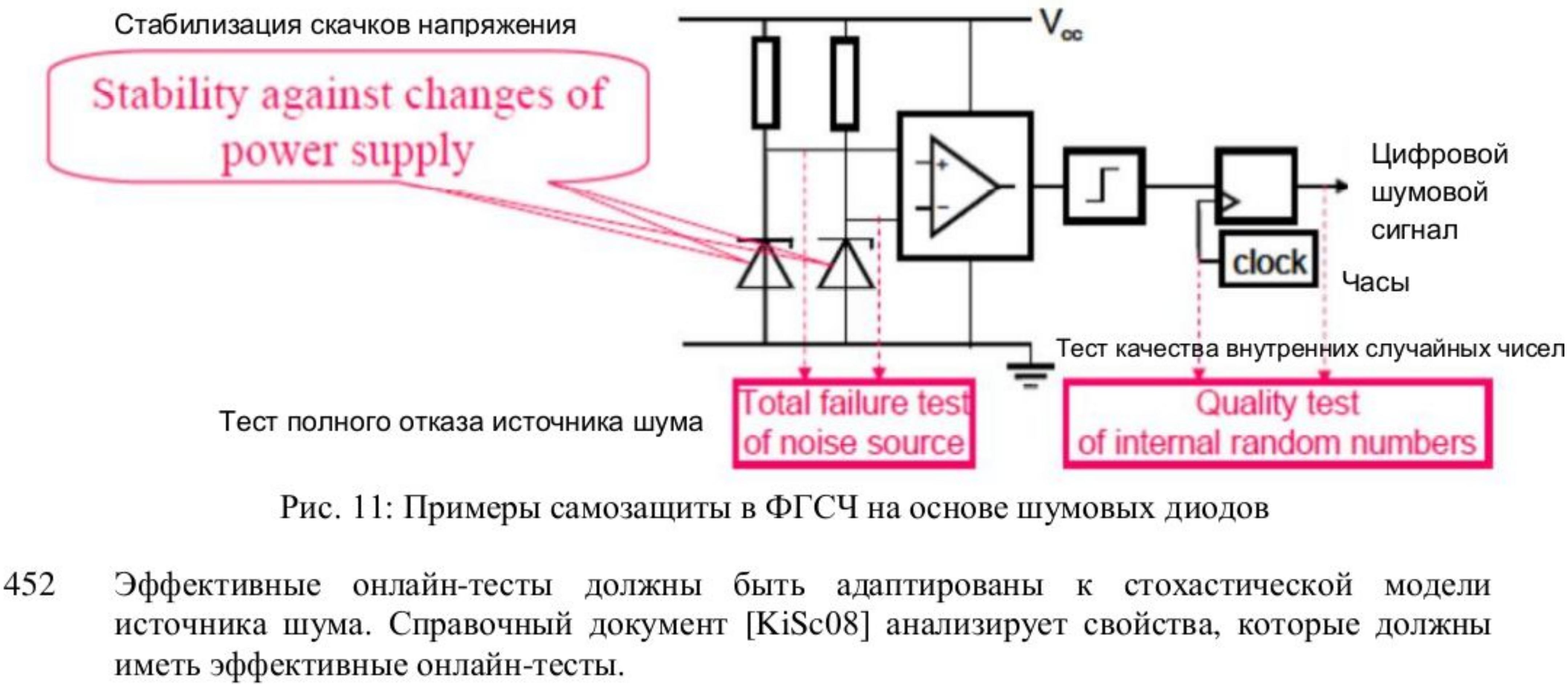

Стабилизация скачков напряжения
Stability against changes of power supply
$V_{cc}$
Цифровой шумовой сигнал
clock
Часы
Тест качества внутренних случайных чисел
Тест полного отказа источника шума
Total failure test of noise source
Quality test of internal random numbers

Рис. 11: Примеры самозащиты в ФГСЧ на основе шумовых диодов

452 Эффективные онлайн-тесты должны быть адаптированы к стохастической модели источника шума. Справочный документ [KiSc08] анализирует свойства, которые должны иметь эффективные онлайн-тесты.

# Entropy Metrics

## Shannon Entropy > Min-Entropy (Rényi Entropies)

**<u>Shannon Entropy</u>** in AIS-31: Traditional “Compression Entropy”

$$H_1(Z_n) = -\sum_z p_z \log_2 p_z$$

**<u>Min-Entropy</u>** of SP 800-90B: “Guessing Entropy”

$$H_\infty(Z_n) = \min_z(-\log_2 p_z) = -\log_2(\max_z p_z)$$

Min-entropy is always smaller (or equivalent) to Shannon entropy. Can be a lot smaller! *Has different combining and “algebra” rules.*

# Physical Noise Source

## What is Required?

**It doesn’t need to be statistically “perfect” but it must be very well understood.**

- ✅ A stochastic model (or a heuristic argument) that explains why the noise source output is from a random, rather than pseudorandom (deterministic) process.
- ✅ A complete physical model is not necessary, but entropy needs to be justified on the technology node (Semiconductor process? Temperature? Freq? etc.)
- ✅ The noise source is not externally observable (e.g., strongly correlated with the time of day, external power or emissions, or otherwise public or predictable).

**Example:** For a *ring oscillator* one could show that the source derives an amount of physical entropy from local, spontaneously occurring Johnson-Nyquist thermal noise.

# Health Testing Circuitry

## Integral part of any Entropy Source

- SP 800-90B mandates circuitry in that monitors output bits and performs **Startup**, **Continuous**, and **On-Demand** Health Tests.

- Explicitly approved continuous health tests: Repetition Count Test (**RCT**), Adaptive Proportion Test (**APT**). Fairly simple fixed circuitry. Failure bounds are be derived from entropy estimates/claims.

- Vendor-defined tests. These should be derived from expected failure modes of the specific physical noise source design.

- **Example**: Ring Oscillator jitter is highly dependent on temperature; health tests must catch temperature anomalies, prevent output.

# Conditioners

## Integral part of any Entropy Source

- **Conditioners** condense raw noise source output into shorter bit strings with higher and/or more consistent entropy rate.

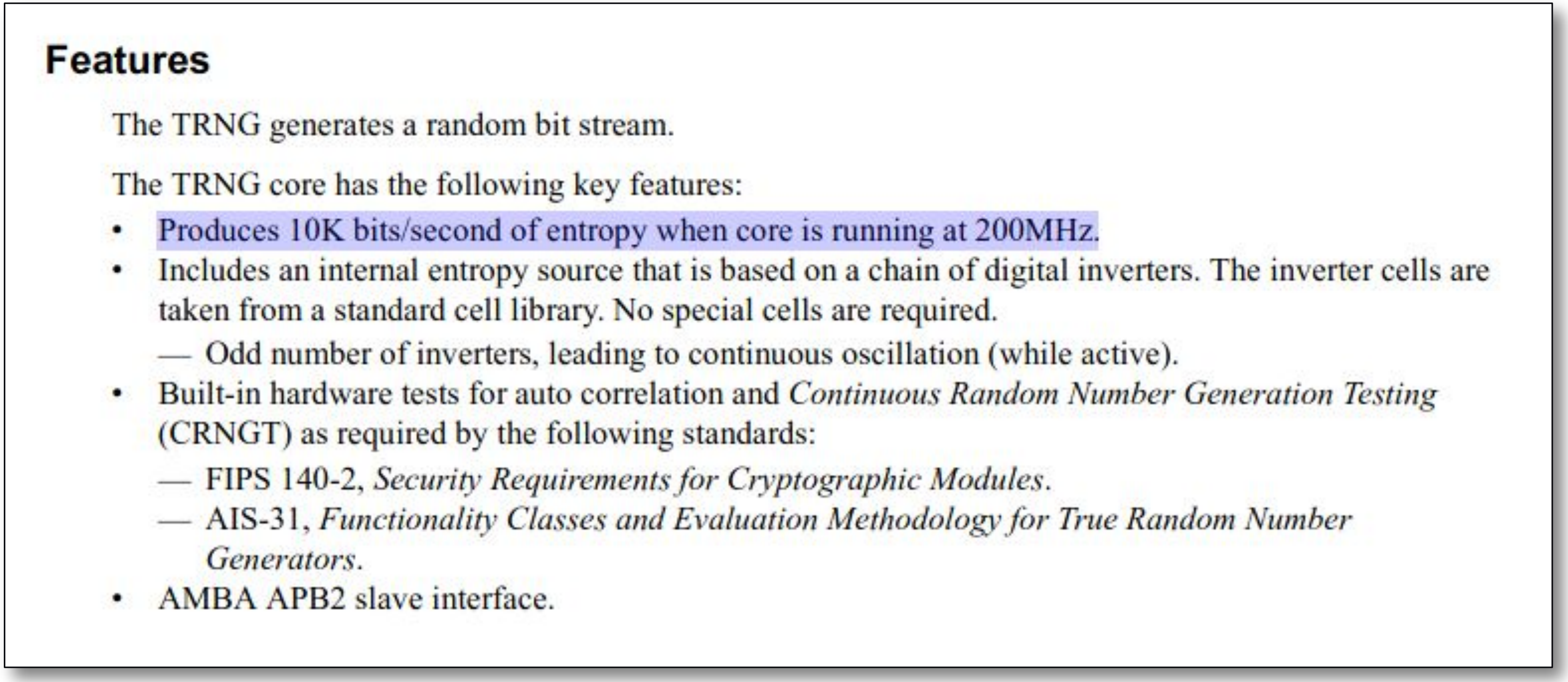
- Can be a part of the entropy source or external (SP 800-90C).

- **Vetted conditioners:** Things like NIST Hash functions (SHA-2/3), HMACs and some AES-based constructions are *pre-approved*. Can be validated with CAVP test vectors to be functioning correctly.

- **Non-Vetted conditioners:** Mathematical entropy extractors; von Neumann debiaser and other lightweight conditioners need testing but are fine as an intermediate post-processing step.

# Low Bit Rates are Usually Okay

## Remember that the Entropy Source just seeds the DRBG



### Features

The TRNG generates a random bit stream.

The TRNG core has the following key features:

- Produces 10K bits/second of entropy when core is running at 200MHz.
- Includes an internal entropy source that is based on a chain of digital inverters. The inverter cells are taken from a standard cell library. No special cells are required.
  - — Odd number of inverters, leading to continuous oscillation (while active).
- Built-in hardware tests for auto correlation and *Continuous Random Number Generation Testing* (CRNGT) as required by the following standards:
  - — FIPS 140-2, *Security Requirements for Cryptographic Modules*.
  - — AIS-31, *Functionality Classes and Evaluation Methodology for True Random Number Generators*.
- AMBA APB2 slave interface.

ARM's "TrustZone TRNG" is likely to be the most popular Random Number Silicon IP.
*In current (2020-) FIPS 140-3 terminology it is probably an* ***Entropy Source****.*

# Stochastic Models (Testing Labs: “Too Hard”)

## Justification: Gaussian Jitter from Physical Sources

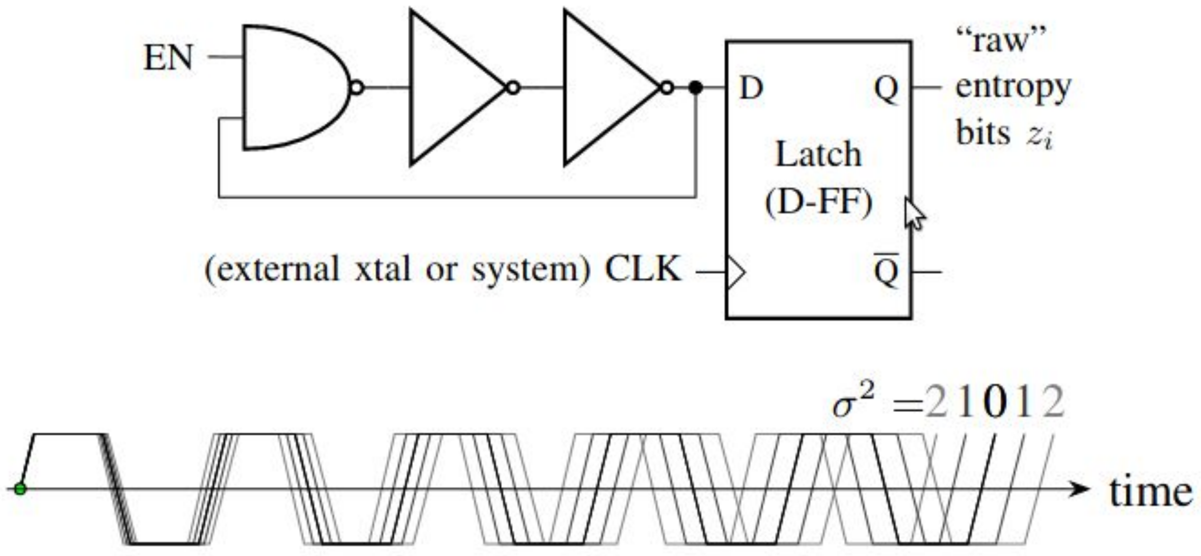
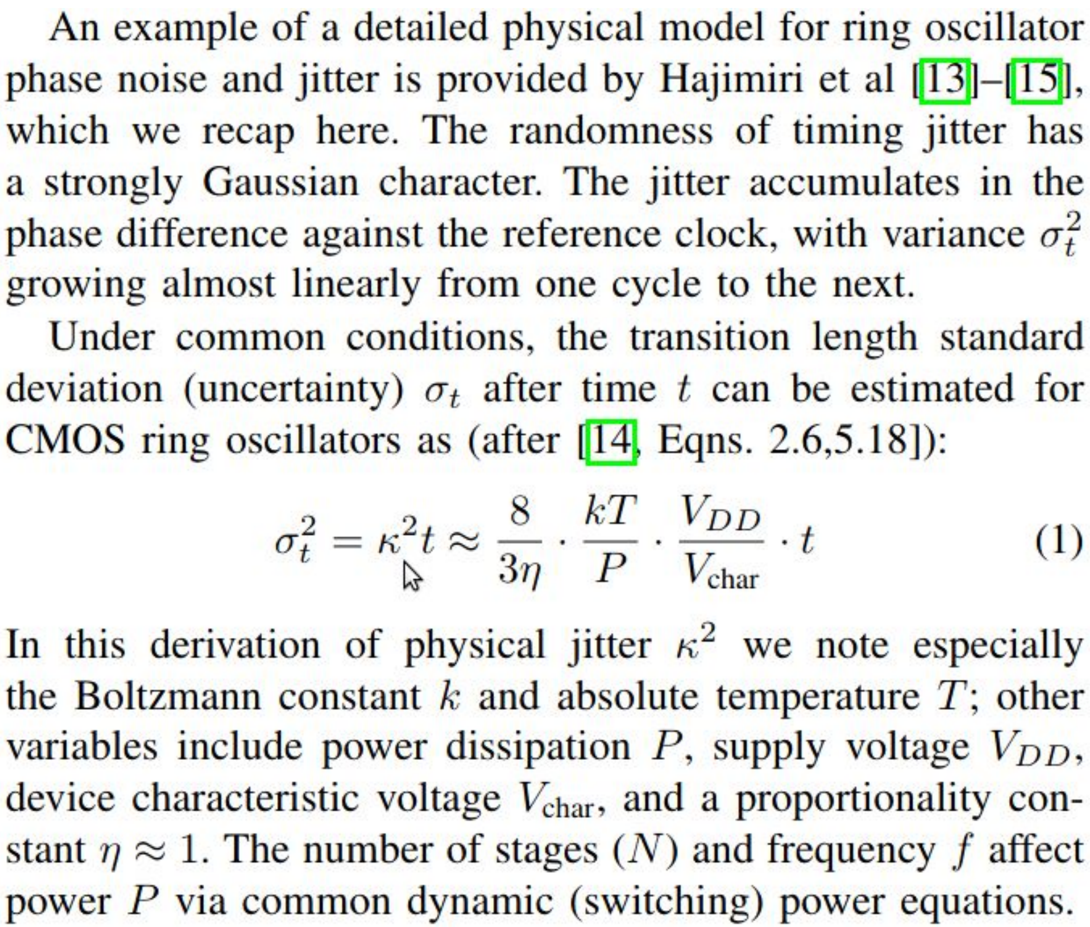


Fig. 1. A ring oscillator consists of an odd (here $N = 3$) number of inverters connected into a free-running loop. The output is sampled using an independent reference clock, such as a crystal oscillator. Transition times are affected by jitter (largely from Johnson-Nyquist thermal noise), whose accumulation causes samples to become increasingly unpredictable.



An example of a detailed physical model for ring oscillator phase noise and jitter is provided by Hajimiri et al [13]–[15], which we recap here. The randomness of timing jitter has a strongly Gaussian character. The jitter accumulates in the phase difference against the reference clock, with variance $\sigma_t^2$ growing almost linearly from one cycle to the next.

Under common conditions, the transition length standard deviation (uncertainty) $\sigma_t$ after time $t$ can be estimated for CMOS ring oscillators as (after [14, Eqns. 2.6,5.18]):

$$\sigma_t^2 = \kappa^2 t \approx \frac{8}{3\eta} \cdot \frac{kT}{P} \cdot \frac{V_{DD}}{V_{\mathrm{char}}} \cdot t \qquad (1)$$

In this derivation of physical jitter $\kappa^2$ we note especially the Boltzmann constant $k$ and absolute temperature $T$; other variables include power dissipation $P$, supply voltage $V_{DD}$, device characteristic voltage $V_{\mathrm{char}}$, and a proportionality constant $\eta \approx 1$. The number of stages ($N$) and frequency $f$ affect power $P$ via common dynamic (switching) power equations.

M.-J. Saarinen, *“On Entropy and Bit Patterns of Ring Oscillator Jitter“ (2021)* https://arxiv.org/abs/2102.02196

# Stochastic Models

## Justification: Gaussian Jitter to Entropy

- With a model like “Gaussian Thermal Jitter” $\sigma^2$ you can derive a distribution for output bits. This is the stochastic model.

- Stochastic model is <u>required</u> for AIS-31, preferred for SP 800-90B (heuristic arguments may still be enough for a FIPS 140-3 ENT).

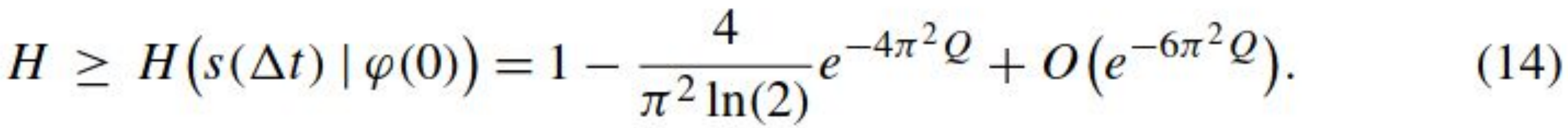
- The stochastic model, together with measurements is used to justify entropy content of noise source output. This is a key part of the Test Lab “entropy source report” in security certification.

# Entropy From Model

## Reports can borrow formulas from academic literature, but..

<u>Are the formulas really sane and applicable?</u>

This is complex-looking thing is sometimes seen in submissions:



$$H \geq H\big(s(\Delta t) \mid \varphi(0)\big) = 1 - \frac{4}{\pi^2 \ln(2)} e^{-4\pi^2 Q} + O\big(e^{-6\pi^2 Q}\big). \qquad (14)$$

( From: M. Baudet et al. *"On the Security of Oscillator-Based Random Number Generators"* J. Cryptol. (2011) 24: 398-425. )

The formula implies Entropy $H_1 > 0.4$ with **no Jitter** (Q = 0)..

🤔

# SP 800-90B Entropy Estimators

## A Big Set of Estimators, take the lowest value

- There is also a standard set of **entropy estimators** for the noise source and entropy output (both IID and non-IID versions).

- Lowest min-entropy estimate is the one overall result.

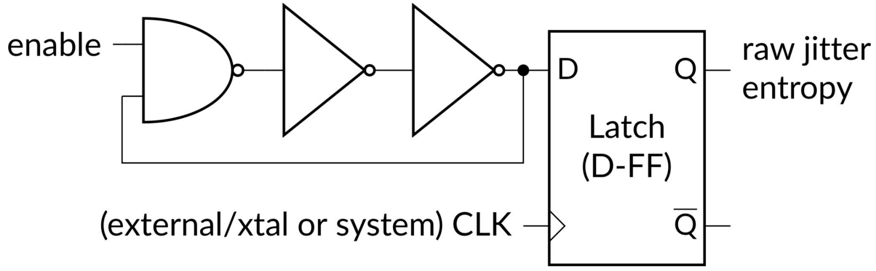
  https://github.com/usnistgov/SP800-90B_EntropyAssessment

1. *The Most Common Value Estimate*
2. *The Collision Estimate*
3. *The Markov Estimate*
4. *The Compression Estimate*
5. *t-Tuple Estimate*
6. *Longest Repeated Substring (LRS)*
7. *The MultiMCW Prediction Estimate*
8. *The Lag Prediction Estimate*
9. *The MultiMMC Prediction Estimate*
10. *The LZ78Y Prediction Estimate ..*

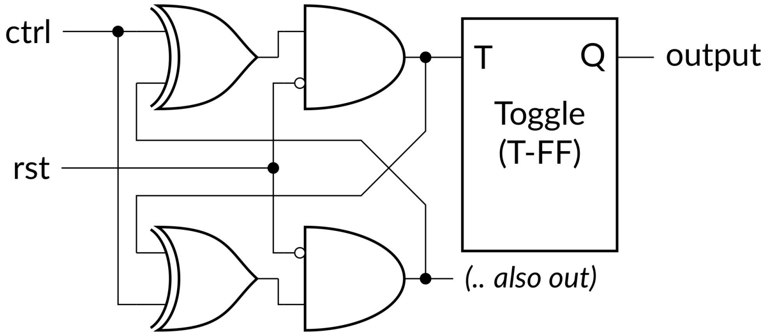
# Physical Noise Sources

## Need well-understood Entropy: Stochastic Models etc.

- **Ring Oscillators** are common choices. Can be built with standard cell libraries: Cheap and small area (as little as few thousand NAND2 gates).
- Entropy is from explainable source such as Johnston-Nyquist thermal noise.
- Note: Post-Quantum Crypto (PQC) doesn't need "quantum" noise sources.



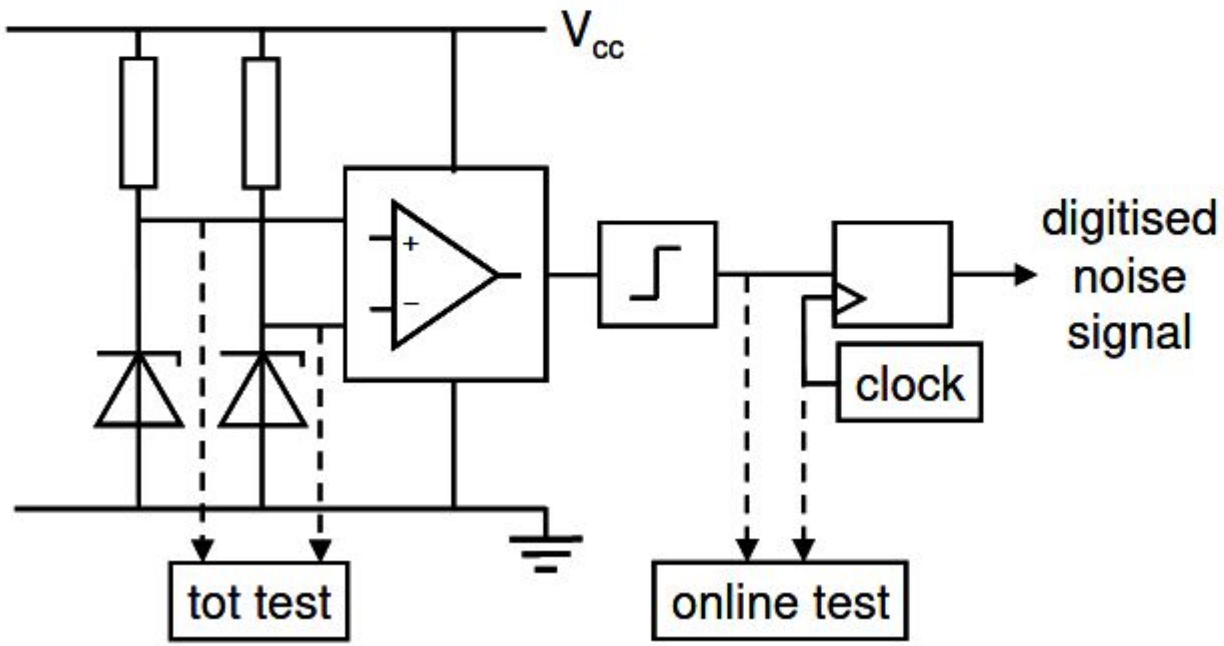
*A ring oscillator with 3 inverters in a free running loop.*



*A temporarily oscillating "metastable" TERO configuration.*

# Other Electronic Noise Sources

## If your security boundary contains a PCB

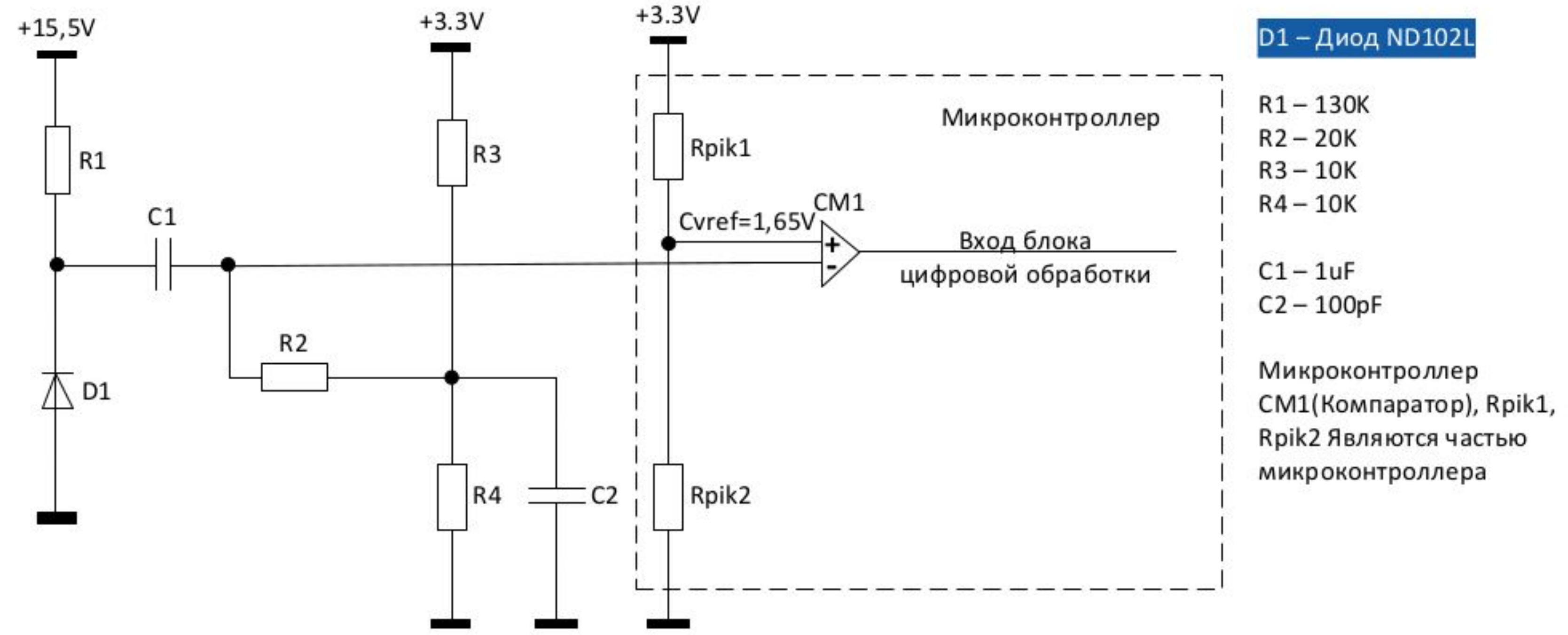


AIS-31 has an example design based on two noisy diodes (avalanche/zener breakdown) and an op amp. A stochastic model is described in [KiSc08].

# Other Electronic Noise Sources

## A Russian Single (Avalanche) Diode Design

Структурная схема аналогового блока приведена на рисунке 2.



Технические условия на изделие «ГСЧ Гроссмейстер», согласованные с войсковой частью 43753;

# Quantum Entropy Sources

## A bit more expensive to build (and to physically protect)

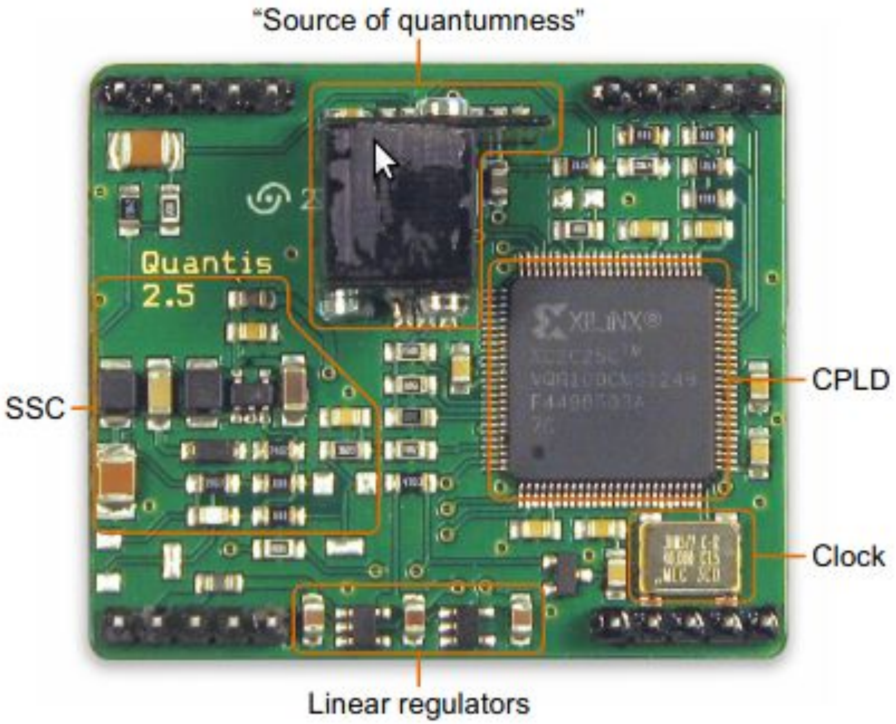


FIG. 1. Main PCB, component side. SSC - step-up switching DC/DC converter, CPLD - complex programmable logic device, Clock - system clock.

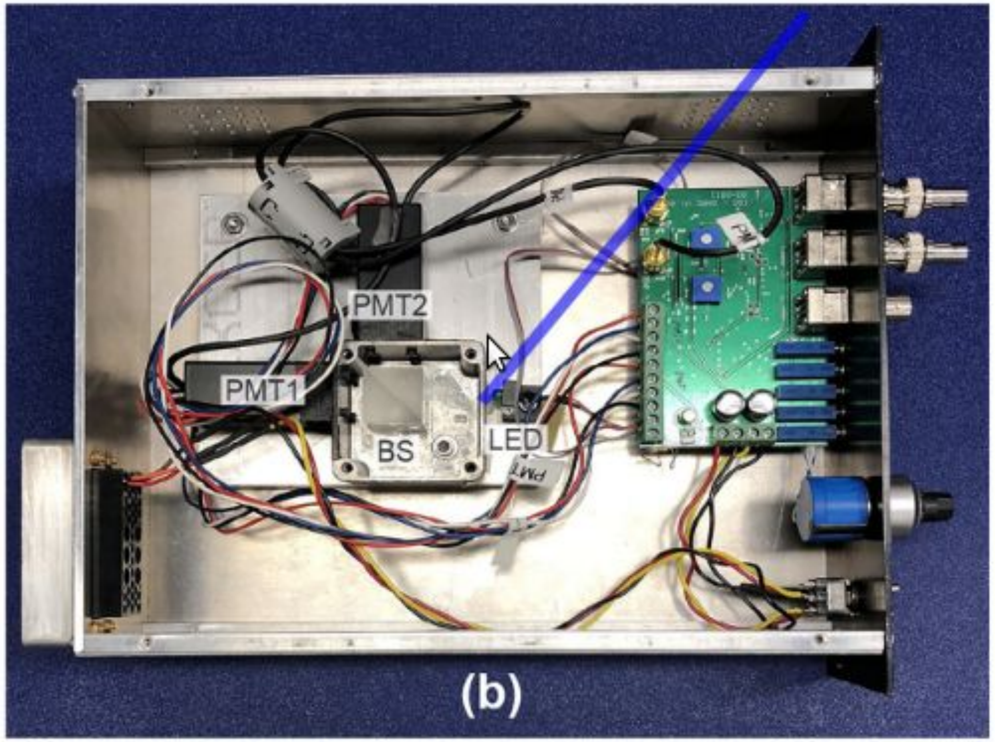


**Fig 6. Quantum random number generator under attack.** (a) Scheme of the QRNG. Light from a LED (green beam) passes a pinhole and a beam splitter (BS) with two outputs leading to detectors PMT1 and PMT2. For our attack we take advantage of a ventilation hole at the top of the case. With additional light, we can make one detector more likely to click. We show in blue a possible path from the ventilation hole to the pinhole that gives access to the metal box with the BS. (b) Picture of the prototype QRNG [65], with covers removed from the enclosure and beam splitter box. The path to the pinhole has been marked with a blue line.

https://doi.org/10.1371/journal.pone.0236630.g006

# Quantum Entropy Sources

## Are Photons more “Quantum” than Electrons?

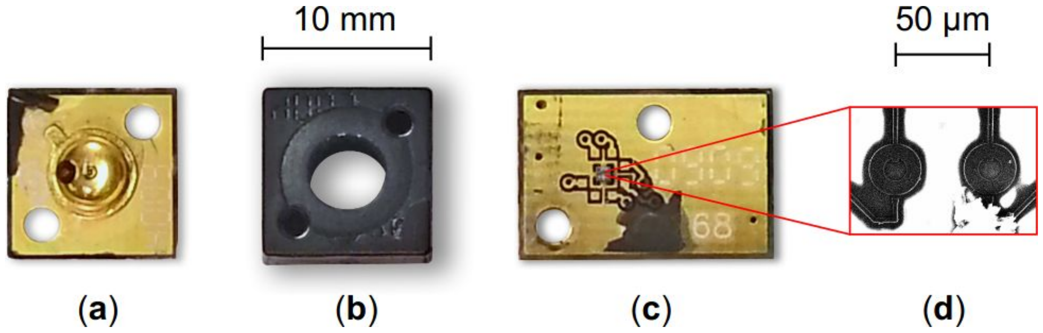


**FIG. 2.** “Source of quantumness” taken apart. (a) Light emitting diode (LED) light source. (b) Anodized aluminum sleeve. (c) Pair of single-photon detectors. (d) Photosensitive areas of the single-photon detectors (electron-microscope image).

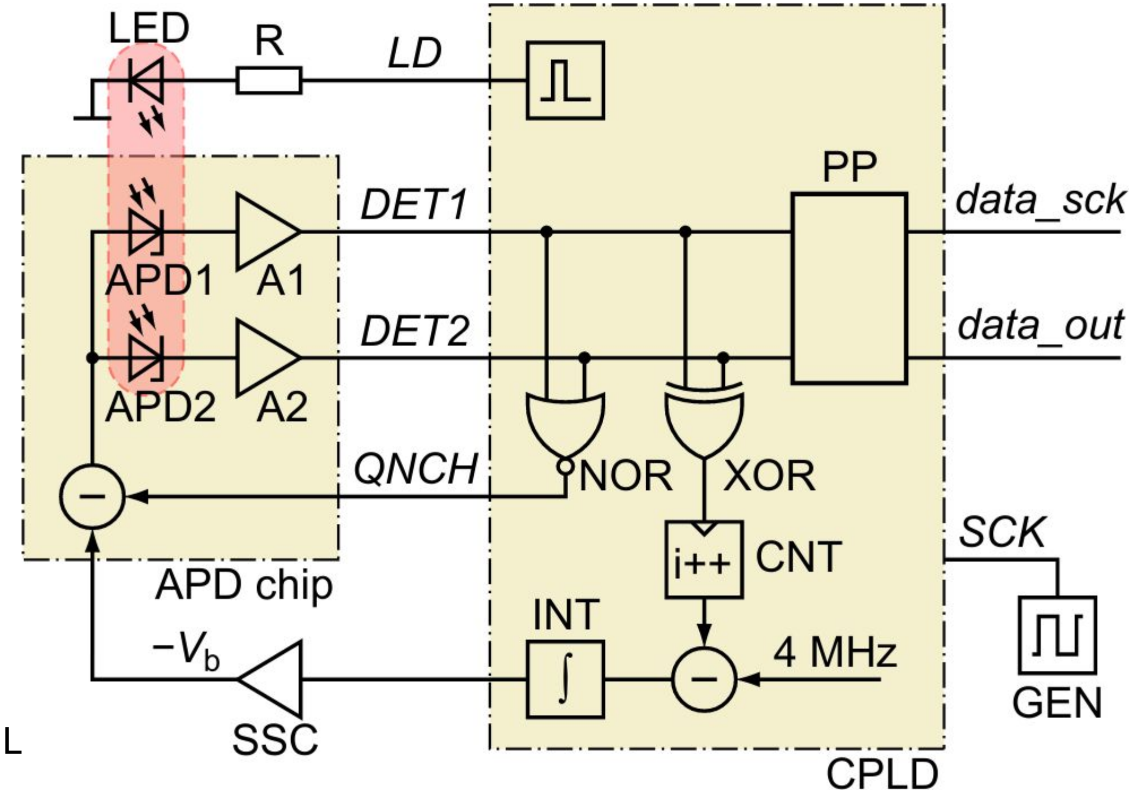


**FIG. 3.** Simplified electrical scheme of Quantis. A, amplifier; APD, avalanche photodiode; CNT, counter; CPLD, complex programmable logic device; GEN, clock generator; INT, integrator; LED, light emitting diode; NOR, inverted OR gate; PP, post-processing algorithm; R, resistor; SSC, switching power supply; XOR, exclusive OR gate.

Figures From: M. Petrov, I. Radchenko, D. Steiger, R. Renner, M. Troyer, V. Makarov. *"Independent security analysis of a commercial quantum random number generator"* (2020) https://arxiv.org/abs/2004.04996

# Quantum Entropy Sources

## NSA and GCHQ emphasize that they don’t require QRNGs

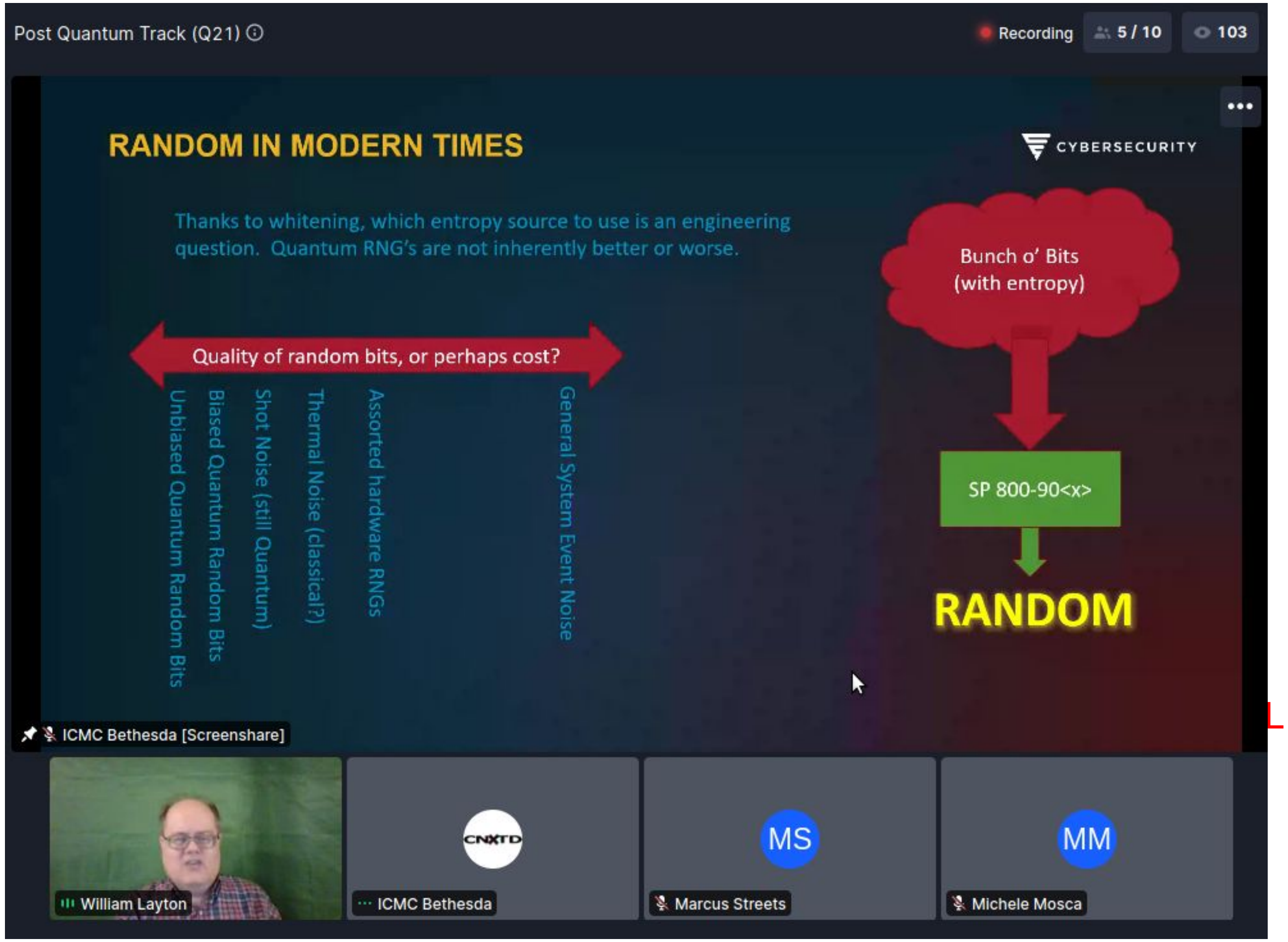
**NSA**: *“There are a variety of non-quantum RNGs available that have been appropriately validated or certified as acceptable for use in NSS or other government applications. They will remain secure even if a CRQC is built.”* (August 2021)
https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

**NCSC/GCHQ**: *“The NCSC believes that classical RNGs will continue to meet our needs for government and military applications for the foreseeable future.”* (March 2020)
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

After the infamous Dual_EC_DRBG generator (that was in SP 800-90A in 2006-2014), it is of course sensible to be suspicious of NSA’s random number recommendations. But I haven’t heard any good reason to use QRNGs either, but many reasons for not to.

# Military Requirements

## Or “National Security Systems” NSS / CSfC / NIAP



Thanks to whitening, which entropy source to use is an engineering question. Quantum RNG’s are not inherently better or worse.

Post Quantum Track (Q21)
Recording
5 / 10
103
RANDOM IN MODERN TIMES
CYBERSECURITY
Quality of random bits, or perhaps cost?
Unbiased Quantum Random Bits
Biased Quantum Random Bits
Shot Noise (still Quantum)
Thermal Noise (classical?)
Assorted hardware RNGs
General System Event Noise
Bunch o’ Bits (with entropy)
SP 800-90<x>
RANDOM
ICMC Bethesda [Screenshare]
William Layton
CNXTD
ICMC Bethesda
MS
Marcus Streets
MM
Michele Mosca

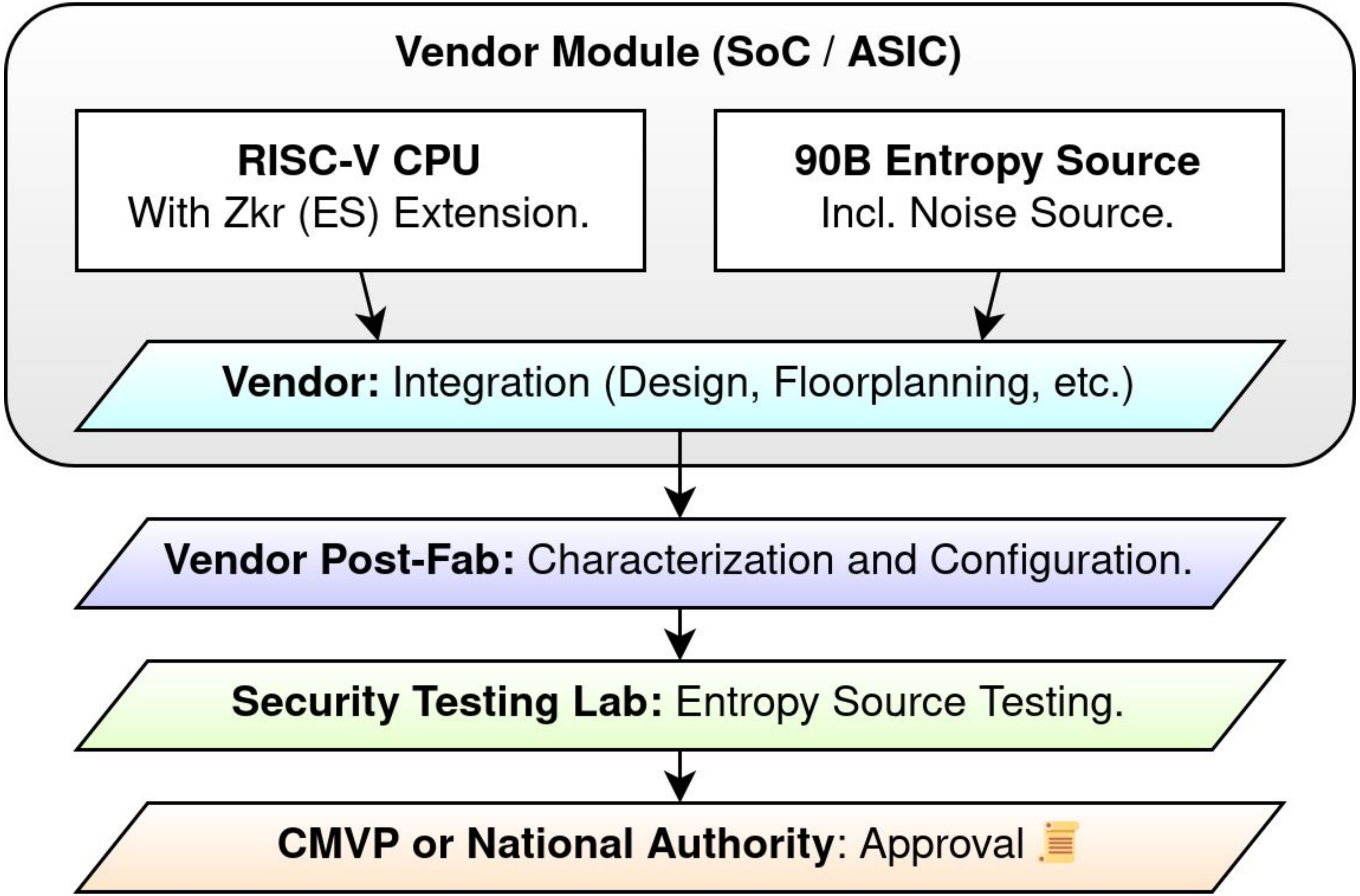
LIC

NSS / NIAP testing can use the same SP 800-90x concepts and procedures.

👉 NSA has no significant preference for the type of physical entropy source.

CNSA & Post-Quantum Transition has no impact on random numbers.

# Entropy Source Integration



**Vendor Module (SoC / ASIC)**

**RISC-V CPU**
With Zkr (ES) Extension.

**90B Entropy Source**
Incl. Noise Source.

**Vendor:** Integration (Design, Floorplanning, etc.)

**Vendor Post-Fab:** Characterization and Configuration.

**Security Testing Lab:** Entropy Source Testing.

**CMVP or National Authority**: Approval 📜