SRA
System Research
and Applications

life.augmented

Random Number Generators in an Industrial Context

Patrick HADDAD – Ugo MUREDDU

Security Design Architect

System Research & Applications

STMicroelectronics

28/06/2023

We are creators and makers of technology

One of the world’s largest semiconductor companies

Over **50,000** employees of which **9,000+** in R&D

$16.1 billion revenues in 2022

Over **80** sales & marketing offices serving over **200,000** customers across the globe

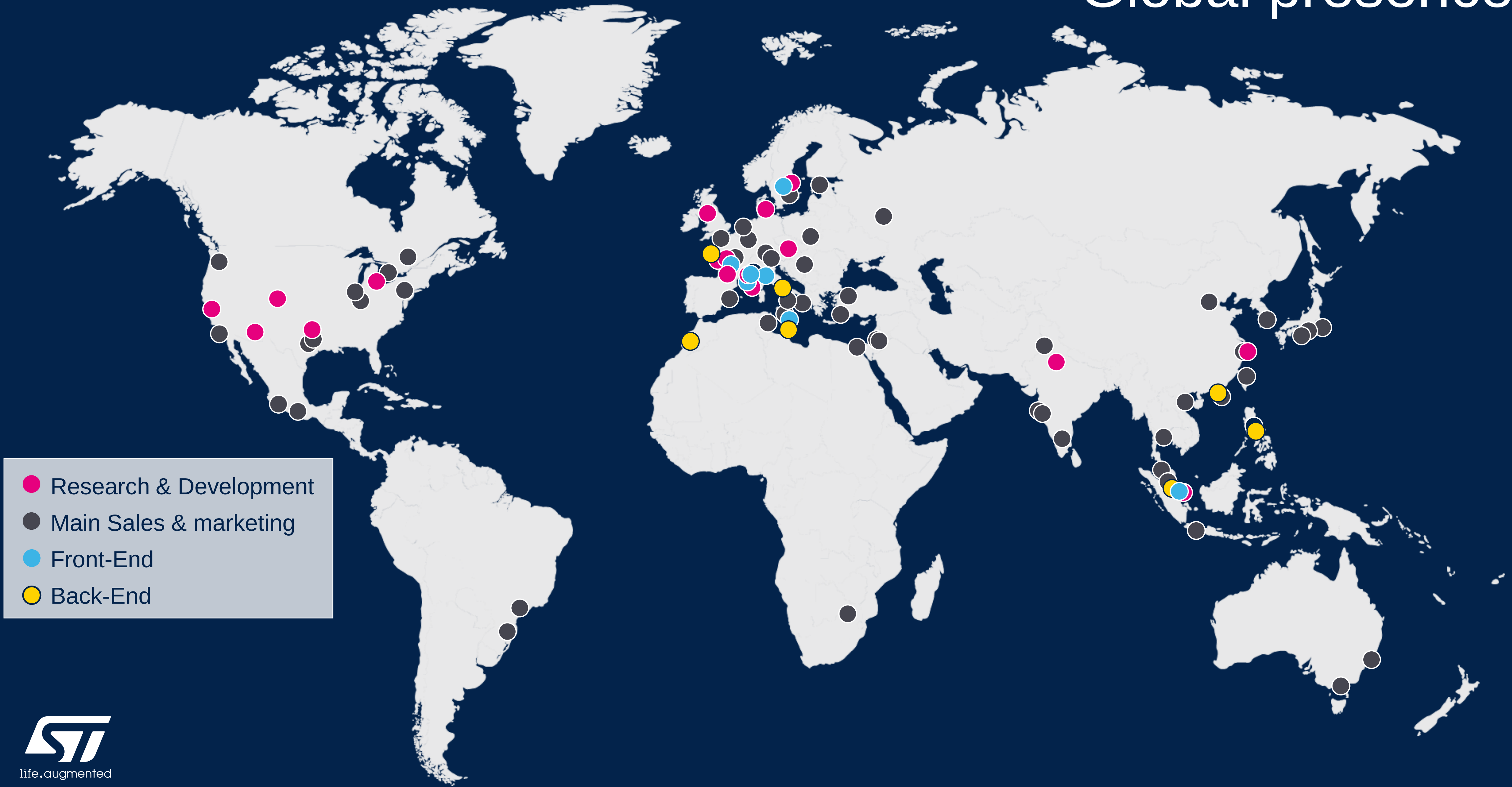
14 main manufacturing sites

Signatory of the United Nations Global Compact (UNGC)
Member of the Responsible Business Alliance (RBA)

life.augmented

As of December 31, 2022

Global presence



life.augmented

SRA security summary

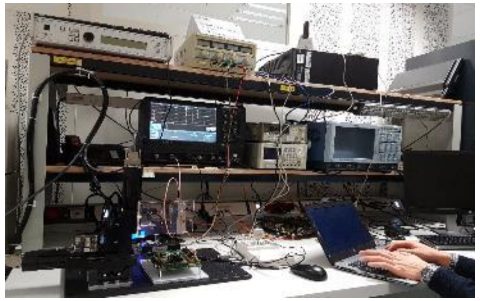
System security, building blocks & SoC-level security

System security
→ understand & anticipate system / applicative needs: IoT, AI, and smart mobility

Providing **security IPs** & expertise to product divisions throughout ST

State-of-the-art lab to perform side-channel and fault-injection attacks

Symmetric crypto	Asymmetric crypto
Random generation	Security subsystem



- General-purpose MCUs (STM32)
- Connectivity products (BlueNRG)
- Imaging sensors (FlightSense)
- Wireless chargers (STWLC)
- Automotive ICs (Stellar)

life.augmented

Random Number Generation

life.augmented

Random Generation – definition of terms

- RNG stands for Random Number Generators
  - TRNG: True Random Number Generators
    - Also called entropy source ES
    - Physical: e.g., Oscillators (noise exploitation)
    - Non-Physical: e.g., CPU jitter
    - Unpredictability

  - PRNG: Pseudo Random Number Generators
    - Also called DRBG: Deterministic Random Bit Generator
    - Algorithmic (e.g., AES based)
    - Good statistical properties

```
/* Intializes random number generator */
srand((unsigned) time(&t));

/* Print 5 random numbers from 0 to 49 */
for( i = 0 ; i < n ; i++ ) {
   printf("%d\n", rand() % 50);
}
```

- NIST standards

  - SP800-90 B: ES
  - SP800-90 A: DRBG
  - SP800-90 C: ES + DRBG

- AIS standards

  - AIS 31: TRNG
  - AIS 20: PRNG
  - AIS 20/31: TRNG + PRNG

life.augmented

Unpredictability vs Good statistical properties

Good statistical properties do not necessarily mean ***Unpredictability***
Unpredictability does not necessarily mean ***Good statistical properties***

Good statistical properties are demonstrated by statistical tests (bias, correlation, compression, etc.)
Unpredictability are demonstrated by a stochastic model and quantified by entropy amount

Entropy: measure of disorder, expressed between 0 and 1 (being the best)

Stochastic model: provides a mathematical description of a noise source using random variables.
Aimed at showing where the unpredictability (entropy) comes from

Challenge : A good RNG needs both!

↳ Why ?

life.augmented

Impact of bias on cipher key generation

Assuming a good TRNG in term of randomness but with some bias

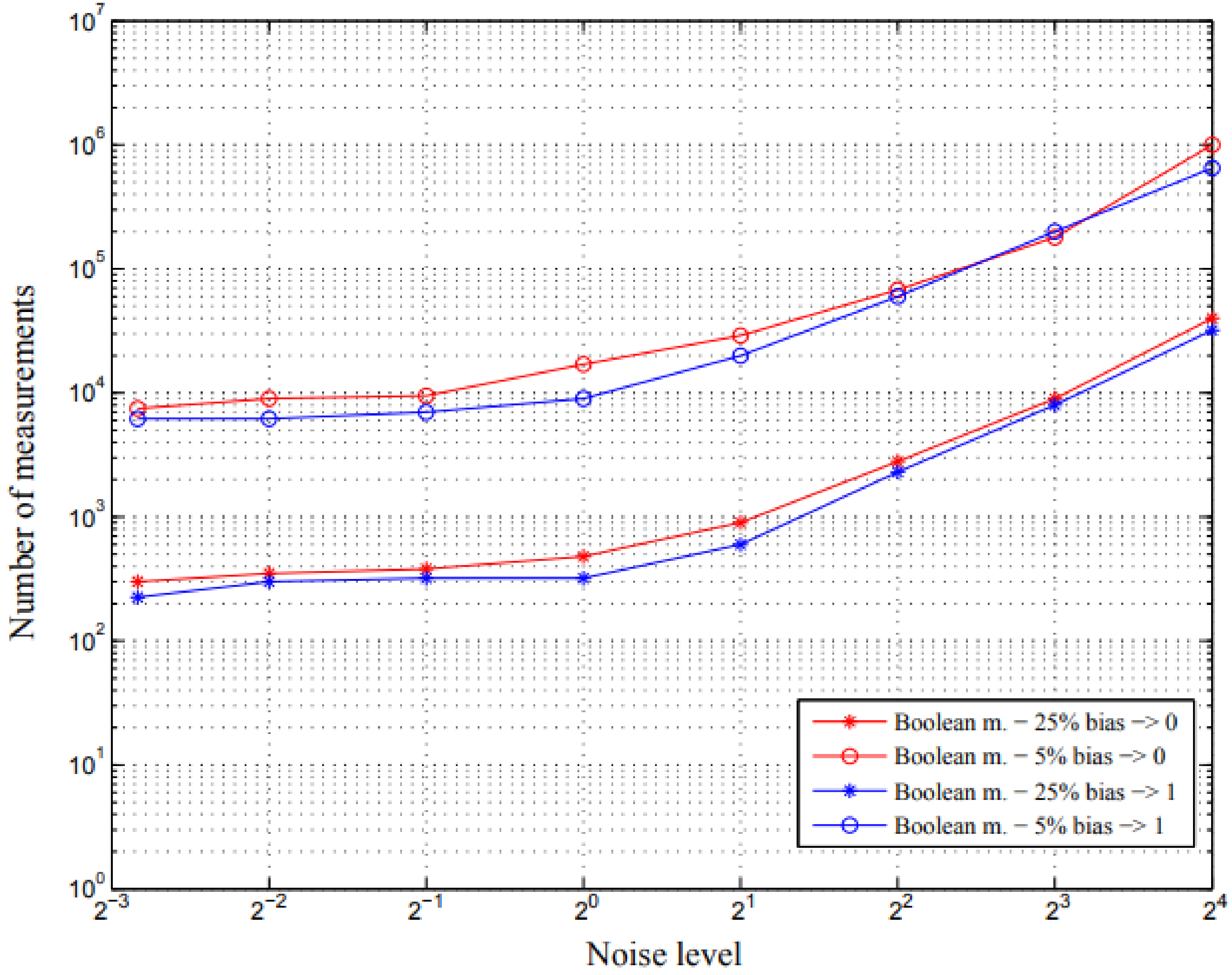
⇨ **ease** a **brute force cryptanalysis**

16 possible keys of 4 bits (0% of bias)		11 possible keys of 4 bits at least 2 bits at ‘1’ (27.2% of bias)		5 possible keys of 4 bits at least 3 bits at ‘1’ (60% of bias)	
0000	1000				
0001	1001		1001		
0010	1010		1010		
0011	1011	0011	1011		1011
0100	1100		1100		
0101	1101	0101	1101		1101
0110	1110	0110	1110		1110
0111	1111	0111	1111	0111	1111

life.augmented

Impact of bias on masking

Univariate CPA attacks against AES Sbox protected by 1st-order Boolean masking scheme

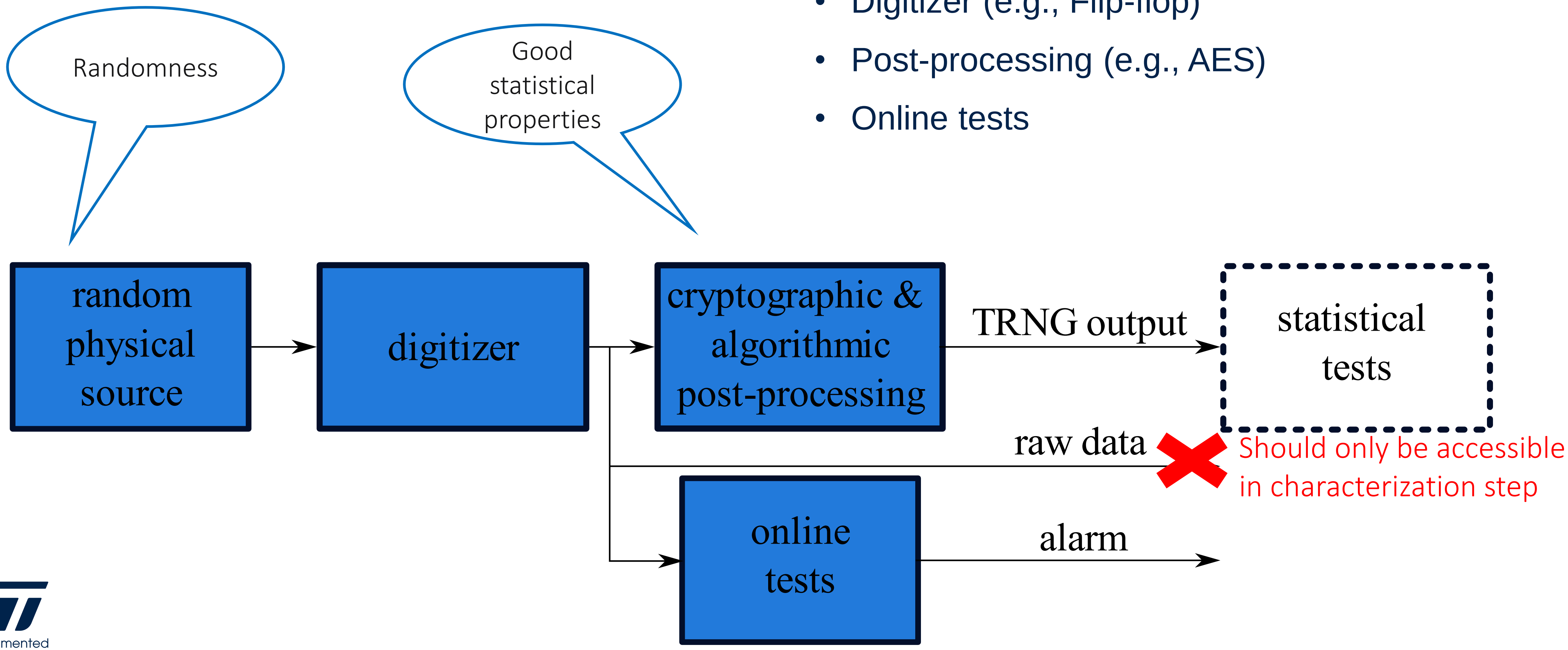


https://www.esat.kuleuven.be/cosic/publications/article-2927.pdf

life.augmented

Commonly approved RNG structure

- Random physical source (e.g., Ring oscillator)
- Digitizer (e.g., Flip-flop)
- Post-processing (e.g., AES)
- Online tests



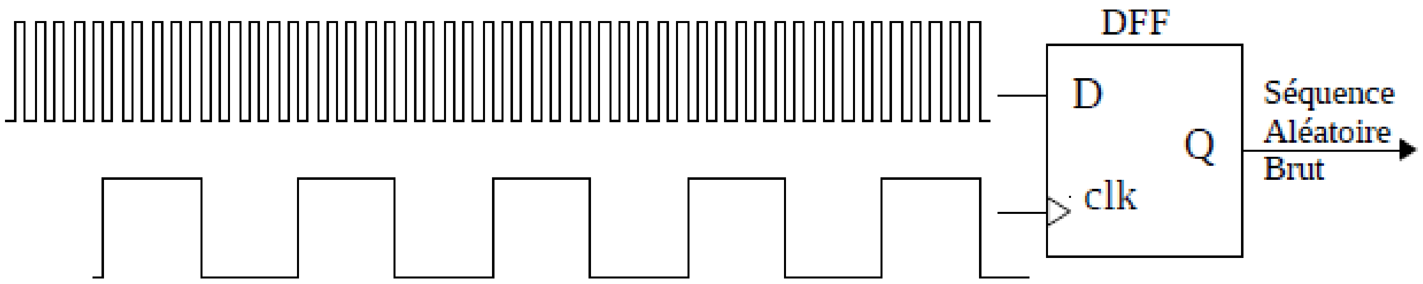
life.augmented

A little bit of history

life.augmented

Last millennium's publications: The pioneers

- Simple digitizers
- Analog flow, simple noise sources
- Security evaluation: black box statistical tests after postprocessing
  - To validate ***Good statistical properties***
- Easy to implement
- Low throughput (order of Kbits/sec)



Digitizer proposed in [1] and [2]

[1] Fairfield, R.C., Mortenson, R.L., Coulthart, K.B. (1985). An LSI Random Number Generator (RNG). In: Blakley, G.R., Chaum, D.
[2] Jun, B., & Kocher, P. (1999). The Intel random number generator.

life.augmented

The golden age: 1st decade of our millennium

- Proliferation of new principles
  - On the shelf noise sources:
    - Inverter based ring oscillators, PLLs, Latch's
  - Simple digitizers
    - Coherent sampling, Asynchronous counter…

- Security evaluation:
  - Black box tests before postprocessing
  - Rational on the noise's origin

- Easy to implement

- Good throughput (order of Mbits/sec)

life.augmented

Age of Reason: 2nd decade of our millennium

- Stochastic model of some of principles of the previous decades
  - PLL based TRNG — $\sim 10^{6}$bits/sec
  - Elementary ROs based TRNG — $\sim 10^{3}$bits/sec
  - Open loop based TRNG — $\sim 10^{6}$bits/sec
  - Latch based TRNG — $\sim 10^{6}$bits/sec

- New principles with corresponding stochastic models
  - Asynchronous oscillators based TRNGs — $\sim 10^{8}$bits/sec
  - Time to digital convertor based TRNG — $\sim 10^{6}$bits/sec

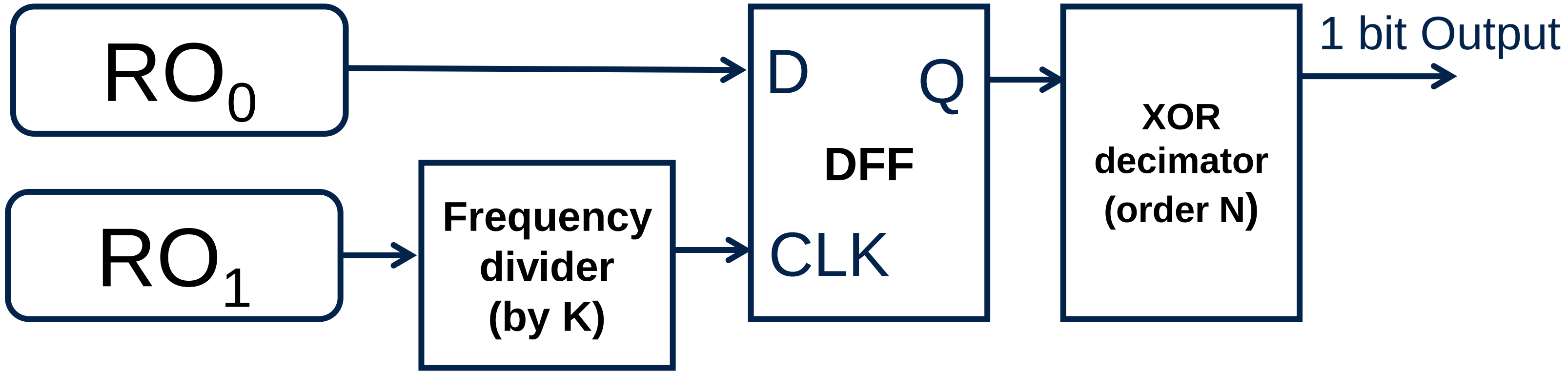
- Security evaluation: model-based entropy estimation
- Hard to implement

Cost
Implementability

life.augmented

Do we really need a fully entropic noise source?

Elementary ROs based TRNG



(K,N)	(1,1)	(2,1)	(3,1)	(4,1)	(5,1)
Entropy Per Output Sample	0.0975	0.1216	0.1397	0.1458	0.1515

(K,N)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
Entropy Per Output Sample	0.0975	0.1913	0.2854	0.3849	0.4805

→ Entropy is better improved by post-processing iterations than raw accumulation

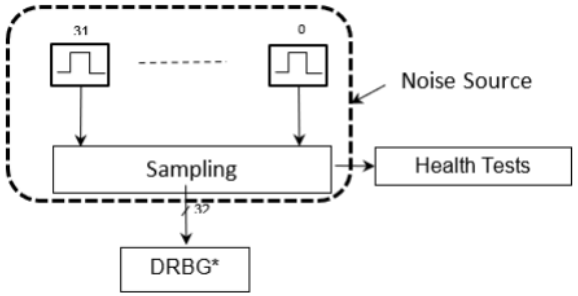
life.augmented

Recently certified RNG

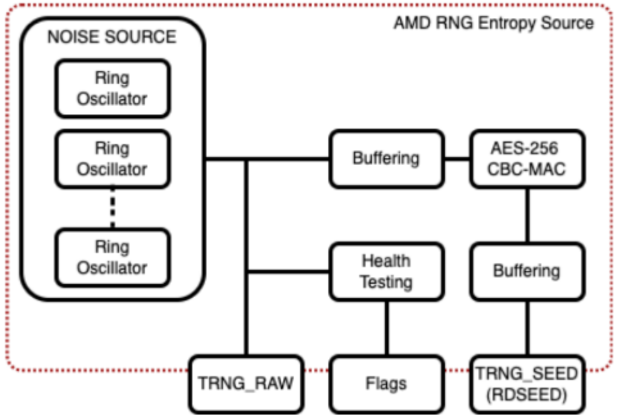
life.augmented

SP800-90B compliant TRNG

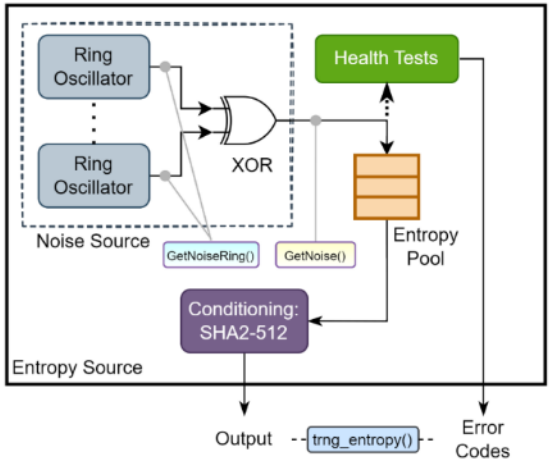
- As of June 8, 2023, 49 standalone entropy sources have been certified
  - 26 classified as “Physical noise source“
    - 18 Ring Oscillators (RO) based, 7 undisclosed and 1 LED + CMOS Sensor based
    - Claimed entropy before conditioning H_{mean}= 0.36



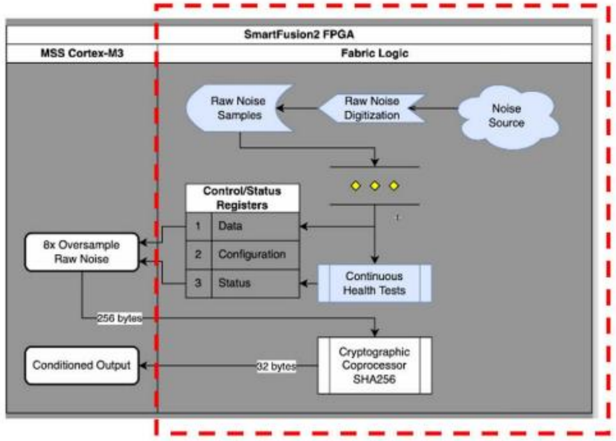
Western Digital



AMD



IBM



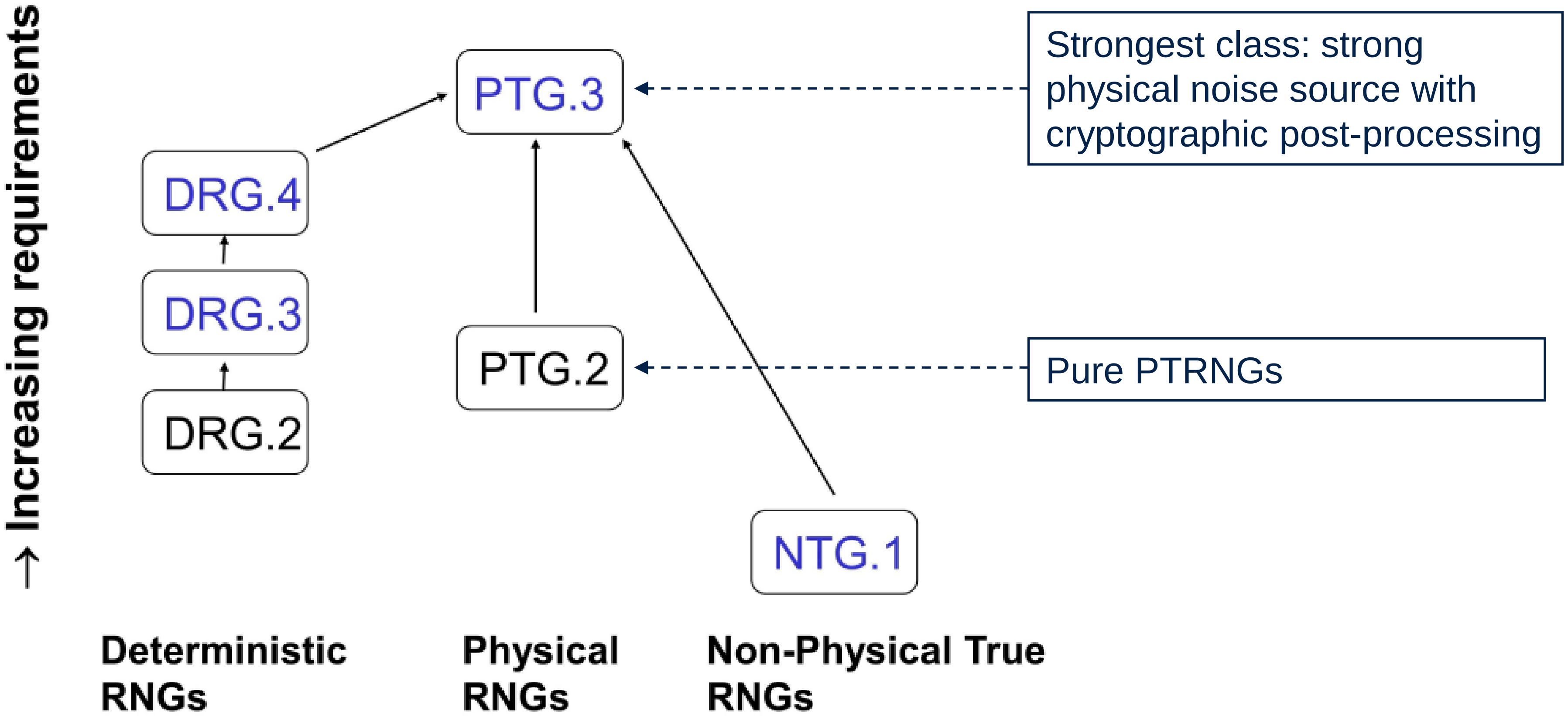
Cisco

life.augmented

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations

AIS 20/31 – Functionality classes

New draft of AIS20/31 from BSI as of June 2023



https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2023.pdf?__blob=publicationFile&v=2

RNG trend

- Standalone TRNG performing in all areas is utopic
  - Always a tradeoff between cost, throughput and good noise extraction

- Trend is to ES/TRNG + DRBG/PRNG => SP800 90C – AIS20/31

  - ES/TRNG:
    - As simple as possible
    - Good randomness extraction
    - Relatively low throughput
    - Statistical properties not ideal (before post-processing)
    - Not intended for ‘direct’ use – Seed for DRBG

  - PRNG/DRBG:
    - Based on cryptographic function
    - Good statistical properties
    - Fast
    - Pseudo-random

life.augmented

RNG requirements

- *Recall* – Two main requirements on RNGs:
  - Output unpredictability: random source
  - Good statistical properties of the output bitstream: post-processing

- Additional requirements for industrial purposes: **robustness**
  - Stability and repeatability over process, voltage and temperature variations

Being able to guarantee a sufficient level of entropy before conditioning : stochastic model

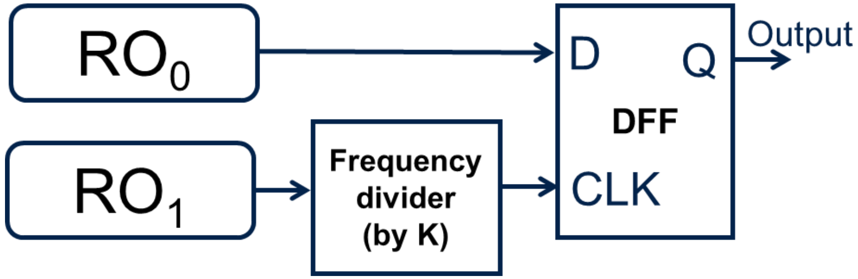
AND

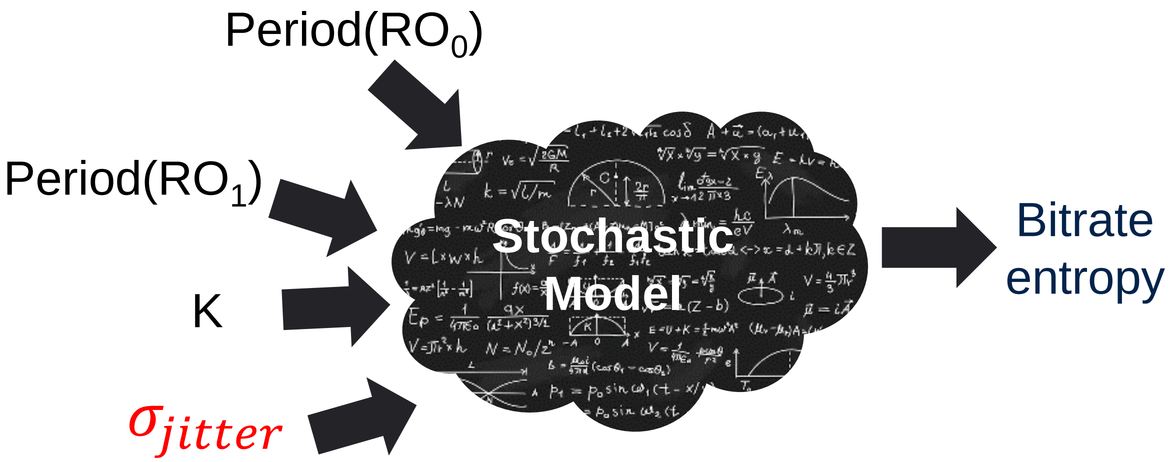
Detect any loss below this level : online tests

Stochastic Model

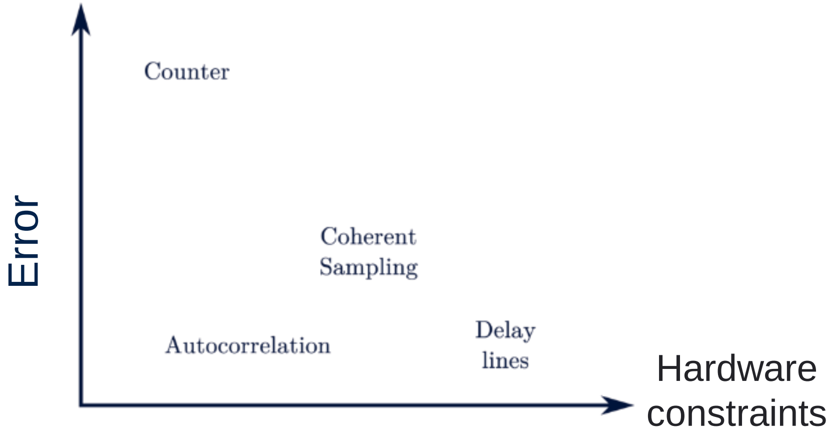
Stochastic model & jitter measurement

Elementary ROs based TRNG





- σ_{jitter} is the key parameter
  - Precise measurement of σ_{jitter} is a challenging task
  - A low constraints & accurate method is still a graal
    - A.Garay, F. Bernard, V. Fischer, P. Haddad, and U. Mureddu.
      An Evaluation Procedure for Comparing Clock Jitter Measurement Methods.
      CARDIS 2022



Online tests

life.augmented

Online tests – What standards say about it

AIS31:

- *“An online test / health test shall :*
  - *Detect non-tolerable entropy defects sufficiently soon,*
  - *Be tailored to the stochastic model,*
  - *Use the raw random numbers, because they contain more information than the internal random numbers. “*

https://csrc.nist.gov/csrc/media/Presentations/2023/use-of-stochastic-models-in-rbg-standards-challeng/images-media/session-3-mittman-use-of-stochastic-models.pdf

SP800-90B

- *“Intended to ensure that the entropy source continue to operate as expected.*
- *Goal is to obtain assurance that failures of the entropy source are caught quickly and with a high probability.“*

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

Online tests – What standards say about it

SP800-90B: two approved online tests

- Repetition Count Test (RCT)
  - Designed to detect total failure (e.g., noise source stuck)
  - Counts identical values generated consecutively
  - If above a cutoff value => triggers an alarm

- Adaptive Proportion Test (APT)
  - Designed to detect large loss of entropy (e.g., strong bias)
  - Counts number of times the same value occurs within 1024 samples (for binary source)
  - If above a cutoff value => triggers an alarm

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

Online tests – What standards say about it

SP800-90B: two approved online tests

- Need to consider false positive vs false negative rates

- False alarm: (false positive)
  - Entropy source operating correctly
  - Alarm raised

- Silent failure: (false negative)
  - Entropy source producing less entropy than claimed
  - No alarm raised

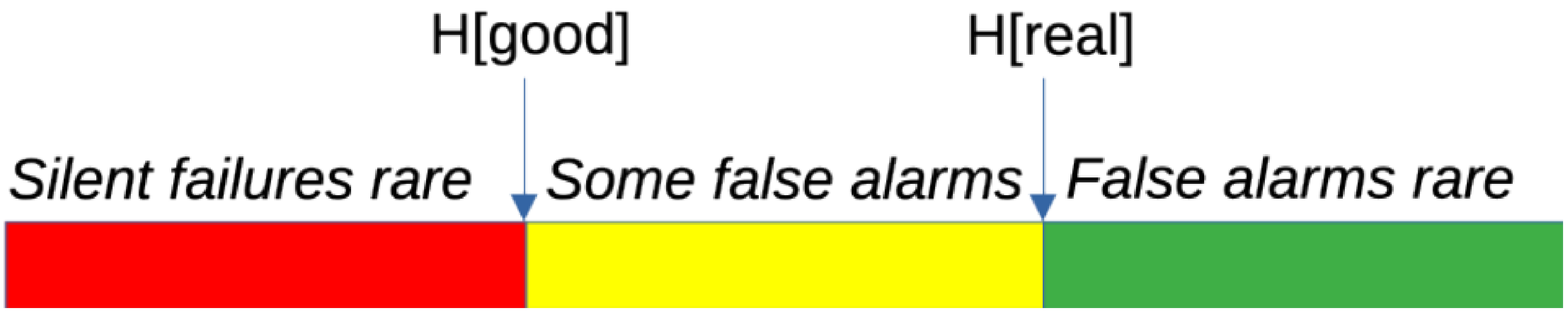
- How to determine cutoff values ?

life.augmented

https://csrc.nist.gov/csrc/media/Presentations/2023/health-tests-for-90b/images-media/session-4-kelsey-health-tests-90B.pdf

NIST 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]



https://csrc.nist.gov/csrc/media/Presentations/2023/health-tests-for-90b/images-media/session-4-kelsey-health-tests-90B.pdf

life.augmented

Choosing test parameters

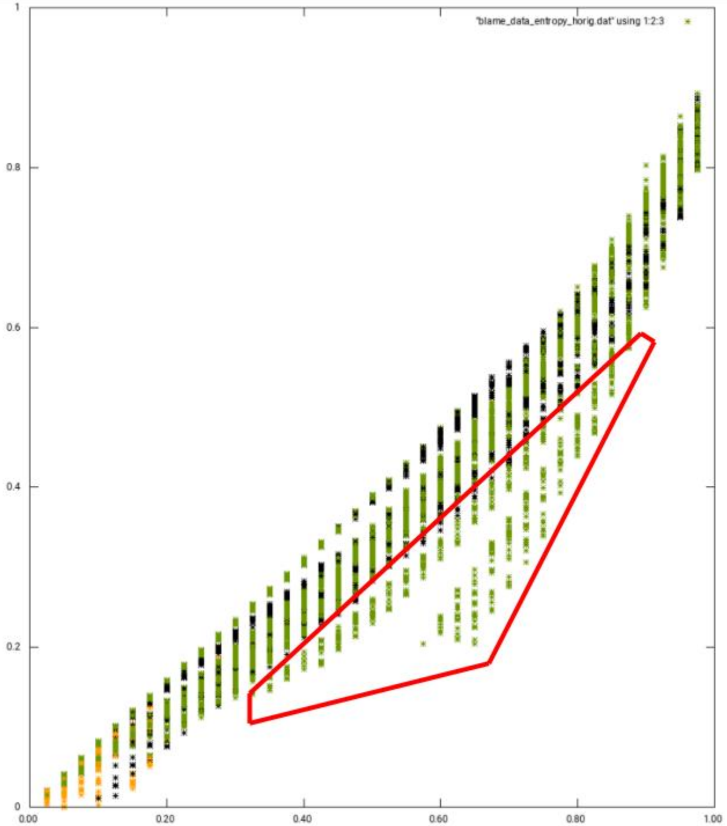
Study from David (DJ) Johnston - Intel Corporation:

- 7800 samples of entropy data inputted to SP800-90B statistical test suite
- Entropy levels from 0.025 to 0.975 in 0.025 increments
- Actual entropy, Bias and H_original, along with estimation error and test with the lowest estimate recorded for each data point
- 200 runs per entropy level
- 39 entropy levels
- `ea_non_iid -i -v -t -l 0,1000000 1` was used

https://csrc.nist.gov/csrc/media/Presentations/2023/vendor-chts/images-media/session-3-johnston-vendor-chts.pdf

Choosing test parameters

Entropy systematically underestimated



Over all 7800 tests	
Average Err	-0.15339
largest Err	-0.44592
Smallest Err	-0.00334
median Err	-0.15689

Over tests where tCompression gave the lowest estimate	
tCompression total	-911.636
tCompression count	6026
tCompression Av err	-0.15128
smallest tC err	-0.00352
largest tC Err	-0.44592

Over tests where any other test gave the lowest estimate	
not tCompression total	-238.804
not tCompression count	1774
not Tc Av Err	-0.13461
smallest not Tc Err	-0.00334
largest not Tc Err	-0.27637

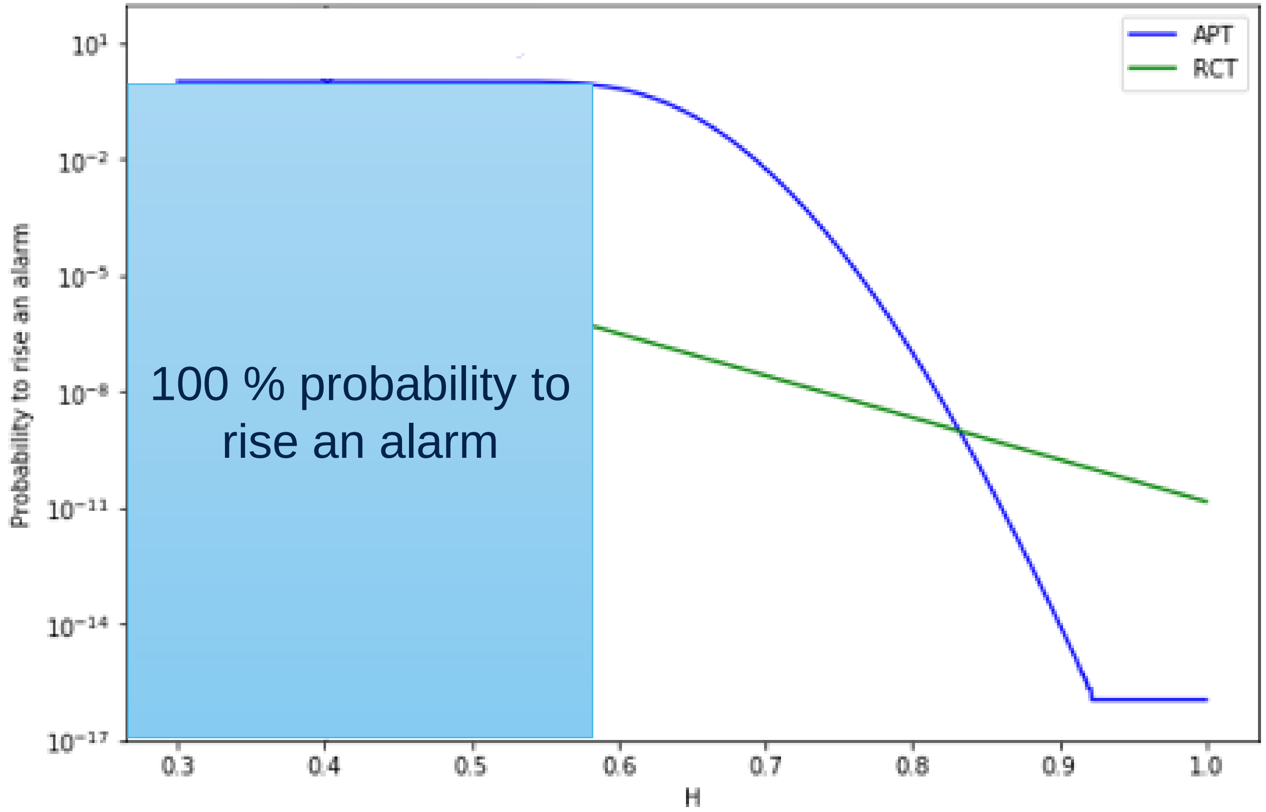
=> SP800-90B min-entropy estimation is already H[good]

life.augmented

Online tests alarm probability

Cut-off values determined with $H_{min} = 0.8$

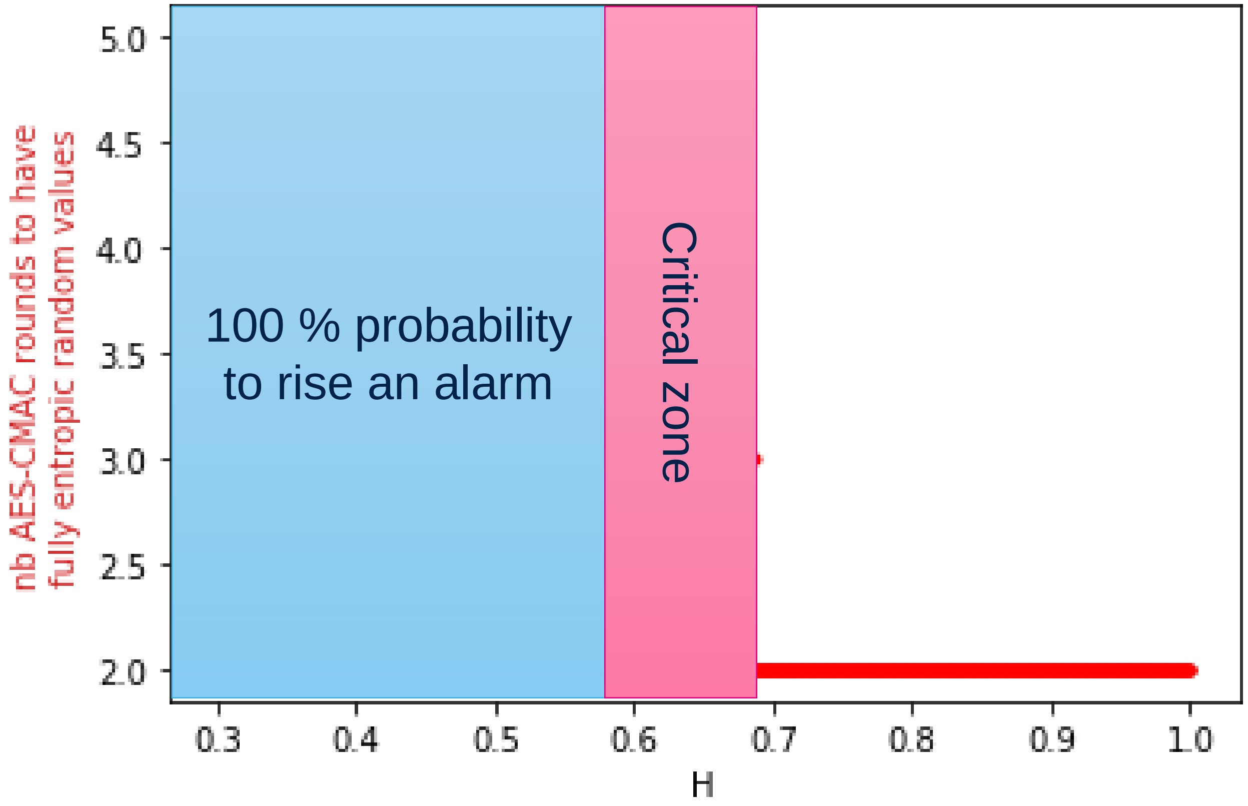
- C = 37 for the RCT
- C = 669 for the APT



life.augmented

Post-processing

Number of AES-CMAC post-processing compression rounds to get full entropy output



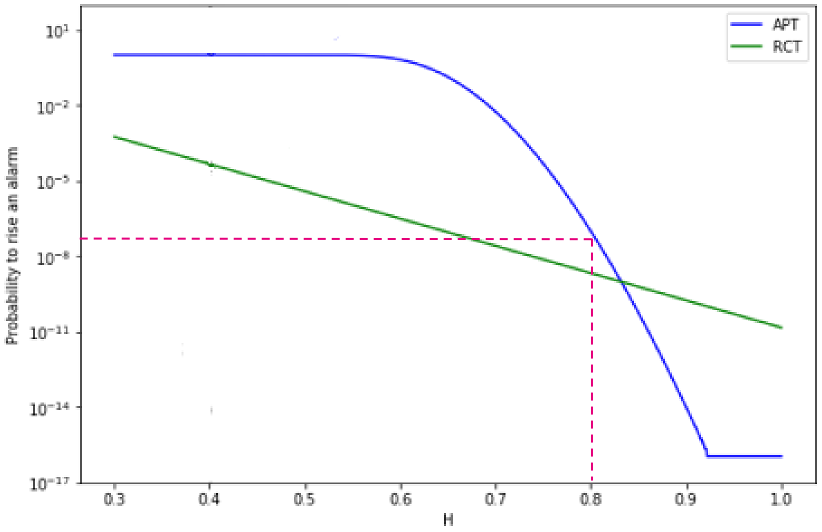
=> 3 rounds of post-processing

life.augmented

Online tests & post-processing

Secure: Either we obtain full entropy output with post-processing or we trigger an alarm with 100% probability

Efficient: If we consider min-entropy of at least 0.8 in normal working conditions, probability of a false alarm is very low (≈ 0.00001% probability)



Conclusion

life.augmented

Conclusion

- A good RNG needs unpredictability and good statistical properties

- Companies, academics and standards are merging to a consensus:
  - Simple and reliable entropy source with stochastic model to seed PRNG
  - Cryptographic post-processing to accumulate entropy
  - Accurate online tests to quickly detect failures
  - Fast algorithmic & cryptographic PRNG

- There still remains a lot of room for improvement

Our technology starts with You

Find out more at www.st.com/careers

life.augmented