PEACE OF MIND IN A DANGEROUS WORLD

High-Quality Random Number Generation on a Semiconductor Device

Matti Tommiska, CEO, Xiphera Ltd.

November 11th, 2025

Agenda

I. Introduction to Randomness

II. RNGs overview

III. Hybrid RNG in an ASIC/FPGA

IV. Summary

Randomness

Examples of (Random) Bit Strings

- Which one of these bit strings is more random than the others?
- And which ones are less random than the others?

a) 0000000000000000

b) 0110001110101110

c) 1111111111111111

d) 0101010101010101

Examples of (Random) Bit Strings

- Which one of these bit strings is more random than the others?
- And which ones are less random than the others?

a) 0000000000000000

b) 0110001110101110

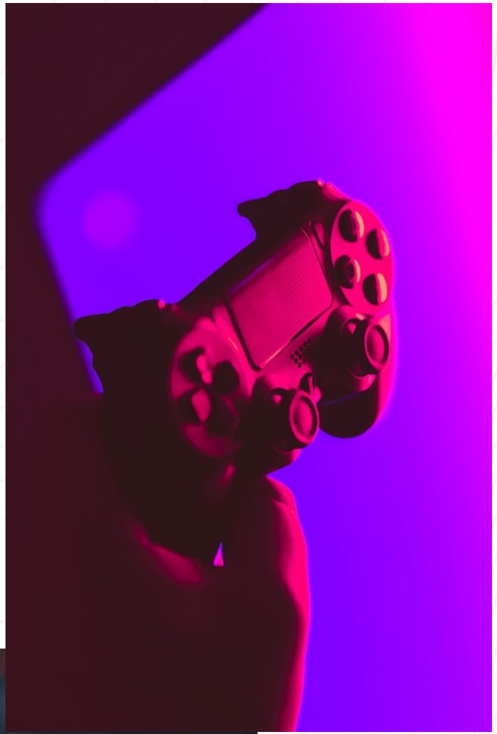
c) 1111111111111111

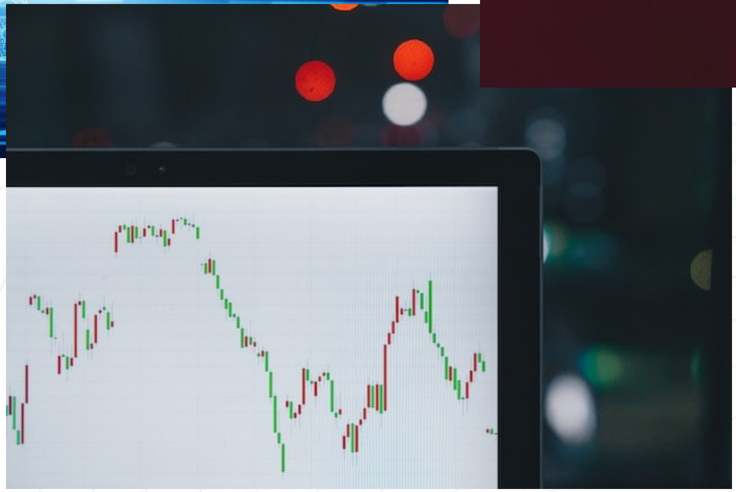
d) 0101010101010101

$$\frac{1}{2^{16}}$$

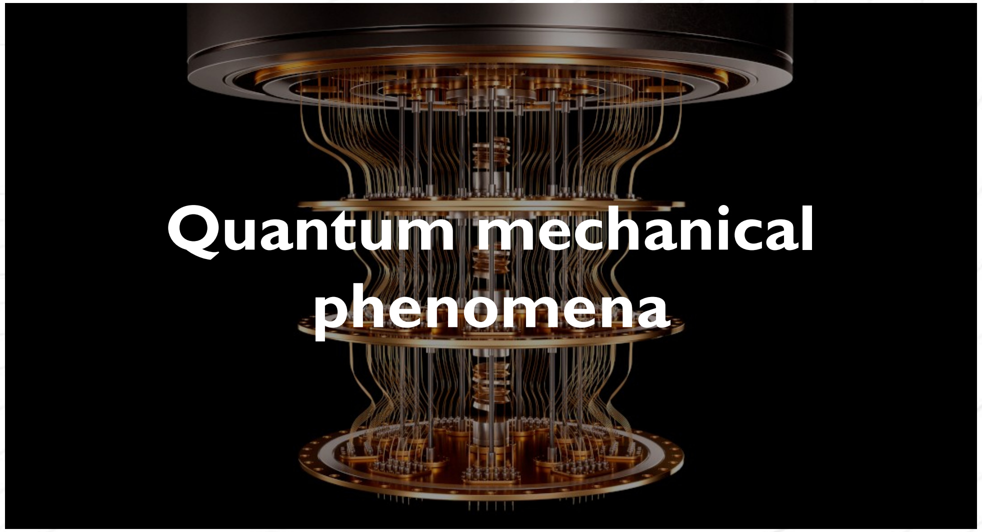
Where Is Randomness Used?

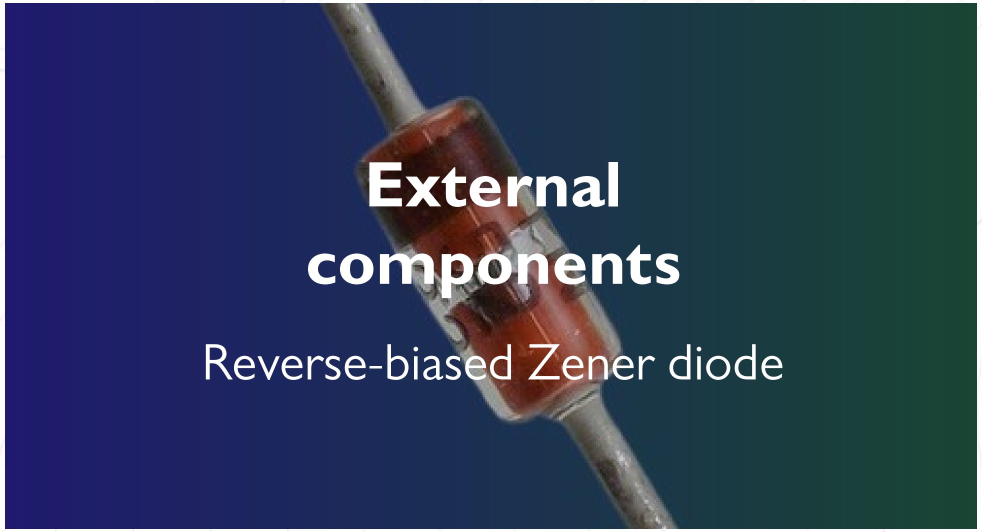
- *Randomness is vital for security!*
- Cryptography:
  - Seed material for secret keys
  - Initialization vectors
- Statistical simulations
- Games
- AI, ML models, LLMs

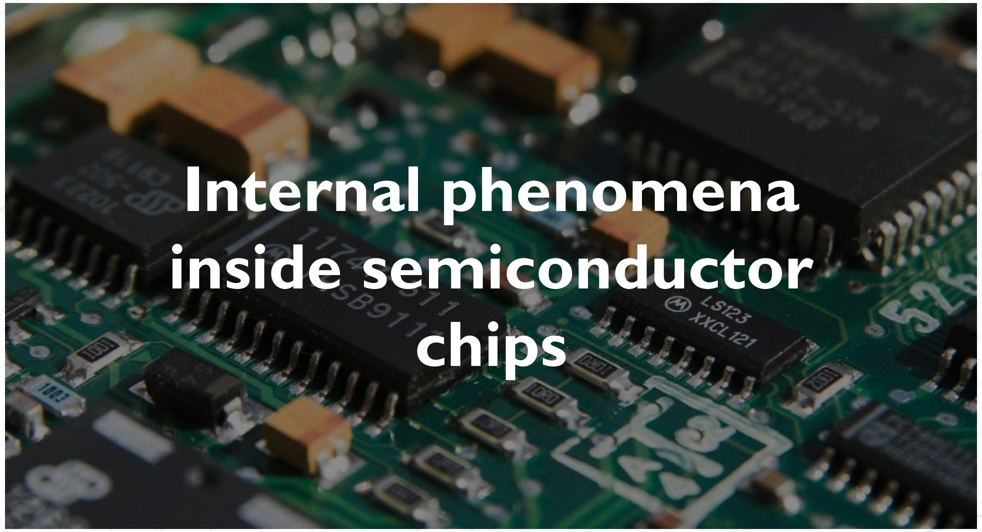




Entropy Sources







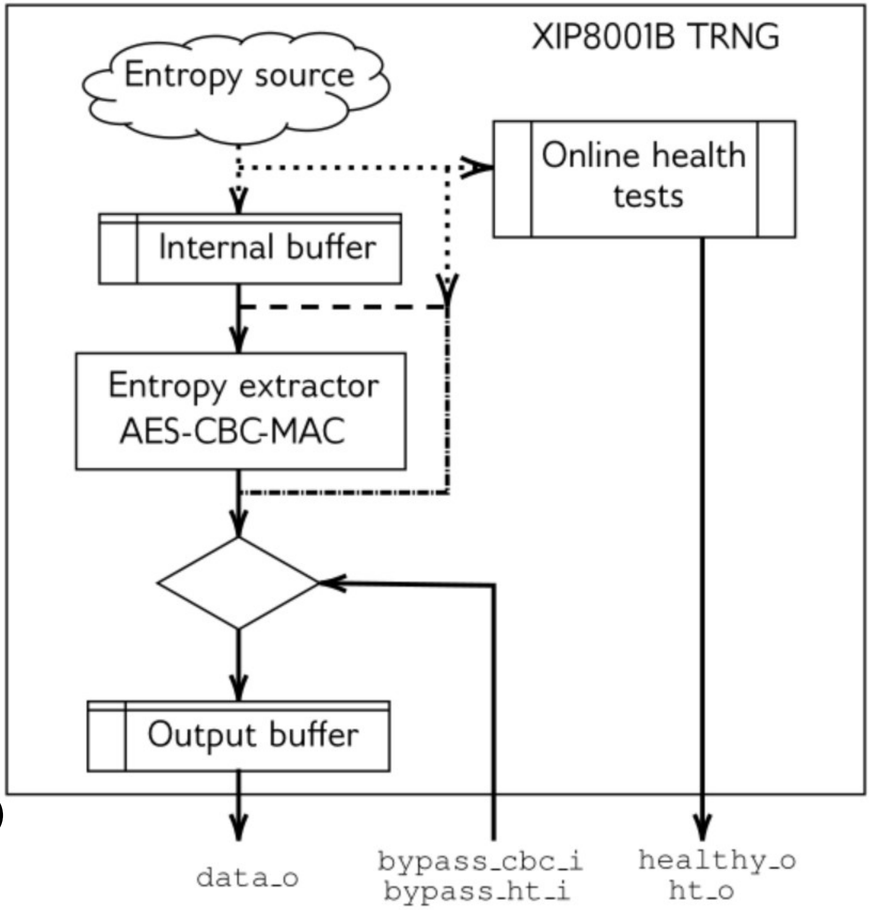
Random Number Generators (RNGs)

(T)RNG terminology & components

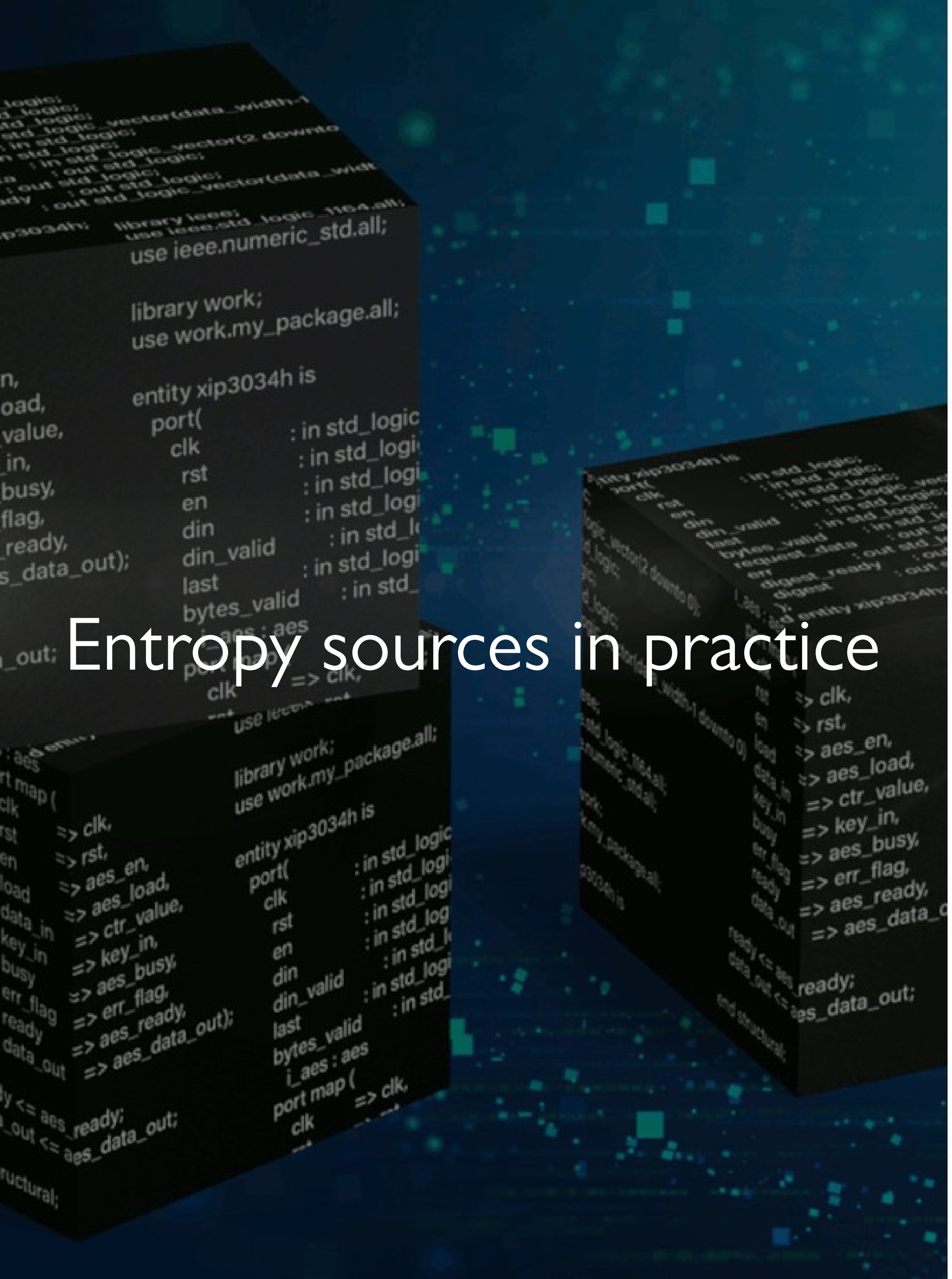
- TRNG, PRNG, CSPRNG, Hybrid RNG
  - Typical
- TRBG, PRBG, CSRBG, Hybrid RBG
  - NIST

- Entropy source
- Online health + Start-up tests
- Conditioning component or Entropy extractor
  - AES-CBC-MAC, GMAC, HASH (SHA3)

- PRNG typically based on some Cryptographic algorithm
  - (CS)PRNG needs a seed to expand the randomness from seed (TRNG)



xiphera.com/random-number-generation/true-random-number-generation



Entropy sources in practice

- Basic Entropy quality meters:
  - Shannon Entropy
  - Min-Entropy
  - Bias
- IID = Independent and identically distributed
- Standards:
  - NIST SP800-90A/B/C for TRNG, PRNG and entropy sources
  - AIS-31
- Stochastic model quantifies entropy source model

Entropy quality assessment

- Every entropy source and implementation needs assessment
- Tools and methods:
  - Standard compliance
  - Stochastic mathematical model
  - During implementation: Schematic, placement and timing analysis
  - After deployment: statistical tests
    - Modern: PractRand, gjrand and TestU01
    - Legacy: NIST SP 800-22 STS, FIPS 140, AIS31, ENT, Dieharder

- No need to test the output of NIST-approved conditioning component
  - Always IID random numbers


TRNG+PRNG
=
Hybrid RNG

Random Number Generation:

TRNG+PRNG

=

Hybrid RNG

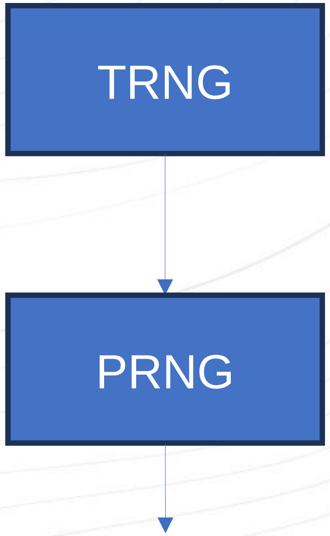
Xiphera Product codes:
XIP8001B,XIP8103B,XIP8103H

- True Random Number Generator - TRNG
  - High-entropy, Cryptographically secure ,true random numbers – essential for secure communications and cryptographic operations, such as key generation. Limited in speed.
- Pseudo Random Number Generator – PRNG
  - High throughput, cryptographically secure, when combined with TRNG/entropy source seeding
- Hybrid solution combines “best-of-both-worlds”

xiphera.com/random-number-generation/true-random-number-generation

Hybrid RNG (TRNG+PRNG)

- TRNG provides seed material for CSPRNG
  - Reseeded once certain amount of random data has been generated (every 2^{19} bits)
    - Prediction & backwards resistance = more often the better
  - If entropy source quality is high, can be used alone as seeder without conditioning

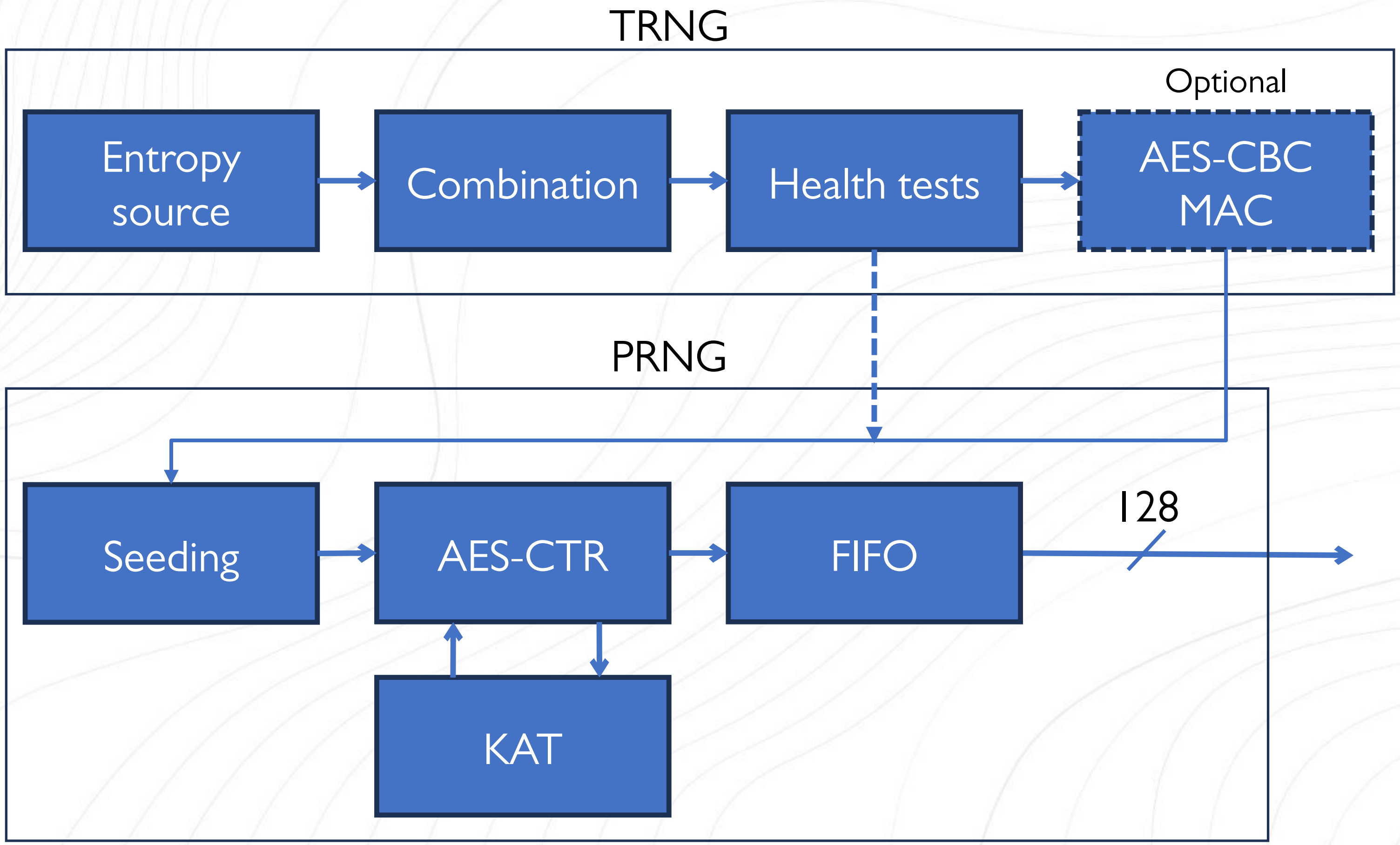


- PRNG expands seed into IID random numbers
  - High to extreme speeds
  - >1Gbps, 40Gbps, 100Gbps, and beyond

- Needed for high speed, quality random numbers
  - Data centre wide key distribution (Key distribution centre, KDC)
  - Large AI / LLM models
  - Large scale simulations

xiphera.com/random-number-generation/true-random-number-generation

Hybrid RNG (TRNG+PRNG)



Xiphera metrics:

- XIP8001B + XIP8103B/H
- Balanced: ~5k 6LUTs
  - 128 bits every 15 clock cycles = >1Gbps
- High speed: ~20k 6LUTs
  - 128 bits every clock cycle = >10Gbps

- Self contained and independent
- Little user control required
- AES-CBC-MAC optional
  - Saves 1k LUTs

xiphera.com/random-number-generation/true-random-number-generation

Summary

- Quality random numbers are the base of cryptography and cybersecurity
- TRNG and Entropy sources deployed in ASICs/FPGAs are great fit to produce randomness
- To achieve high throughput, a PRNG is needed
- Hybrid solution provides cryptographically secure random bits in tens of Gbps

PEACE OF MIND IN A DANGEROUS WORLD

Learn more at

xiphera.com/random-number-generation/

Xiphera Ltd.
info@xiphera.com
https://xiphera.com