



Tuesday, January 24, 2023

15:00 CET

**What Everyone  
Should Know About  
Randomness?**

**Webinar series:  
Cryptography  
Under the Hood**

Speaker

**Matti Tommiska**

CEO & Co-founder,  
Xiphera





# Agenda

- I. What is Randomness?
- II. Relevant Standards
- III. Structure and Testing of a Random Number Generator



# Quotes on Randomness

“The generation of random numbers is too important to be left to chance.”

– *Robert R. Coveyou*

“Random numbers should not be generated with a method chosen at random.”

– *Donald Knuth*

“Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.”

– *John von Neumann*



# 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

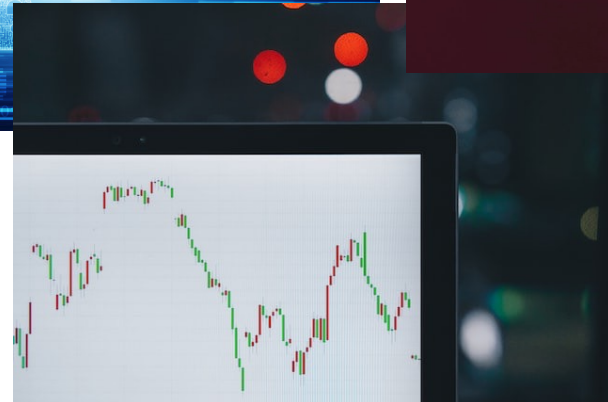
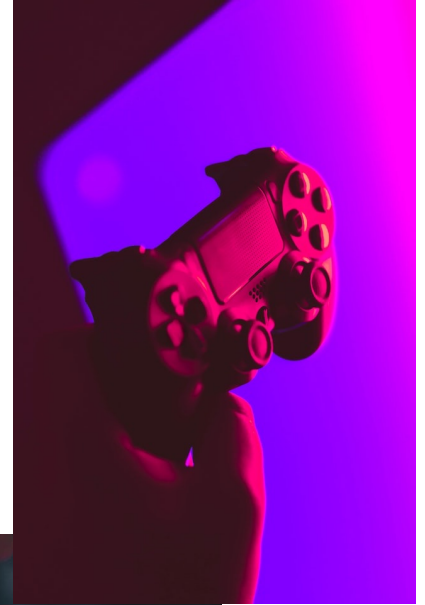
d) 0101010101010101

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



# Where Is Randomness Used?

- *Randomness is vital for Internet security!*
- Cryptography:
  - Seed material for secret keys
  - Initialization vectors
- Statistical simulations
- Games





# Entropy

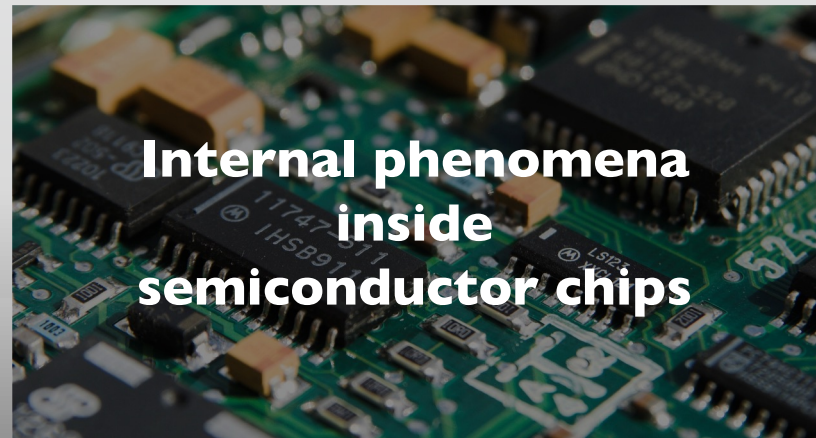
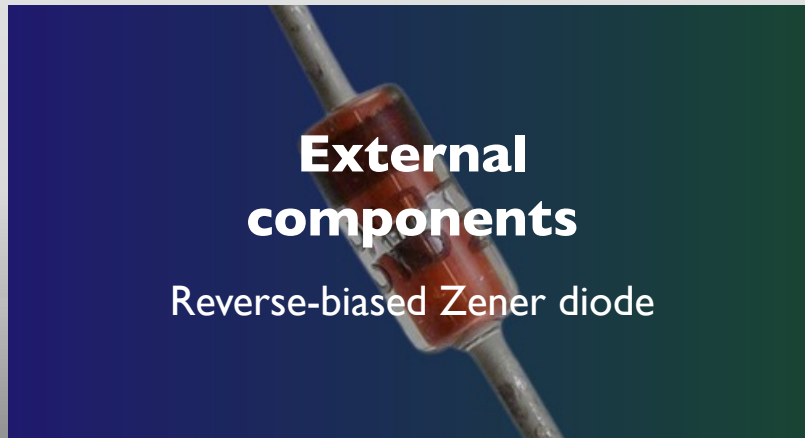
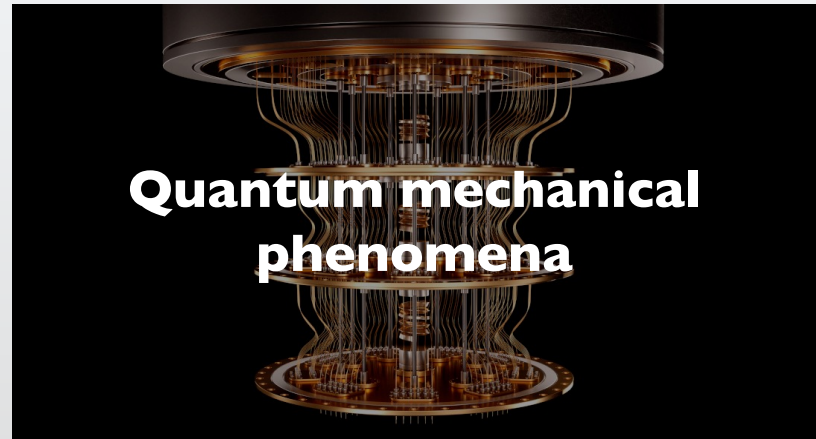
- Entropy  $\approx$  *unpredictability, unguessability*
- Shannon's formula (1948):

$$H(X) = - \sum_{i=1}^n P(x_i) \log(P(x_i))$$

- X is the source producing n number of different symbols, denoted by  $x_1, x_2, \dots, x_n$
- Each of these symbols has the probability of  $P(x_i)$
- The Shannon entropy is  $H(X)$ , where the measurement product H represents the information per symbol, or entropy per symbol, of the specific entropy source X
- Not to be confused with the entropy concept in thermodynamics!



# Entropy Sources







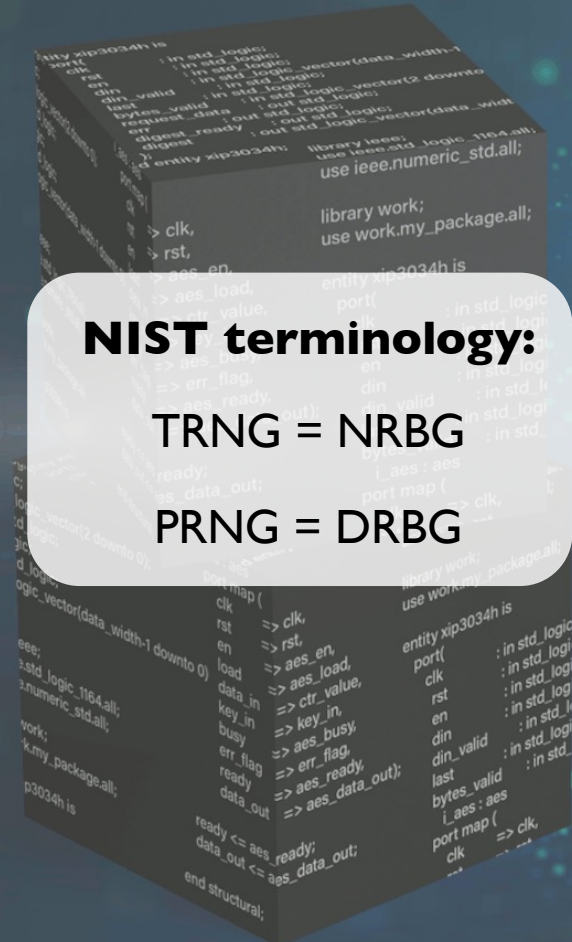
# Relevant Standards

- NIST SP 800-90A Rev. 1 (June 2015)
  - Recommendation for Random Number Generation Using Deterministic Random Bit Generators
  - "Specifications and requirements for approved PRNGs"
- NIST SP 800-90B (January 2018)
  - Recommendation for the Entropy Sources Used for Random Bit Generation
  - "How to design and test entropy sources (=TRNGs)"
- NIST SP 800-90C (September 2022)
  - Recommendation for Random Bit Generator (RBG) Constructions (3<sup>rd</sup> draft)
  - "How to connect TRNGs and PRNGs together"
- AIS-31: Functionality Classes and Evaluation for Physical Random Number Generators



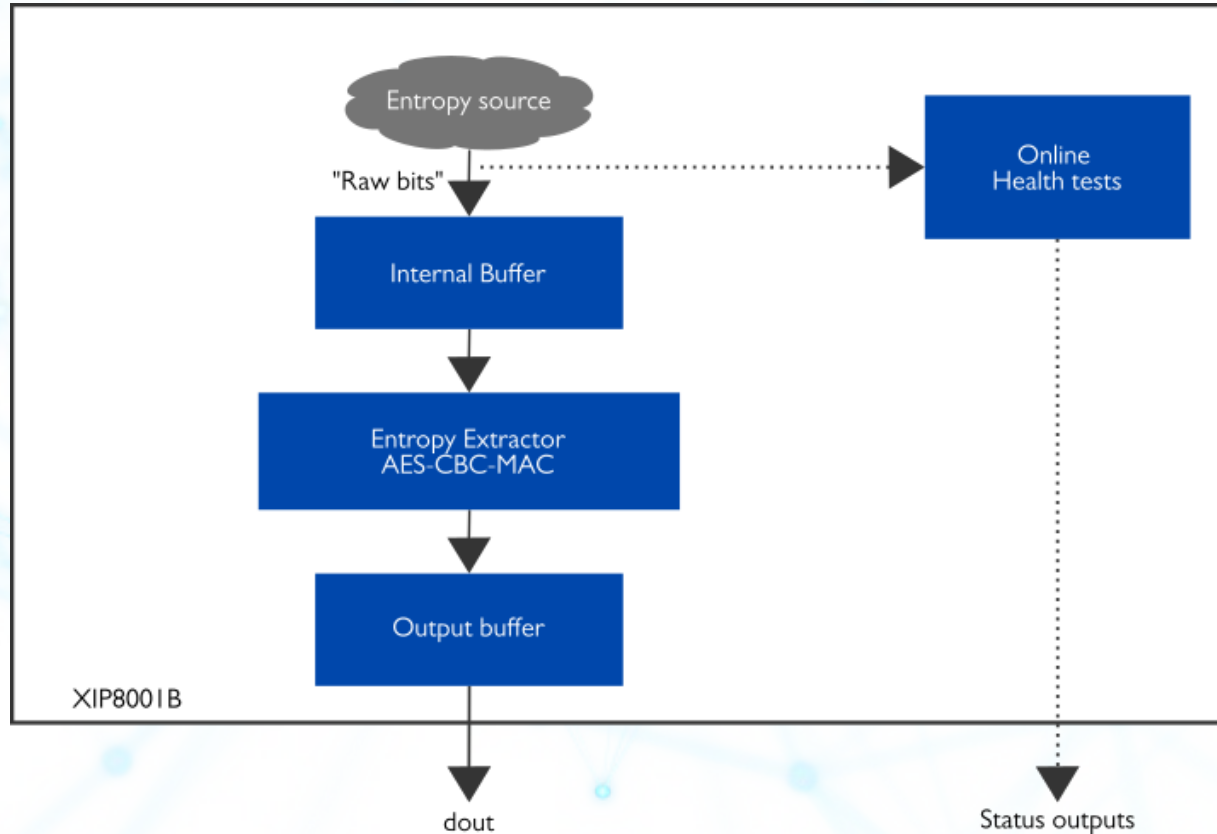
# TRNG and PRNG

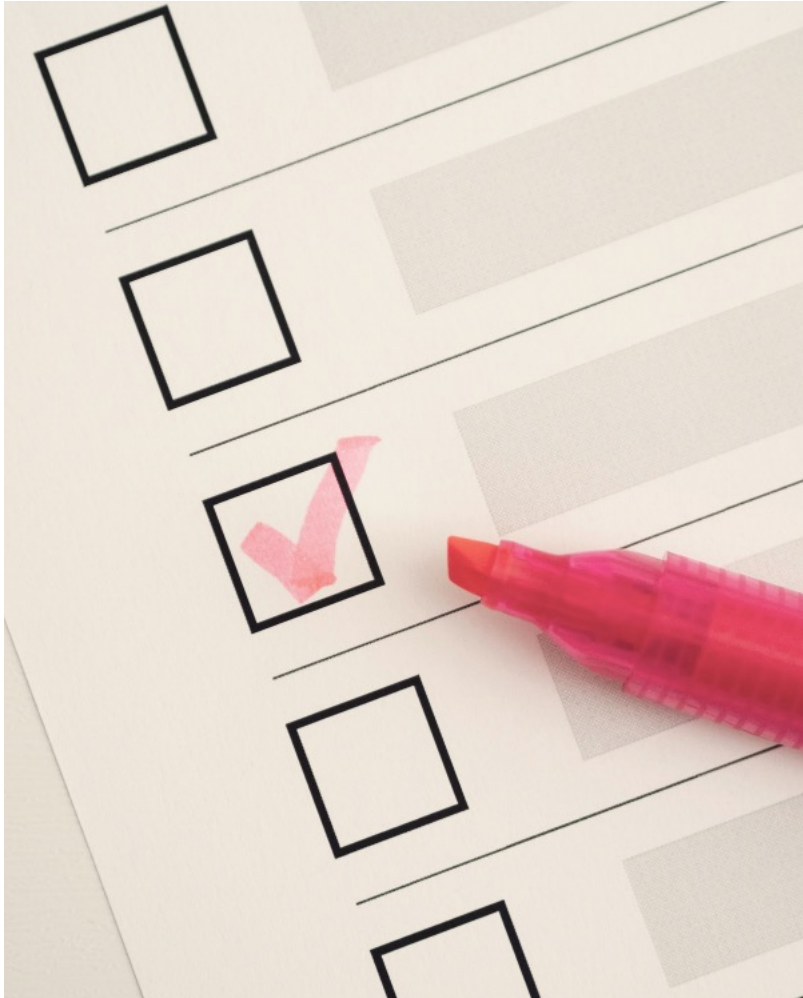
- It is important to distinguish between *True Random Number Generators (TRNG)* and *Pseudo Random Number Generators (PRNG)*!
  - pseudo (from Greek ψευδής, pseudes, "false")
- PRNGs are *deterministic*,
  - Always same output sequence with the same initial conditions
- PRNGs need to be periodically *re-seeded* by TRNGs
- PRNGs are typically fast and can be software-based





# TRNG Structure





# Testing

- Online testing
  - NIST SP 800-90B mandates the use of two health tests
  - Repetition count
  - Adaptive proportion
- Startup tests
- Offline testing
  - Statistical tests for random numbers are needed to verify the robustness of the entropy source
  - ent, gjrand, PractRand, TestU01, (SP 800-22 Rev. 1a (to be reviewed))



# Stochastic Model

- Passing offline statistical tests is a necessary, but not sufficient requirement for a true random number generator
- The entropy source needs to have a stochastic model

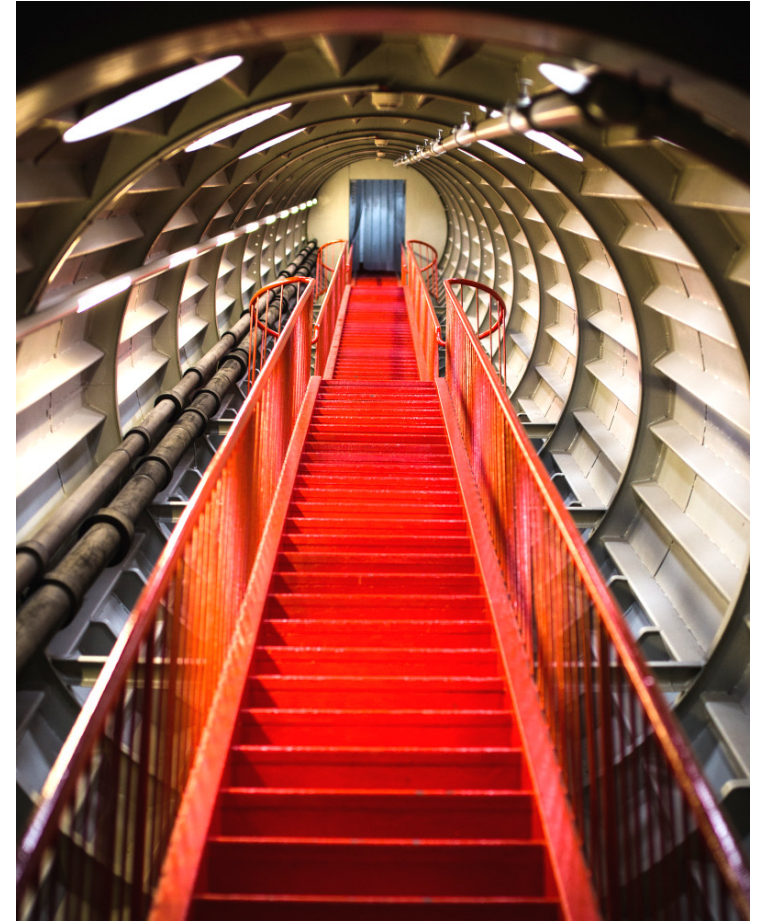
## BSI definition

*“The stochastic model provides a partial mathematical description (of the relevant properties) of a (physical) noise source using random variables.”*



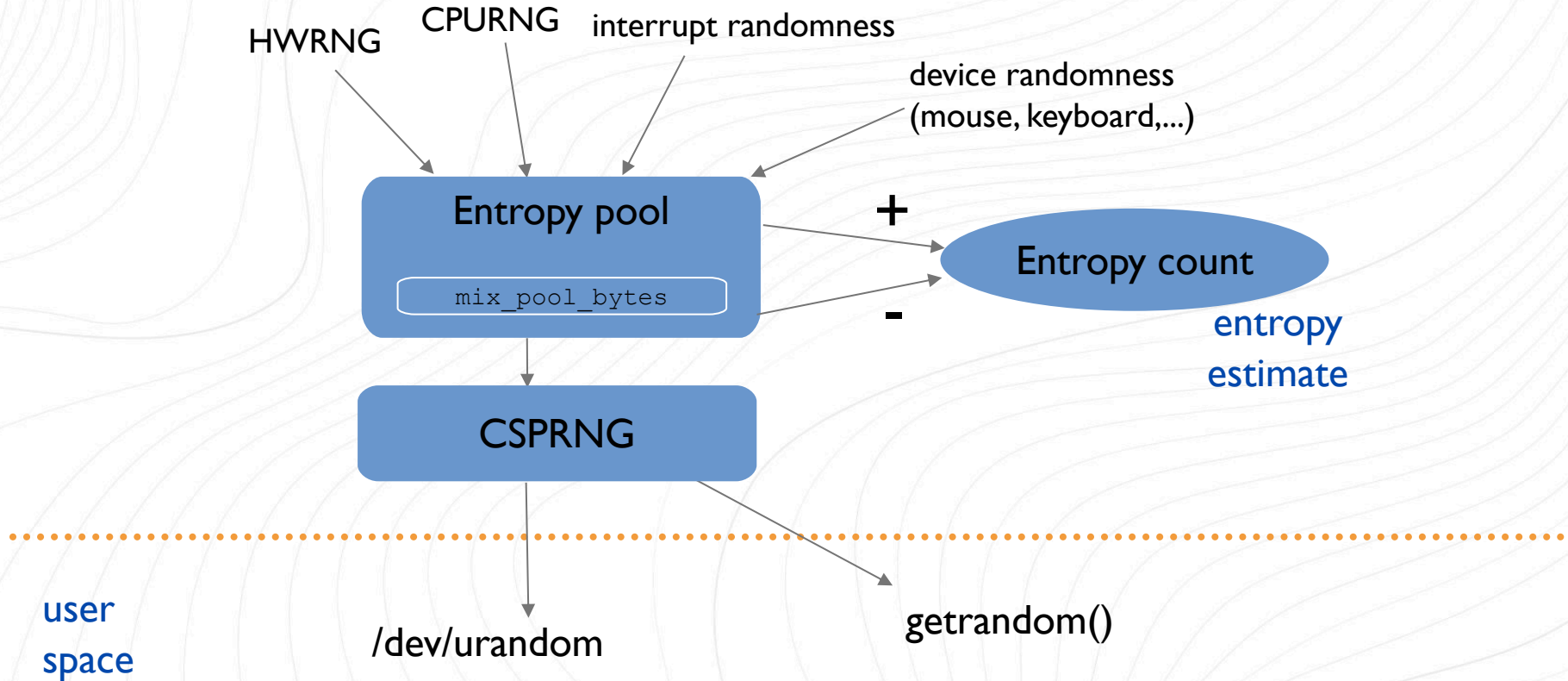
# Entropy Extractor

- Entropy extractor increases the entropy per bit to close to 1
- Decreases the rate of entropy source
- Entropy extractors standardized by NIST:
  - AES-CBC-MAC
  - AES-CMAC
  - Hash-based
    - ... and 3 derivation functions





# Integration with Operating System (Linux)






# Want to Experiment?

AMD  
XILINX


Home / App Store / True Random Number Generator with comprehensive statistical tests



Click to Enlarge

**True Random Number Generator with comprehensive statistical tests**

Xiphera's FPGA-based TRNG consists of an independent entropy source, online health tests and a standard compliant AES-CBC-MAC - based entropy extractor. The design complies with NIST SP 800-90B. More information can be found on [Xiphera's TRNG product description](#). In AWS platform TRNG can be evaluated for free for 14 days by collecting random data and analyzing it with provided free statistical tools. TRNG can also be added to an existing design to provide required randomness.

  
**Vendor:** Xiphera

**Try or Buy**

Obtain an entitlement to evaluate or purchase this product.

[Test Drive](#)

Click and run the virtual application demo for free.

[Free Trial](#)

Begin a free trial and run the application example below.

[Buy Now](#)

View and purchase available pricing plans for this application.

→ [True Random Number Generator with comprehensive statistical tests](#)





# Good Sources

- NIST SP 800-90A Rev. 1 (June 2015)
  - Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- NIST SP 800-90B (January 2018)
  - Recommendation for the Entropy Sources Used for Random Bit Generation
- NIST SP 800-90C (September 2022)
  - Recommendation for Random Bit Generator (RBG) Constructions (3rd Draft)
- AIS-31: Functionality Classes and Evaluation for Physical Random Number Generators
- David Johnston (2018): *Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers*
- Random Number Generation – Xiphos: <https://xiphos.com/random-number-generation.php>





# XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

# Thank you!

[www.xiphera.com](http://www.xiphera.com)

[info@xiphera.com](mailto:info@xiphera.com)

The logo for XIPHERA, featuring a stylized blue 'X' followed by the word 'IPHERA' in white, all in a bold, sans-serif font. The background of the entire image is a night sky with a starry pattern and a faint grid of green and blue lines, suggesting a digital or cryptographic theme. In the lower-left foreground, there is a silhouette of a person holding a flashlight that illuminates the ground.

# XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

**Cryptography  
Under the Hood**

will continue  
in early summer!

More info coming soon.

[www.xiphera.com](http://www.xiphera.com)

[info@xiphera.com](mailto:info@xiphera.com)

# Reference

Lightning image: Photo by [Johannes Plenio](#) on [Unsplash](#)

Zener diode image: <https://www.smeshops.com/st-bzx55c3v3-zener-diodeb2367456/>

Checkbox image by Freepik: [https://www.freepik.com/free-photo/top-view-marked-checking-box\\_5330479.htm#query=checklist&position=3&from\\_view=keyword](https://www.freepik.com/free-photo/top-view-marked-checking-box_5330479.htm#query=checklist&position=3&from_view=keyword)