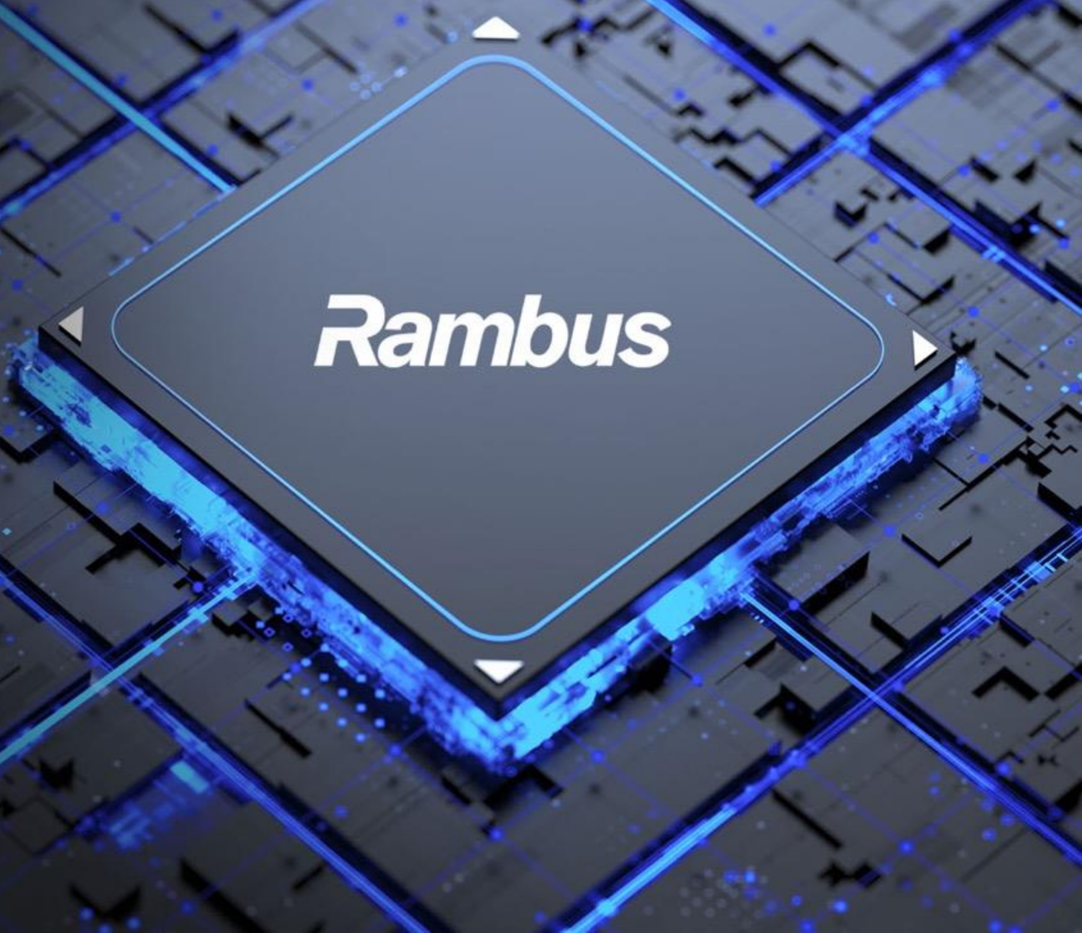
Random Number Generators in an Industrial Context



Rambus Secure Silicon IP

November 2024

Forward Looking Statement

Statements in this presentation concerning future prospects, business outlook, and product availability and plans are forward looking statements that involve a number of uncertainties and risks. Factors that could cause actual events or results to differ materially include: sales productivity; possible disruptive effects of organizational changes; shifts in customer demand; perceptions of the Company and its prospects; technological changes; competitive factors; unanticipated delays in scheduled product availability dates; general business conditions; and other factors. The information on the roadmap is intended to outline our general product direction and it should not be relied on in making purchasing decisions. The information on any roadmap shown is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release and timing of any features or functionality described for our products remains at our sole discretion. Future product will be priced separately. This roadmap does not constitute an offer to sell or license any product or technology.

Revised April 2023

Rambus

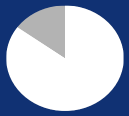
Data · Faster · Safer

$225M
2023 Product Revenue

$196M
2023 Cash from Operations

GSA 2023
Most Respected Emerging Semiconductor Company
$100-500M Revenue

Industry-Leading
Chips and Silicon IP



Data Center
>75% of Chip and Silicon IP Revenue

+42%
5-year CAGR
Product Revenue

34 Years Technology Leadership	San Jose HQ Global Footprint	~700 Employees >70% in Engineering	~2700 Patents and Patents Pending

Rambus Silicon IP Pedigree

Data Center | Automotive | 5G/Edge | Government | IoT

Silicon IP

Security IP
Security Cores and Provisioning

Interface IP
Memory and Peripheral Controller IP

Cryptography Research
- Root of Trust
- Quantum Safe Crypto
- DPA & FIA Resistance
- Secure Provisioning
- Defense Security

inside secure — DRIVING TRUST
- Root of Trust
- Classic Crypto
- Secure Protocol HW & SW
- MACsec & IPsec
- Memory Encryption

Northwest Logic
- HBM
- GDDR
- (LP)DDR
- MIPI

Hardent
- Display Stream Compression and Error Correction

PLDA
- PCIe
- CXL

Industry's Most Comprehensive Silicon Security IP Portfolio

Market Specific Product

- **Defense:** FPGA DPA FIPS
- **Auto:** Automotive ASIL
- **Cloud:** AI/ML
- **IoT Devices:** IoT; China
- **IIoT:** Industrial Automotive
- **5G Network:** OTNsec; 5G Networking
- **Cloud / Data Center:** Data Center 5G; Cloud Storage; PCIe Encryption
- **SoC:** Memory Encryption

Platform

Data-at-Rest Protection

- Programmable Root of Trust RT-6xx series
- FW Controlled Root of Trust RT-1xx/2xx series
- Secure Element CryptoIsland CI-300-P-C
- TrustZone CryptoCell CC-312 CC-71x

Data-in-Motion Protection

- MACsec HW & SW
- IPsec & TLS HW & SW
- TLS SW

Data-in-Use Protection

- IME & IDE AES/SM4-XTS/GCM DPA or non-DPA

Technology Differentiator Crypto Building Blocks

Platform Security Components

- Anti-Tamper
- Anti-Counterfeit
- Camouflage
- Canary Logic
- Entropic Array

Protocol Engines

- MACsec Engine
- IPsec Engine
- TLS Engine

Inline Encryption

- Inline Cipher Engine
- Inline Memory Encryption

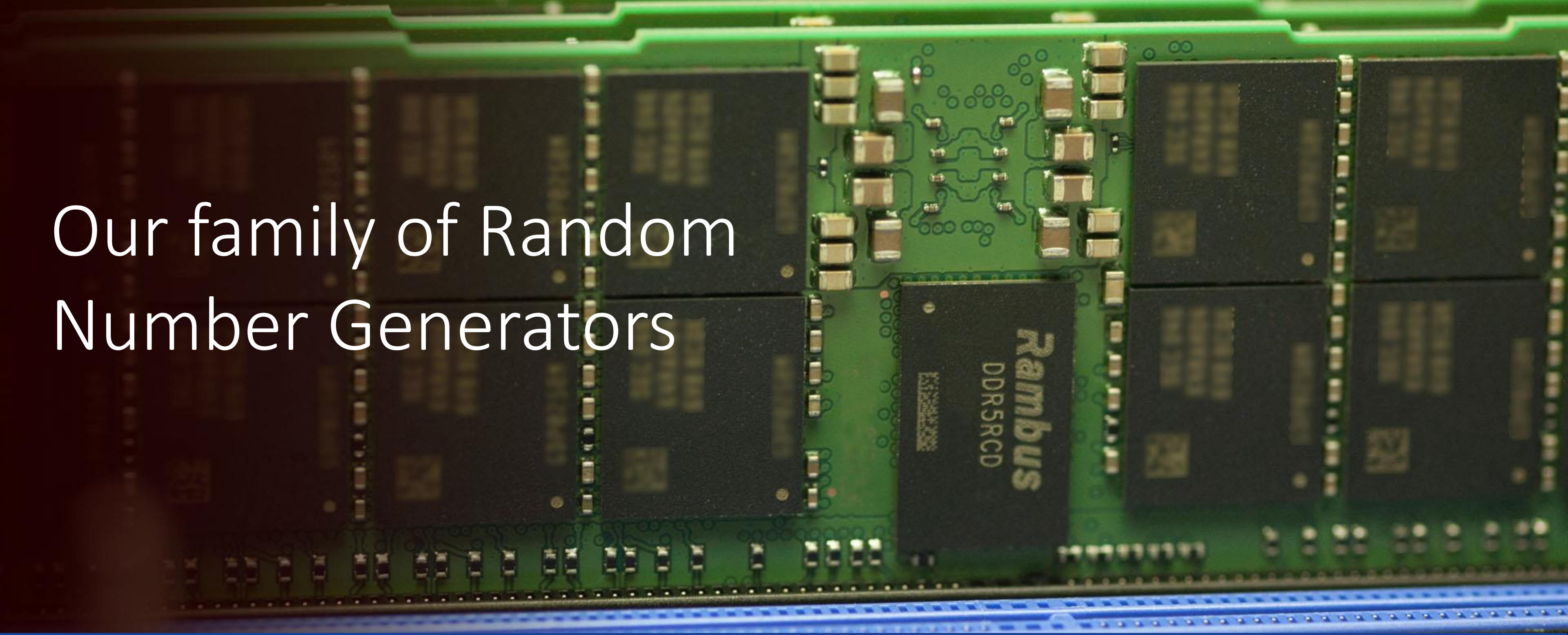
DPA and Fault Injection Protected Cores

- Public Key RSA-ECC-SM2
- Quantum Safe Crypto
- Symmetric AES & SM4
- HMAC Keyed Hash

Standard Crypto Accelerator Cores

- Public Key RSA-ECC-SM2
- Quantum Safe Crypto
- Random Nr Generator
- Symmetric AES-SM4
- Hash & HMAC SHA1/2/3-SM3
- Wireless Algorithms
- Lightweight Crypto

Our family of Random Number Generators

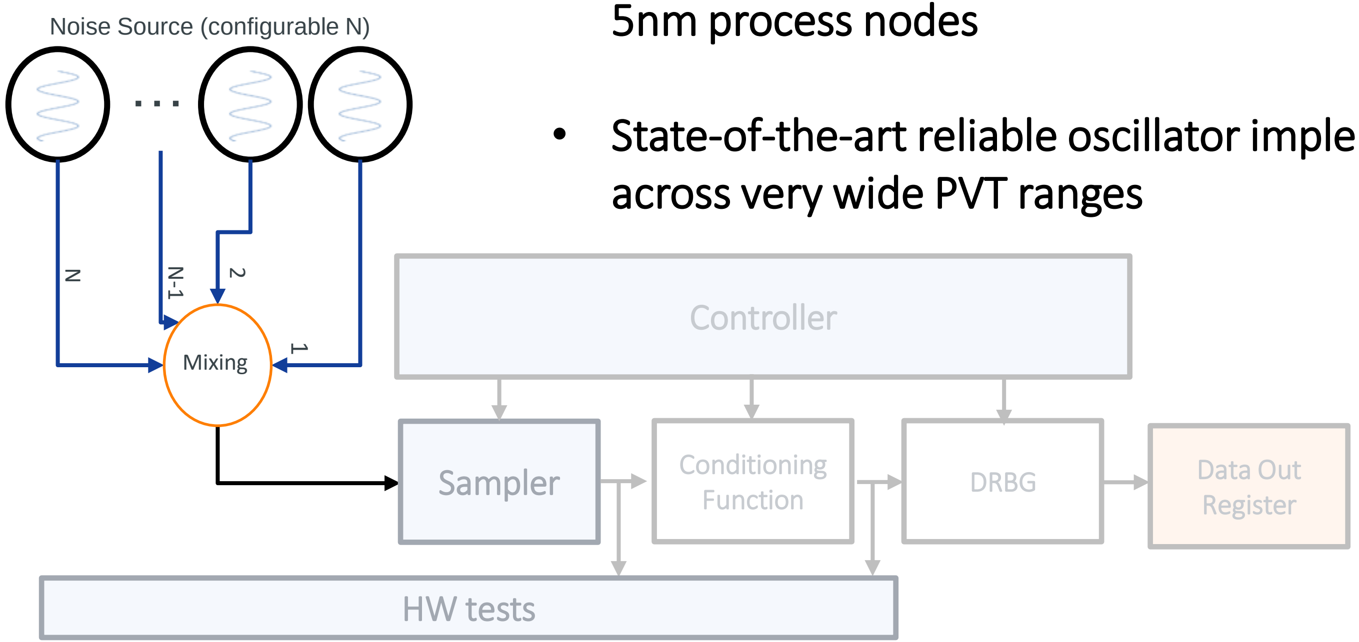


The forest hidden by a tree

Our family of Random Number Generators

The Noise Sources

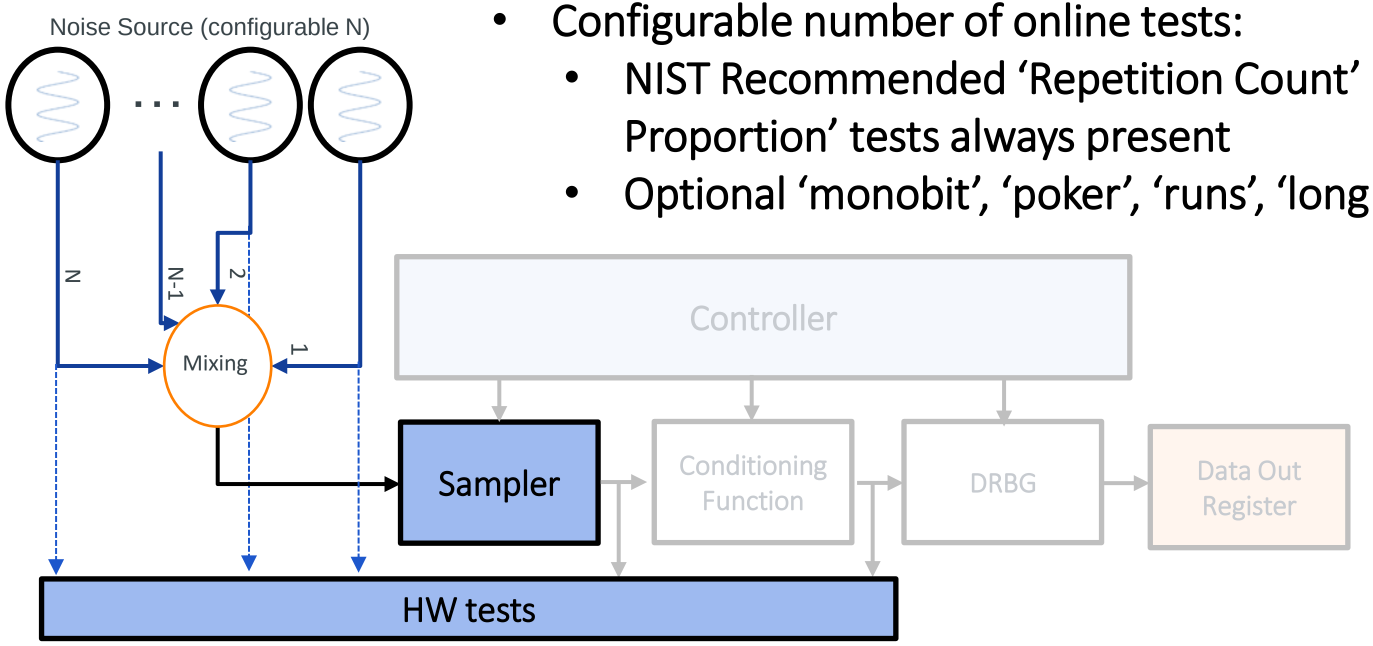
- 2 possibles 100% digital noise sources from 90 to less than 5nm process nodes
- State-of-the-art reliable oscillator implementation stable across very wide PVT ranges



Our family of Random Number Generators

Embedded Hardware Tests

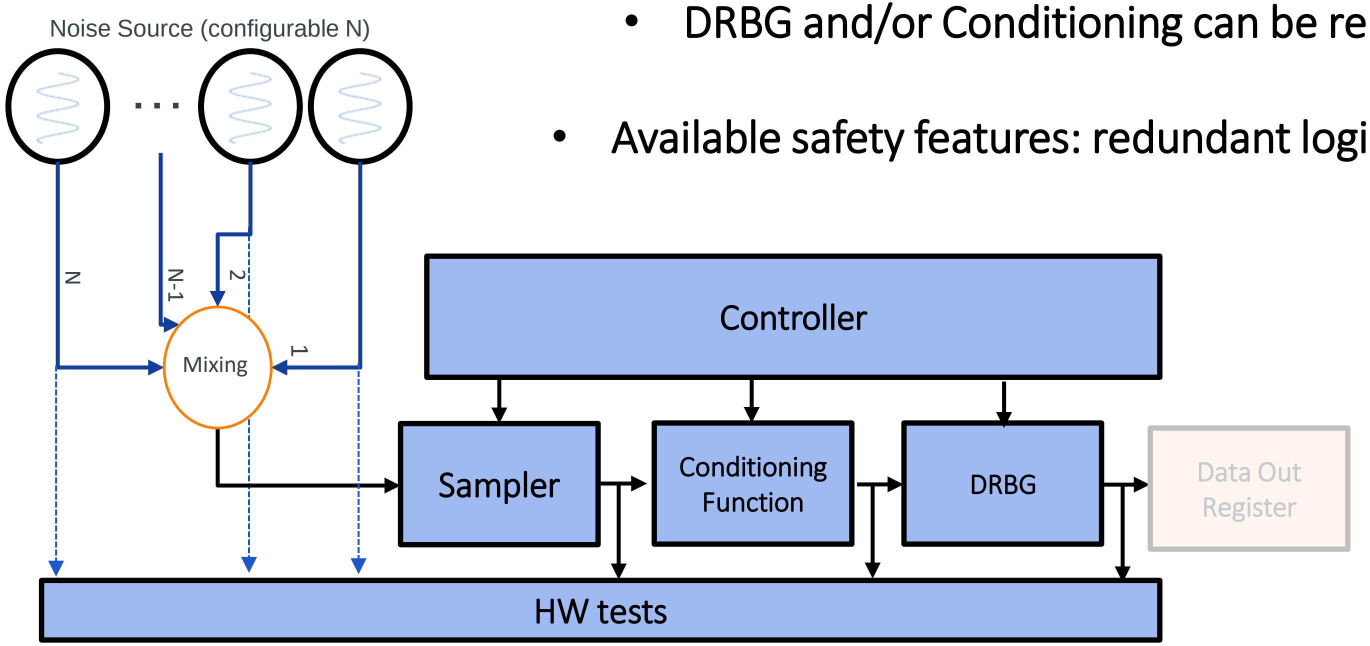
- Proprietary locking detector and built-in self-test circuits
- Configurable number of online tests:
  - NIST Recommended 'Repetition Count' & 'Adaptive Proportion' tests always present
  - Optional 'monobit', 'poker', 'runs', 'long runs'



Our family of Random Number Generators

Conditioning, DRBG and Safety features

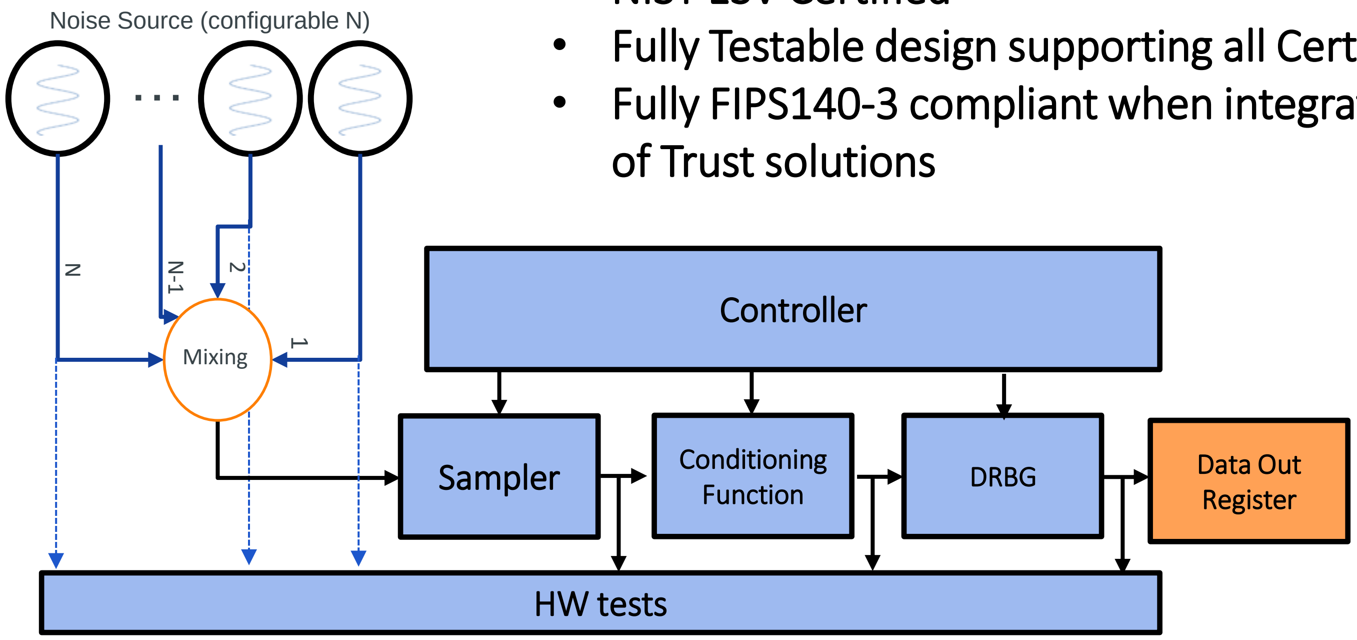
- Certified SHA-2 Conditioning function and AES-256-CTR DRBG
  - DRBG and/or Conditioning can be removed
- Available safety features: redundant logic & error detection



Our family of Random Number Generators

Compliances & certifications

- NIST SP800-90A/B/C, ANSI X9.31 & AIS-31
- NIST ESV Certified
- Fully Testable design supporting all Certification Testing
- Fully FIPS140-3 compliant when integrated into Rambus Root of Trust solutions

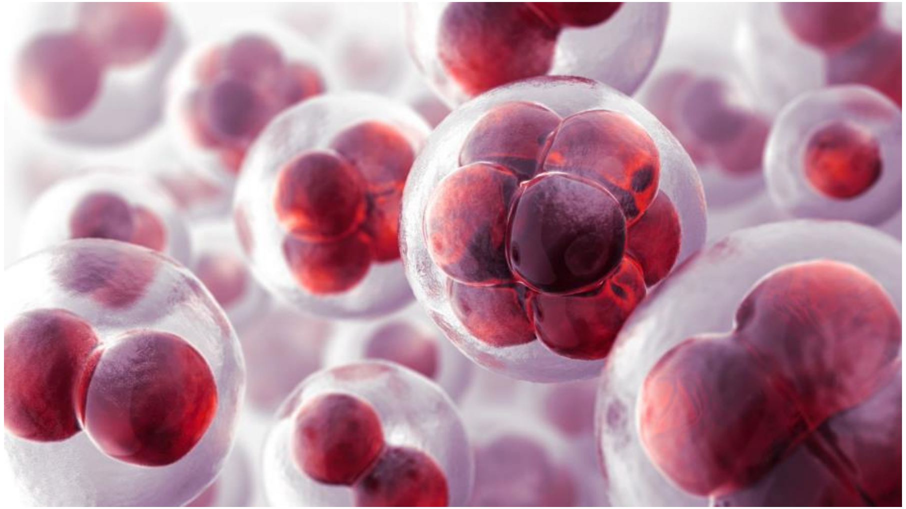


Intermediate Questions ?

Ring based TRNG from a different corner

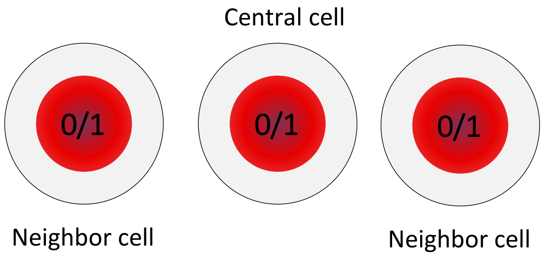
The forest hidden by a tree

Cellular Automaton

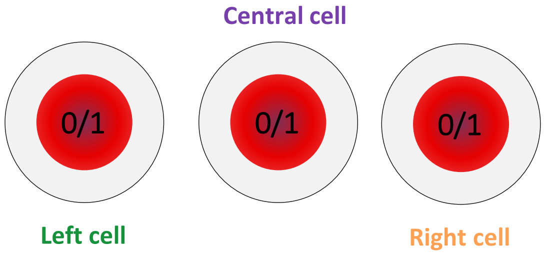


- A regular grid of cells:
- Each cell contains a “state”
  - chosen from a finite set
  - can evolve over time
- The state at time t+1 is a function of:
  - the state at time t
  - the states of neighbor cells

- Let us focus on simple cases:
  - Cells can only take two states
  - One-dimensional grid.



Cellular Automaton

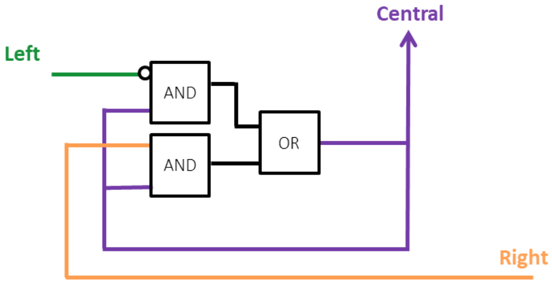


Truth table of a simple cell

t	Left	1	1	1	1	0	0	0	0
	Central	1	1	0	0	1	1	0	0
	Right	1	0	1	0	1	0	1	0
t+1	Central	1	0	1	1	1	0	0	0

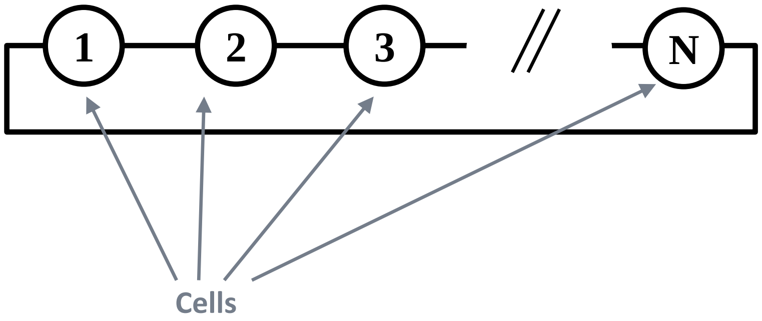
Wolfram code: 184 = $2^7 + 0 + 2^5 + 2^4 + 2^3 + 0 + 0 + 0$

- There are 2^3 possible neighborhood configurations
- 2^8 different ways of doing simple cells
- They are referred by their Wolfram code
- Easy to implement with logic gates



Cellular Automaton Ring

- Cells can be looped as a ring

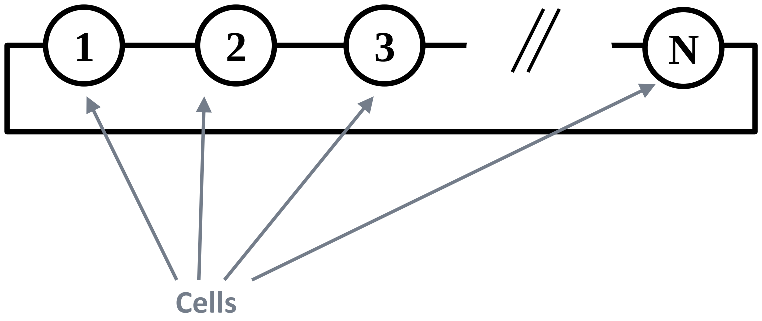


- Depending on the code, cells values can:

Oscillate	Converge	Look random
000000000	100000000	100111000
111111111	111111111	111001101
000000000	111111111	001110100
111111111	111111111	010010110
000000000	111111111	111110011
111111111	111111111	000011100
000000000	111111111	000100110
111111111	111111111	001111011
000000000	111111111	110001001
111111111	111111111	011011110
000000000	111111111	101000011
111111111	111111111	101100100
000000000	111111111	100111111
111111111	111111111	111000000
000000000	111111111	001100001
111111111	111111111	110110011

t	Left	1	1	1	1	0	0	0	0
	Central	1	1	0	0	1	1	0	0
	Right	1	0	1	0	1	0	1	0
t+1	Central	Wolfram code							

Cellular Automaton Ring



- Cells can be looped as a ring
- Depending on the code, the cells values can:
  - Oscillate, Converge or Look random
- This is a Muller gate for a STR based TRNG.
- Stochastic models published and presented at CHES 2013[1]
- Studied in at least [2],[3],[4] and [5]

Which cell is 232 ?

t	Left	1	1	1	1	0	0	0	0
	Central	1	1	0	0	1	1	0	0
	Right	1	0	1	0	1	0	1	0
t+1	Central	1	1	0	1	0	1	0	0

[1] Cherkaoui, A., Fischer, V., Fesquet, L., Aubert, A. (2013). A Very High Speed True Random Number Generator with Entropy Assessment. In: Bertoni, G., Coron, JS. (eds) Cryptographic Hardware and Embedded Systems - CHES 2013.
[2] A. Cherkaoui, Laurent Fesquet, V. Fischer, A. Aubert. Self-Timed Rings as Entropy Sources. 18th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC)
[3] G. Gimenez, A. Cherkaoui and L. Fesquet, "A Self-Timed Ring based PUF," 2020 26th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC)
[4} G. Gimenez, A. Cherkaoui, R. Frisch and L. Fesquet, "Self-timed Ring based True Random Number Generator: Threat model and countermeasures," 2017 IEEE 2nd International Verification and Security Workshop (IVSW).
[5] A. Cherkaoui, V. Fischer, A. Aubert and L. Fesquet, "A Self-Timed Ring Based True Random Number Generator," 2013 IEEE 19th International Symposium on Asynchronous Circuits and Systems, Santa Monica, CA, USA, 2013, pp. 99-106

Mushroom hunting is open

- Several ways to digitize a ring exists.
  - 1 cell sampled
  - XOR of all Cells
  - XOR Decimation
  - ….
- Few of the 256 Cellular Automaton rings have been studied as noise source.
- Is the Graal still already in the literature ?

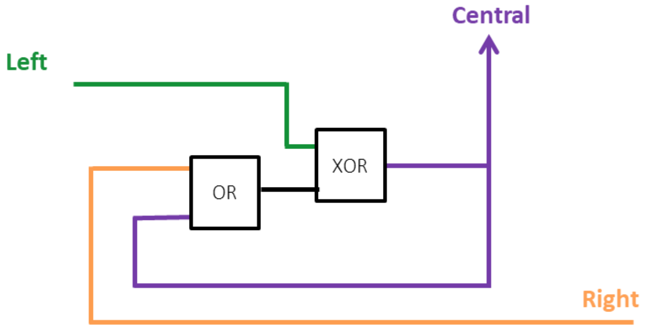
The Cellular Automaton 30 **based TRNG**

Cellular Automaton 30 used for TRNG

- TRNG proposed in 2019 [6] is driven by a cellular automata (CA) topology analysis.
- The random likeness has been validated thanks to SP800-22, SP800-90B & AIS31 black box tests.
- Up to 1.6Gb/sec for a 40nm ASIC implementation.
- Stochastic analysis proposed in next slides.

t	Left	1	1	1	1	0	0	0	0
	Central	1	1	0	0	1	1	0	0
	Right	1	0	1	0	1	0	1	0
t+1	Central	0	0	0	1	1	1	1	0

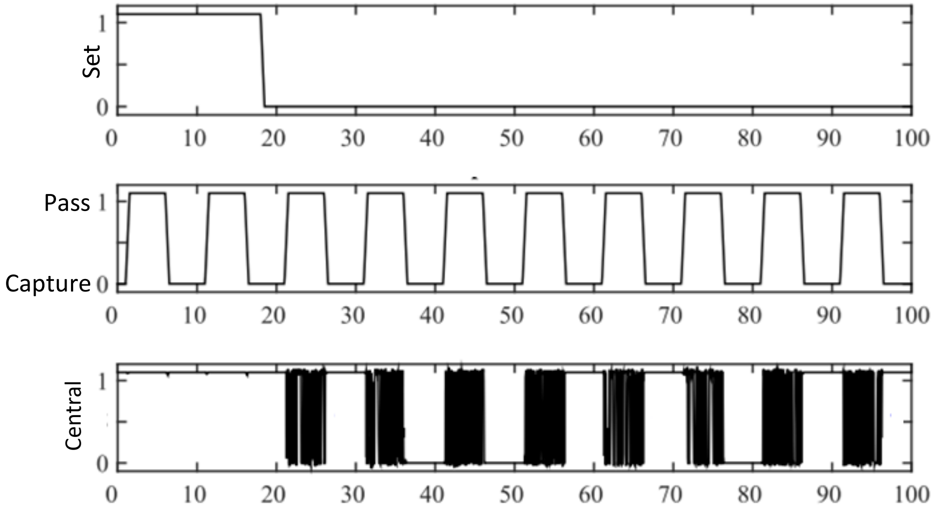
Truth table of cell 30

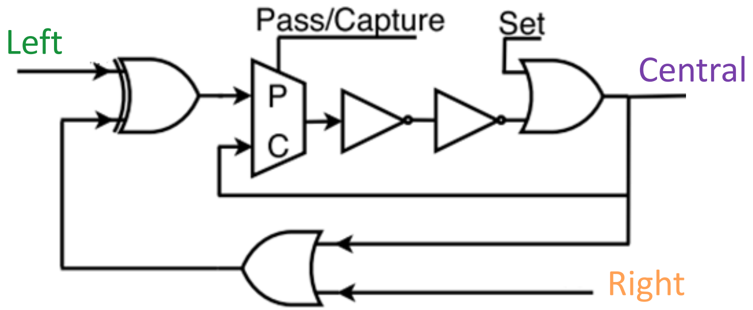


[6] S. Best and X. Xu, "An All-Digital True Random Number Generator Based on Chaotic Cellular Automata Topology," 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)

Cellular Automaton 30 used for TRNG

- Not freely running ring
  - As in Transient Effect Ring Oscillator based RNG
    - Proposed in 2010[7] and modeled in 2015 [8].

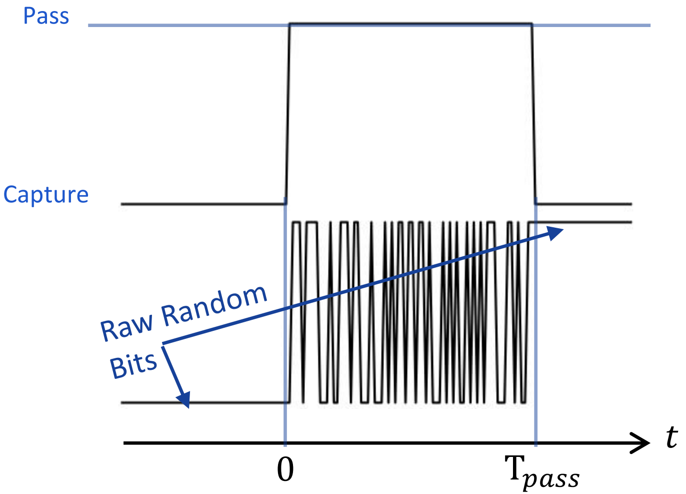




- Consumes only 53 LUTs and 22 DFFs when implemented in FPGA.
- **Raw random number is composed by current bits when capturing.**
- Longer pass time results in better statistical quality.

[7] Varchola, M., Drutarovsky, M. (2010). New High Entropy Element for FPGA Based True Random Number Generators. In: Mangard, S., Standaert, FX. (eds) Cryptographic Hardware and Embedded Systems, CHES 2010.
[8] Haddad, P., Fischer, V., Bernard, F., Nicolai, J. (2015). A Physical Approach for Stochastic Modeling of TERO-Based TRNG. In: Güneysu, T., Handschuh, H. (eds) Cryptographic Hardware and Embedded Systems, CHES 2015.

Cellular Automaton 30 used for TRNG



- Let us call :
  - $X(t)$ a W-bits word composed by states at instant t
    - X is a time indexed stochastic process.
  - $x_1\ (t)$ and $x_2\ (t)$ two realizations of X.
- Knowing the TRNG behavior:
  - When $t \leq 0$ the cell value is captured,
  - When $0 < t < T_{pass}$ the mux is pass
  - When $T_{pass} \leq t$ the cell value is captured again,
- We know that Lyapunov exponent > 0 when ring is noiseless. **What does that mean ?**
  - If $x_1\ (0)$ and $x_2\ (0)$ are close, for t large enough,
  - $x_1\ (t)$ and $x_2\ (t)$ may diverge from each others.
  - $Pr\{X\ (T_{pass}) = a | X\ (0) = b\} = \begin{cases} 1, & a = f_{T_{pass}}(b) \\ 0, & a \neq f_{T_{pass}}(b) \end{cases}$ with $f_{T_{pass}}(b)$: the value taken by $X\ (T_{pass})$ if $X(0) = b$

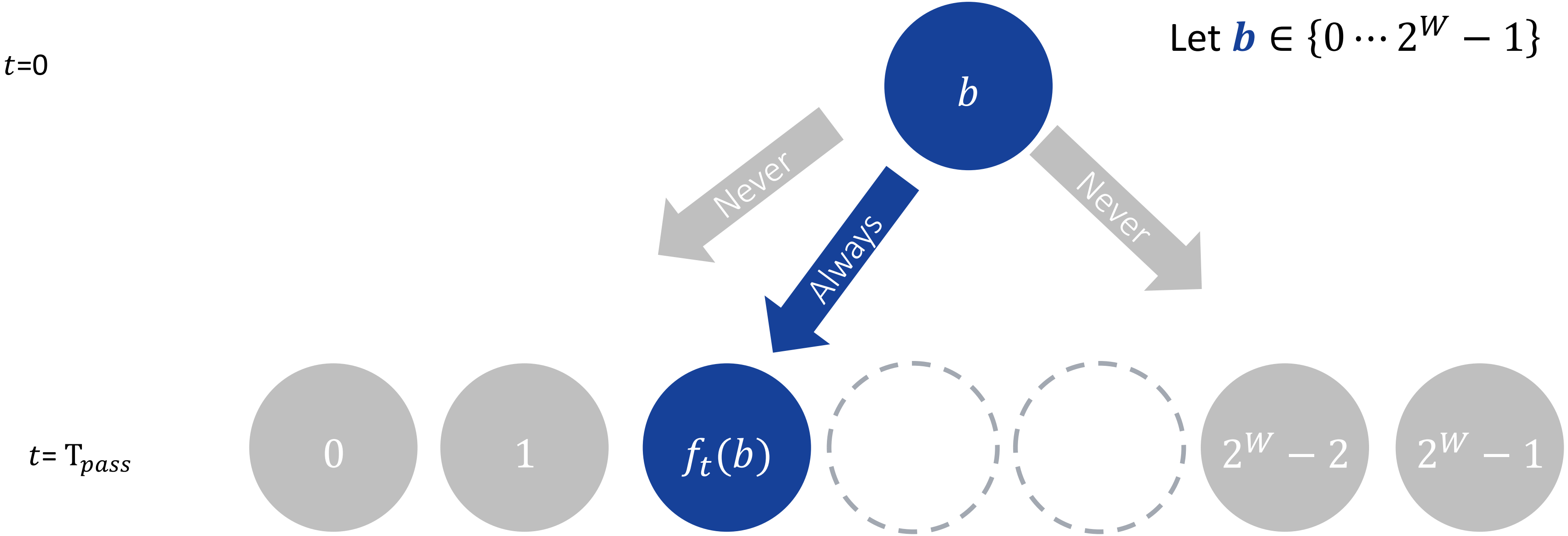
Is it useful for stochastic analysis ?

Yes

Cellular Automaton 30 TRNG stochastic analysis

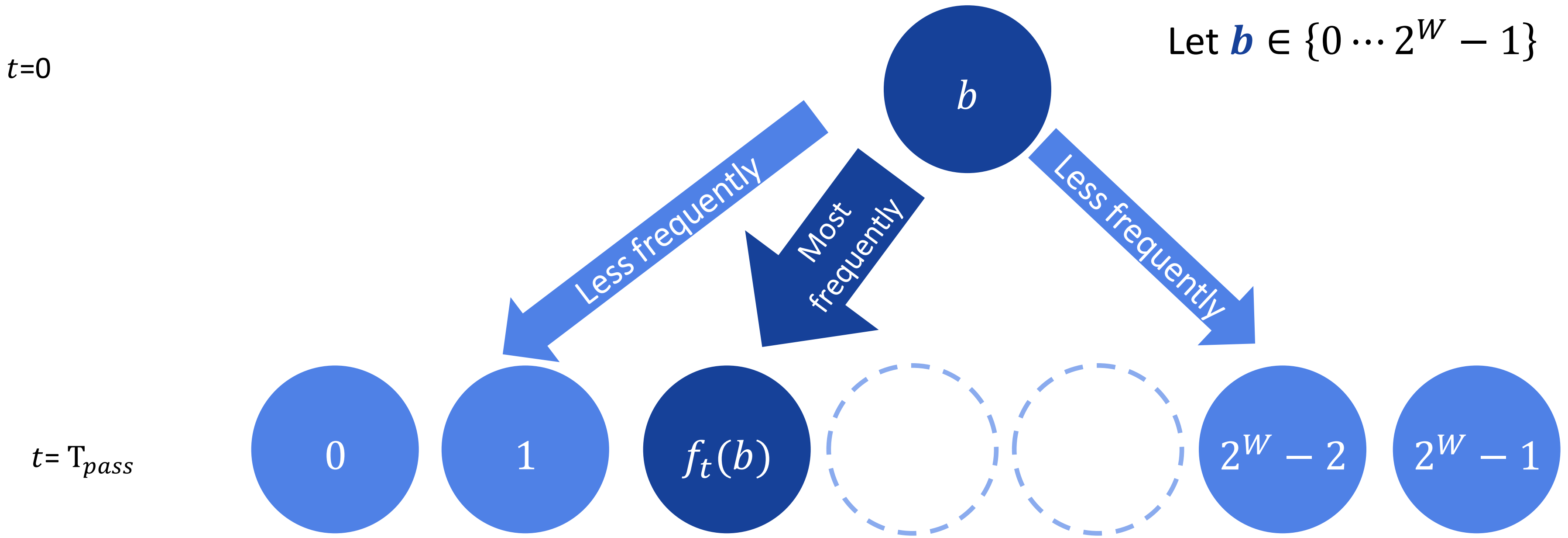
- When the ring is noiseless:

Let $\boldsymbol{b} \in \{0 \cdots 2^W - 1\}$



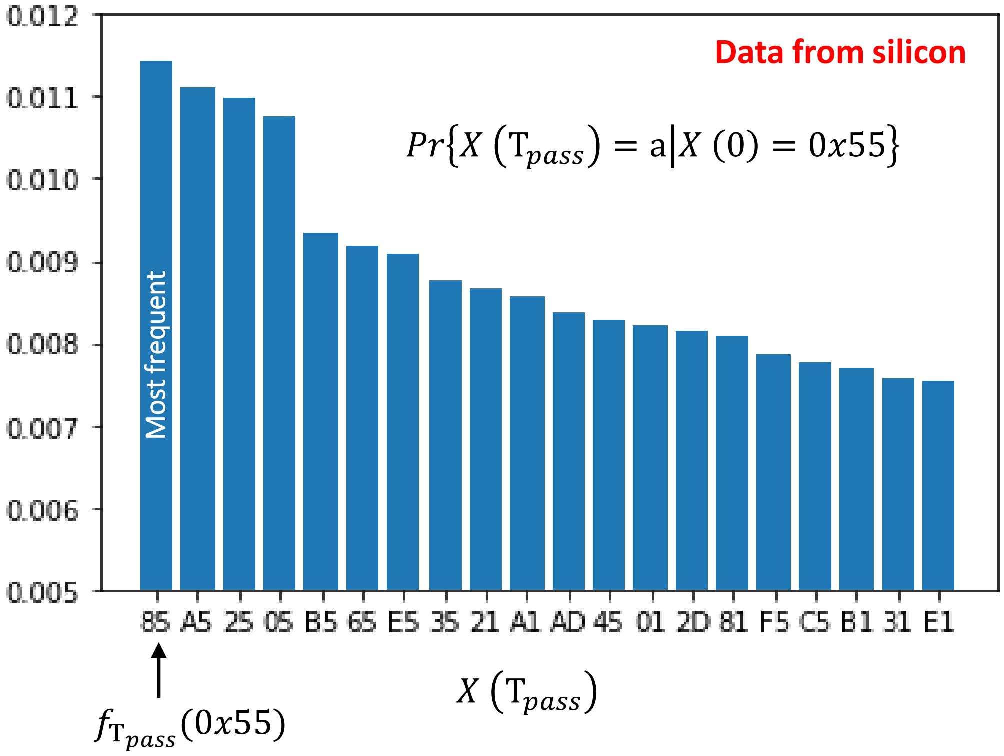
Cellular Automaton 30 TRNG stochastic analysis

- When the ring is noisy:



Cellular Automaton 30 TRNG stochastic analysis

- When the ring is noisy:



Cellular Automaton 30 TRNG stochastic analysis

- Let define H_L a lower bound of the Shannon entropy of the generator such as

$$H_L = H\{X\left(\mathrm{T}_{pass}\right)|X\left(0\right)\}$$

$$H_L = -1 \cdot \sum_{b=0}^{b=2^W-1} Pr\{X\left(0\right) = b\} \cdot \sum_{a=0}^{a=2^W-1} Pr\{X\left(\mathrm{T}_{pass}\right) = a|X\left(0\right) = b\} \cdot \log_2\left(Pr\{X\left(\mathrm{T}_{pass}\right) = a|X\left(0\right) = b\}\right)$$

- When the ring is noiseless: $H_L = 0$
  - As $Pr\{X\left(\mathrm{T}_{pass}\right) = \mathrm{a}|X\left(0\right) = b\} = \begin{cases} 1, & a = f_{\mathrm{T}_{pass}}(b) \\ 0, & a \neq f_{\mathrm{T}_{pass}}(b) \end{cases}$, $H_L = -1 \cdot \sum_{b=0}^{b=2^W-1} Pr\{X\left(0\right) = b\} \cdot \sum_{a=0}^{a=2^W-1} 0$

- When the ring is noisy $H_L > 0$.
  - 7.0726(40nm ASIC) and 7.86924 (Virtex6) [9]

[9] Y. Luo, W. Wang, S. Best, Y. Wang and X. Xu, "A High-Performance and Secure TRNG Based on Chaotic Cellular Automata Topology," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 67, no. 12, pp. 4970-4983, Dec. 2020

A last slide before ending

The last slide as a recap

- Industry’s Most Comprehensive Security IP Portfolio.
- This presentation focuses on our RNGs family

- We reminded some lectures on Cellular Automaton
  - Open doors for new Ring based TRNG principles

- The Cellular Automaton 30 is one of them
  - Its randomness has been stochastically analyzed
  - An entropy lower bound has been presented.

Thank You

www.rambus.com/security