True Random number generators:
the point of view of a semiconductor company

Patrick Haddad

System Research and Application: Security Team

With the helpful support of B. Kasser, J. Lee, U. Mureddu, M. Lacruche, A. Martinez, M. Agoyan, S. Chesnais

life.augmented

Agenda

- **Introduction**
  - STMicroelectronics
  - Security in ST products
  - The System Research and Application Security Team
  - Our TRNG activities
- **TRNG in the design / integration flow of a product**
- **Analysis of promising TRNGs proposed in the literature**
  - Study of the manufacturability
  - Study of the voltage supply influence
  - Study of malicious manipulations

Who We are

- A global semiconductor leader
- 2017 revenues of **$8.35B** with year-on-year growth of **19.7%**
- Listed: NYSE, Euronext Paris and Borsa Italiana, Milan

- Research & Development
- Main Sales & Marketing
- Front-End Manufacturing
- Back-End Manufacturing

life.augmented

- Approximately **45,500** employees worldwide
- Approximately **7,400** people working in R&D
- **11** manufacturing sites
- Over **80** sales & marketing offices

As of December 31, 2017

Security Pervasion

Security becoming key for our target end-markets / applications

Internet of Things

Smart Driving

Smart Things

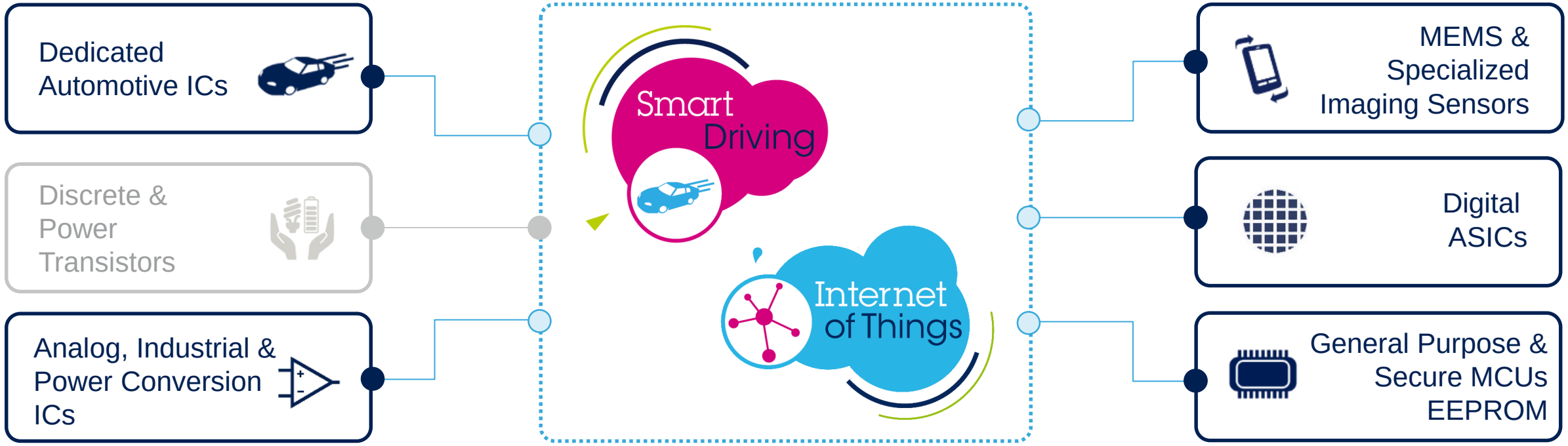
Smart Home & City

Smart Industry

Smart Driving

Security Needs Across ST Products

System security needs to translate into hardware security foundations in ST products



- Except for “discrete”, most of ST product lines are impacted by security
- ST products provide foundations & enablers for designing secure systems

life.augmented

SRA Security Team

- **SRA Missions:**
  - To provide ST with leading edge innovation in security, imaging-video, connectivity, ultra-low power & healthcare ensuring an early IP access to **all ST's divisions**
- **SRA Security team:**
  - **Anticipate** (customers, consortia & standards, ...)
    - Develop or make available (3rd parties, partners, etc.) critical hardware or software security IP blocks, architectures or expertise that will be needed by ST product divisions 3-5 years down the road.
    - Work closely with product divisions to ensure proper awareness and anticipation
  - **Support** ST product divisions & deploy **security expertise** within ST
  - **Help promote ST's product portfolio** to customers when our security expertise can make the difference (reference designs, demonstrators, ...)
  - Identify, prototype & champion/nurture **innovation opportunities** for ST in the field of security
- **The team: 2^4 security engineers & researcher (Rousset + Agrate)**

The Strategy of Our TRNG Activities

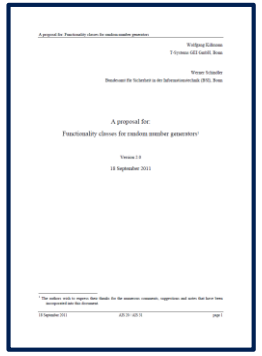
- Address a worldwide market with the same RNG IP
- Provide to our customers (internal/external):
  - Common RNGs for cryptographic application
    - **SP800-90 compliant**
    - **AIS31 compliant**
    - **PCI compliant**
    - **KCMVP**
    - **…**


NIST Special Publication 800-90B

Recommendation for the Entropy Sources Used for Random Bit Generation

COMPUTER SECURITY

NIST


A proposal for:

Functionality classes for random number generators

- **Leveraging the most advanced research activities & funneling them into commercial products, helping improve security of products in the field**
- **In concertation with national / private certification agencies**

life.augmented

Our TRNG Activities

- **Support** ST product divisions for integration in products
  - More details in next slide
- **Support** ST product divisions for certification:
  - Payment Card Industry → classical statistical tests suites
  - Korea Crypto Module Verification Program → classical statistical tests suites
  - Common Criteria → AIS31
  - Federal Information Processing Standard → SP800-X
- **Follow** and **contribute** to evolutions of evaluation methodologies
  - AIS31 V2.0, SP800-90B, …
- **Follow** and **contribute** to worldwide research activities
  - Several publications: CHES, FDTC, DATE, …
- **Anticipate** security features and performances next years needed for ST product.
  - Test structures proposed in recent publications

TRNG in the Design / Integration Flow

TRNG in the Design / Integration Flow

SYSTEM SPECIFICATIONS

Marketing analysis feedback

- Secure firmware
- ECC, AES, RSA
- HO SCA prot.
- HA SCA prot.
- TRNG certif.
- ….

ARCHI. SPECIFICATIONS

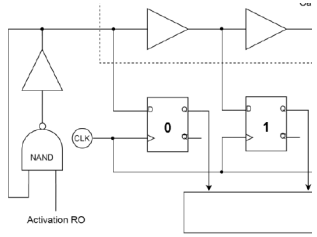
Mapping of unitary blocks

- RAM
- Masked AES
- Robust CPU
- TRNG interface.
- ….

FUNCTIONAL & LOGIC DESIGN

HDL code writing / reuse

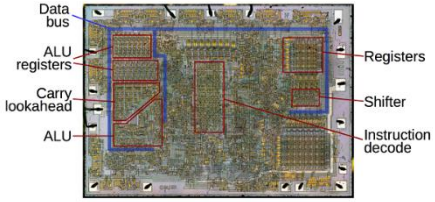
- Mode of Oper.
- Wrappers,
- Boolean masked AES
- TRNG:
  - Online Tests
  - Post Proces.
- ….



CIRCUIT DESIGN

Gate level modif. / tuning

- Avoid glitches
- Ring Oscillators
- Delay chains
- Paths for testing
- ….



PHYSICAL DESIGN

Silicon level modif. / tuning

- Place and route
- ….

MANUFACTURING

Master the TRNG behavior is a key point for an IC manufacturer

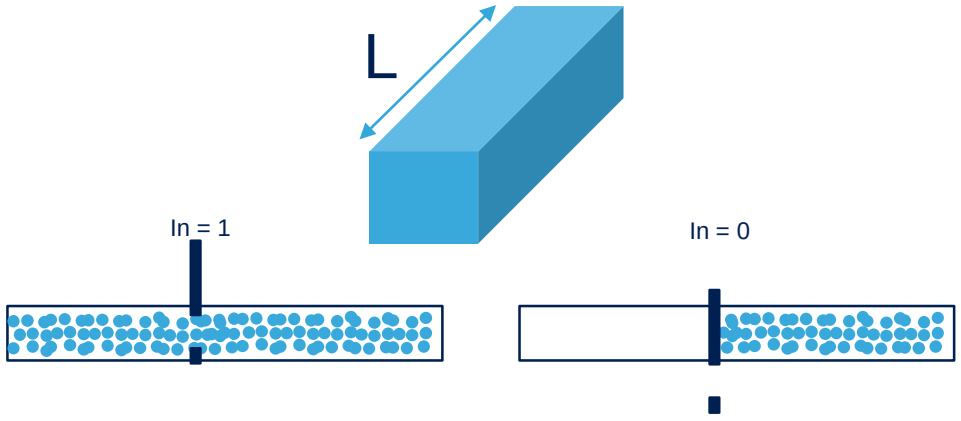
- against variation of manufacturing process
- against variation of power supply
- against variation of temperature
- against malicious environmental modifications
- …

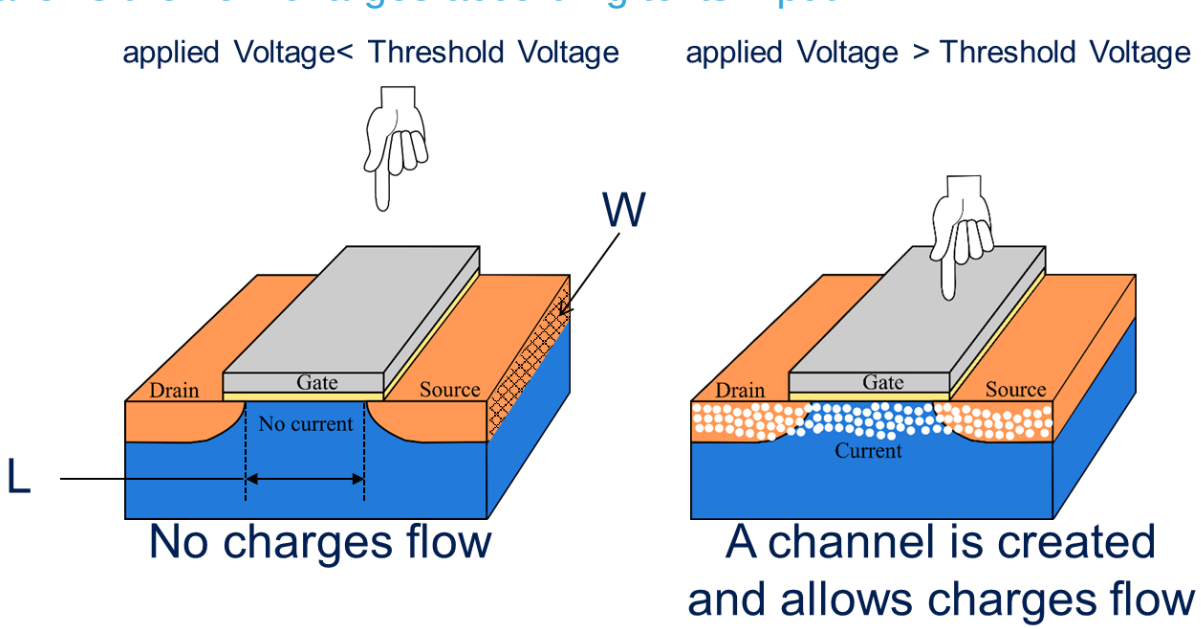
life.augmented

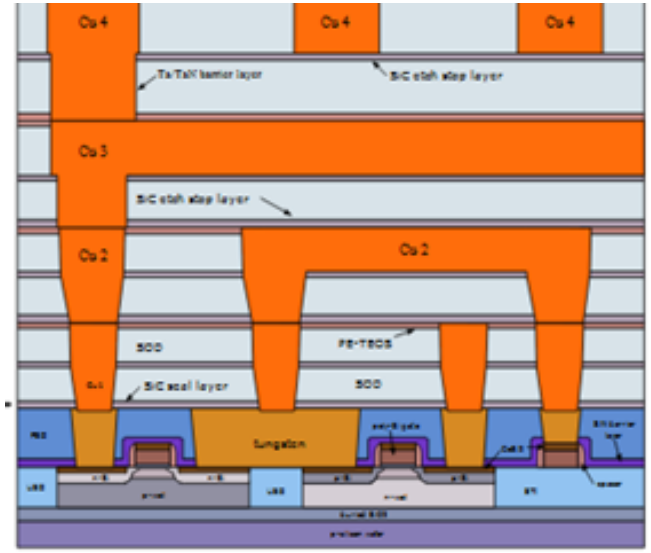
Study of the TRNG Manufacturability

A Transistor

- ICs are composed of gates and memories
  - Inverter, XOR, NAND, Flip-flops …
- Logic gates and memories are composed of transistors
- A transistor is like a valve
  - Allows the flow according to inputs values
- A transistor is a stack of different materials
  - allows the flow charges according to its input



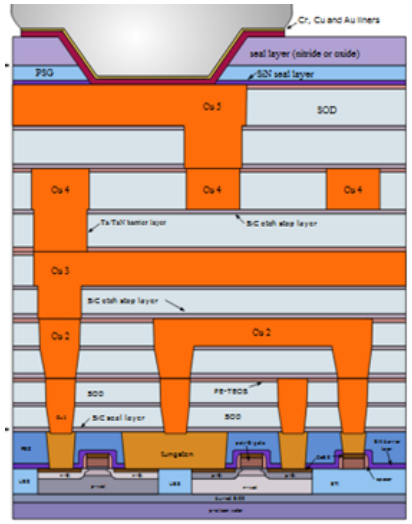


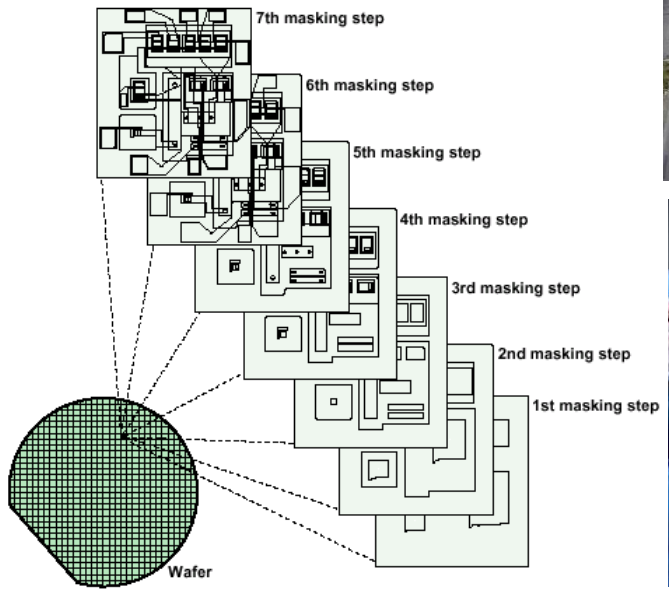


life.augmented

The Manufacturing

- Manufacture an **IC is not a print process**
- Manufacture an IC is
  - A set of **complex** & **precise** «stencil printing»
  - **Expensive** to set up
  - A **long** process (few months for one µC)
    - Fortunately we can manufacture in parallel
- Tailored for mass production
- Not tailored for test chips
  - Fortunately we can design/manufacture some
- **Under quality control**
  - But quality transistors is not cloned transistors



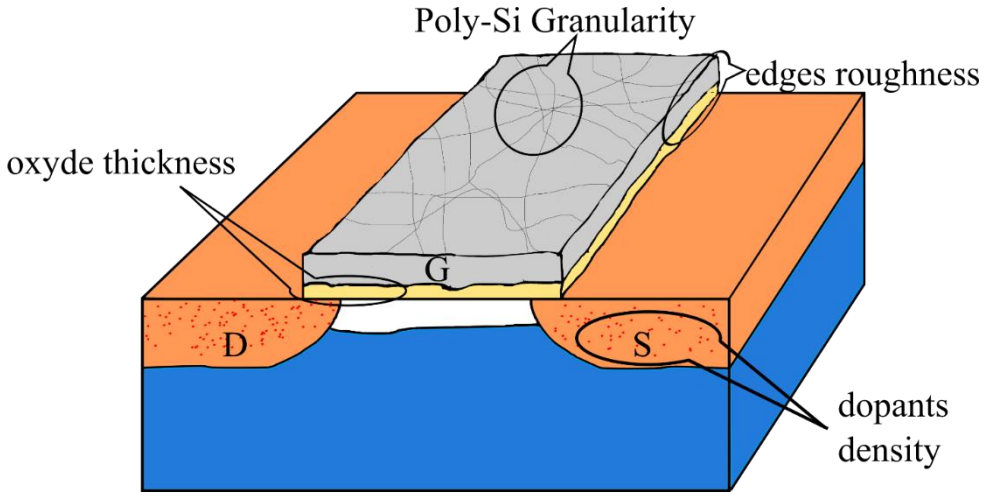


Cost of a set > 2^{21} dollars

life.augmented

The Defaults of a Transistor

- Electrical parameters of the transistor are slightly impacted by:
  - The regularity of the stacks
  - The doping variations of the materials



- Example:

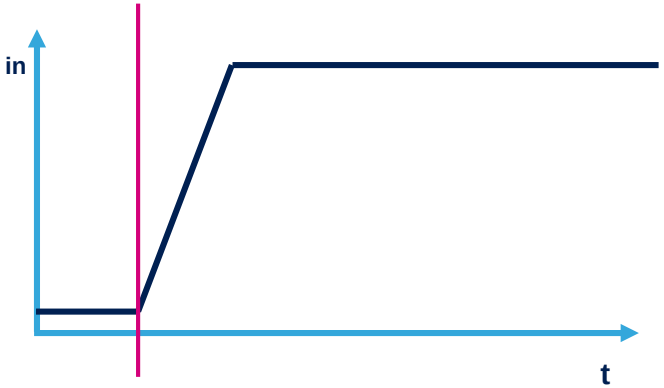
$$I_{DS} = \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot \frac{(V_G - V_{TH})}{2}$$

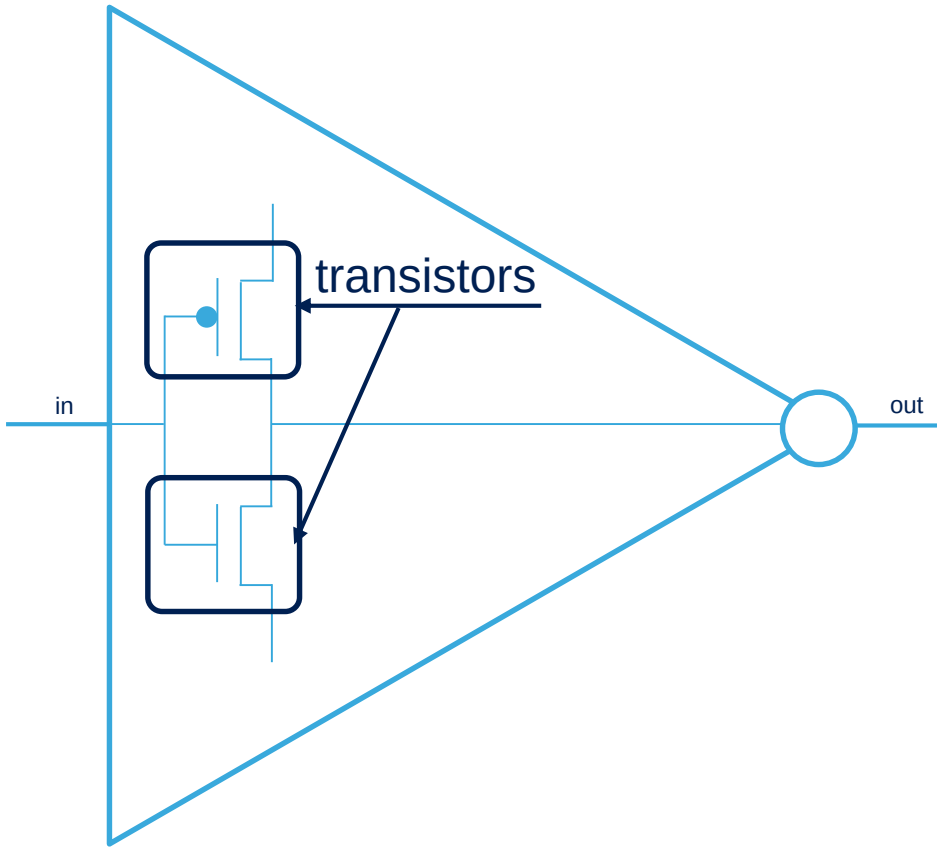
- Fortunately variation of μ, W, L, C_{OX} and V_{TH} are well studied
  - We know theirs laws
  - The laws can be used for simulations

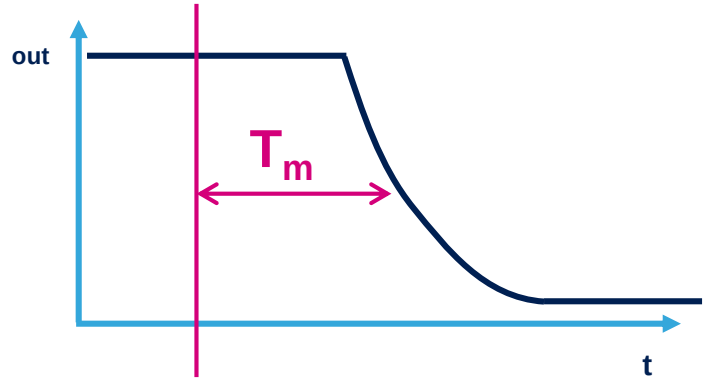
The Defaults at Gate Level

Logic gates and memories are composed of non homogeneous transistors

Ex: the inverter





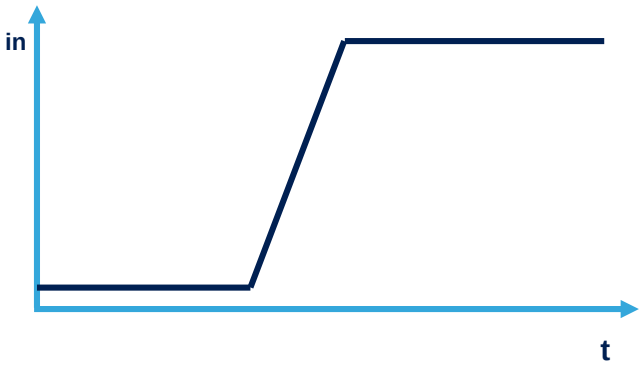


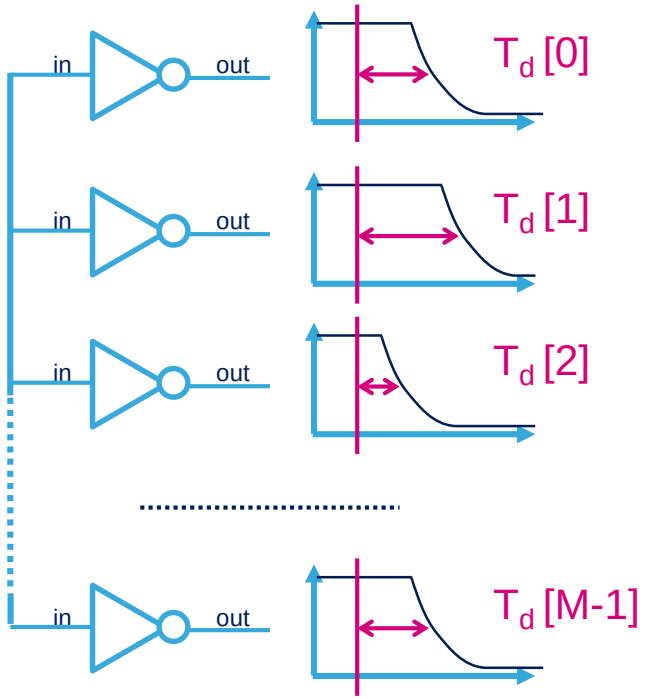
life.augmented

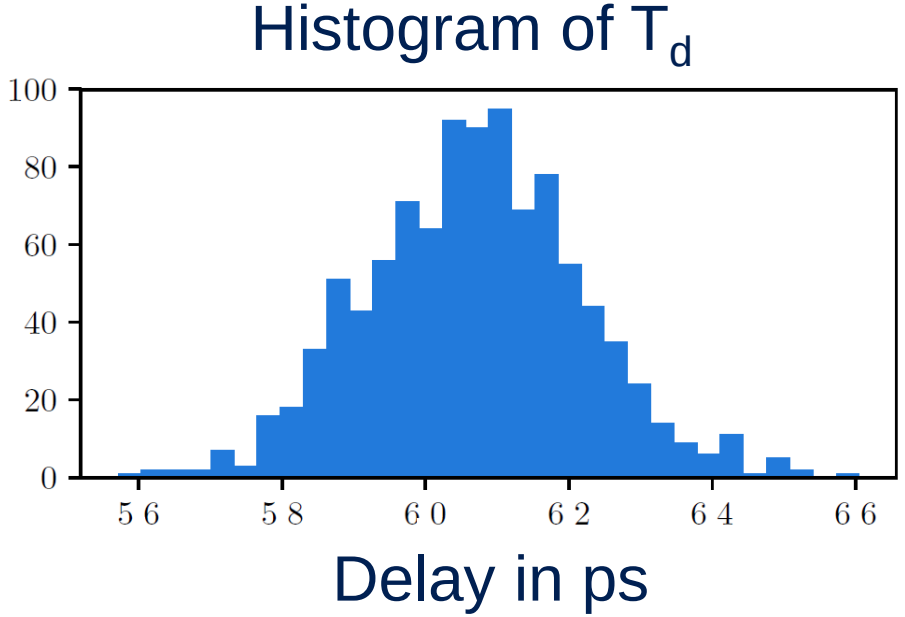
The Defaults at Gate Level

Logic gates and memories are composed of non homogeneous transistors

Ex: the inverter



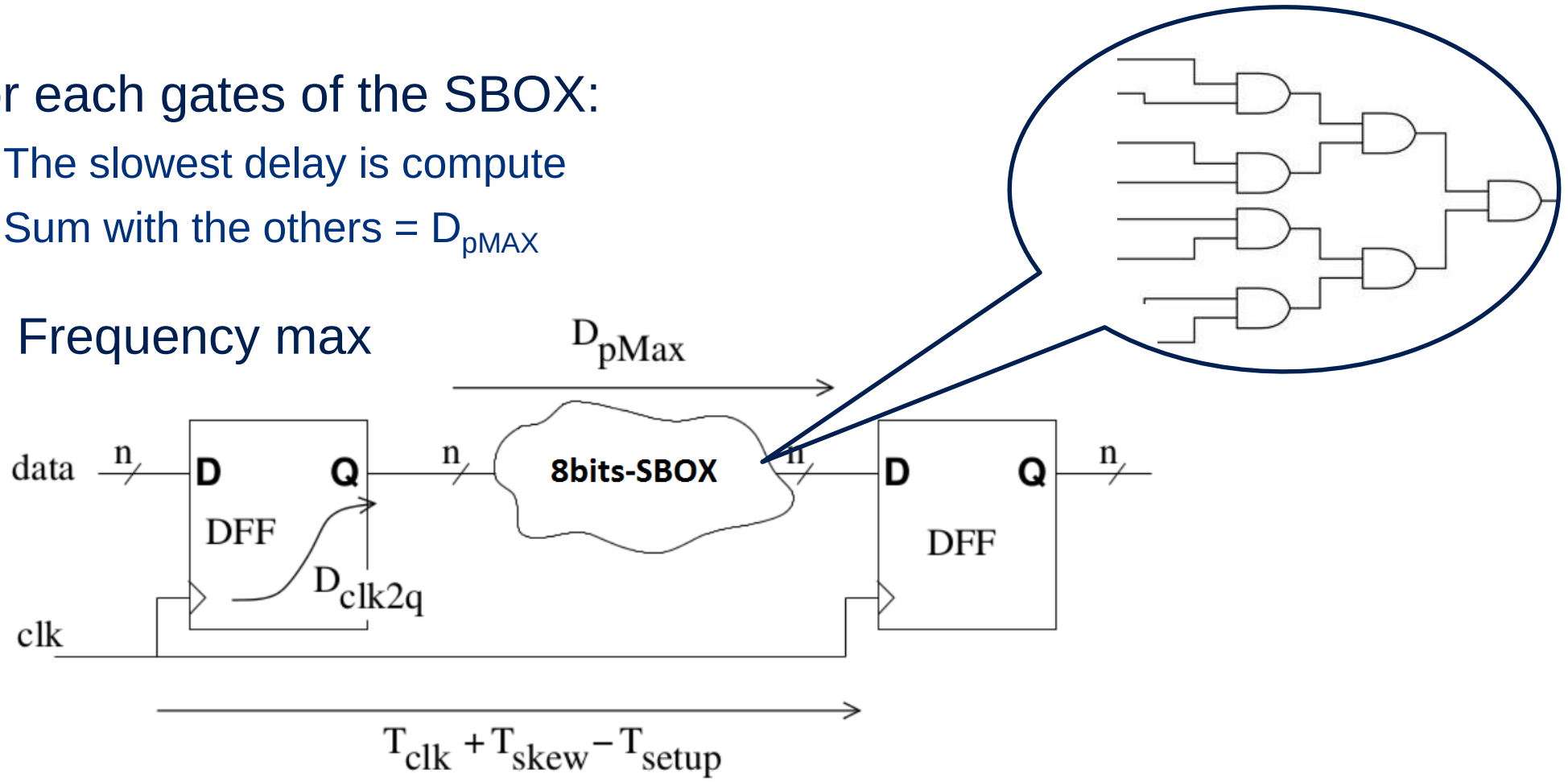




This is an issue for several TRNG, but not for deterministic blocks such as AES

Not a Problem for Deterministic Block

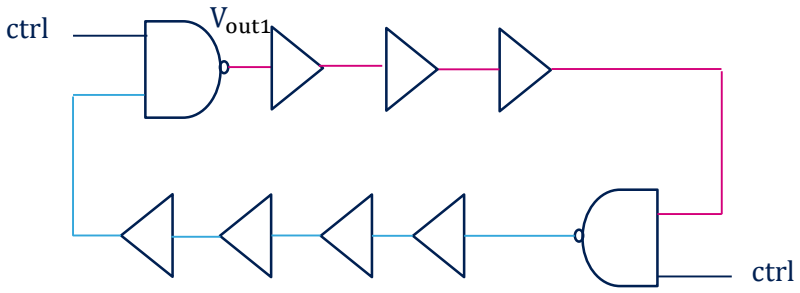
- For each gates of the SBOX:
  - The slowest delay is compute
  - Sum with the others = D_{pMAX}
- => Frequency max

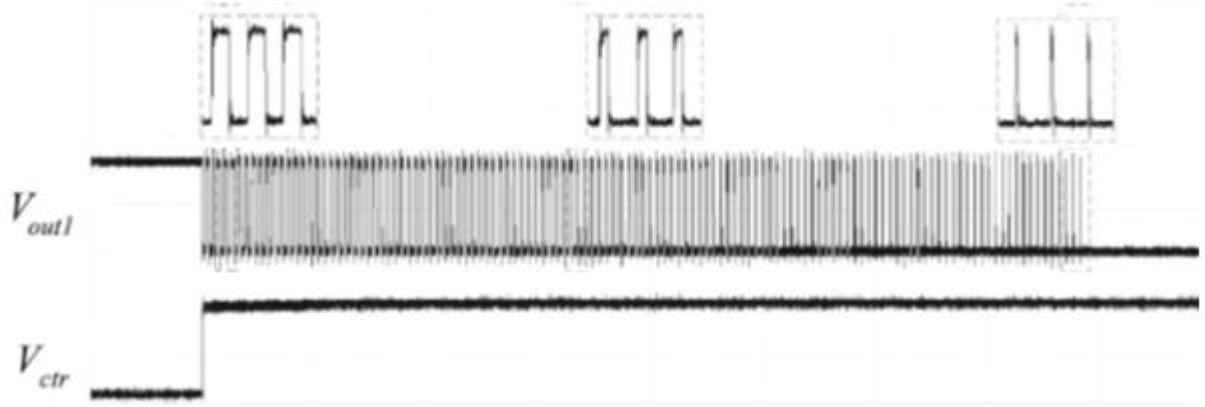


For several TRNGs this is an even more complex issue

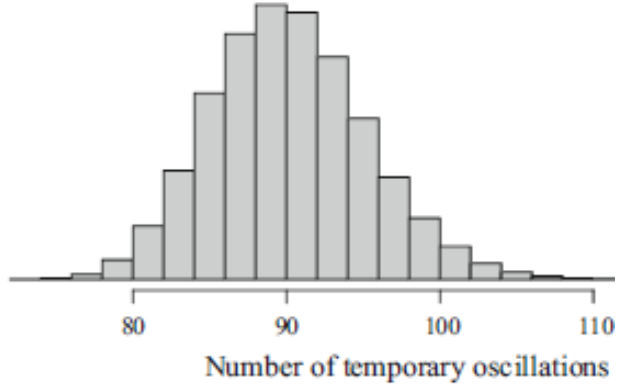
The Effect at TRNG Level

- The case of the TERO





- When CTRL signal is “0”, TERO does not oscillate and it output is “1”
- When CTRL goes to “1”, then TERO oscillates until it reaches a stable state
- There is a race between the 2 delay lines which leads to oscillation
- TERO generates pulses whose widths decrease until complete disappearance
- Entropy is carried by the phase noise which accumulates along the successive pulses
- The random bit is the parity value of the number of generated pulses.

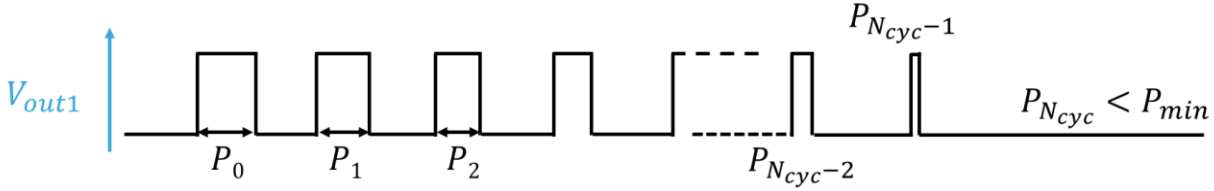


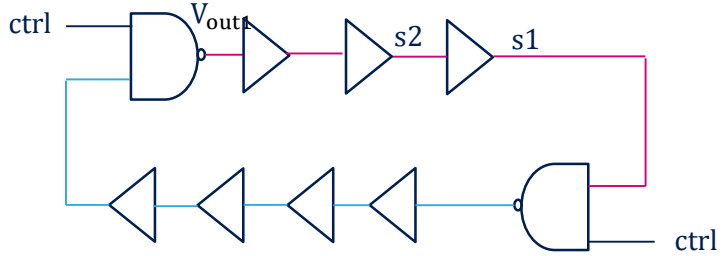
life.augmented

[VD10] M. Varchola, M. Drutarovsky, New high entropy element for FPGA based true random number generators

The Effect at TRNG Level

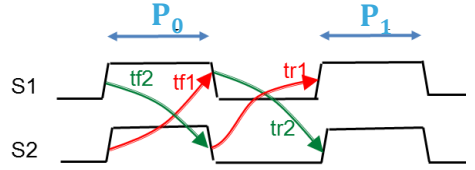
- TERO stop oscillates when P becomes too small to be propagated



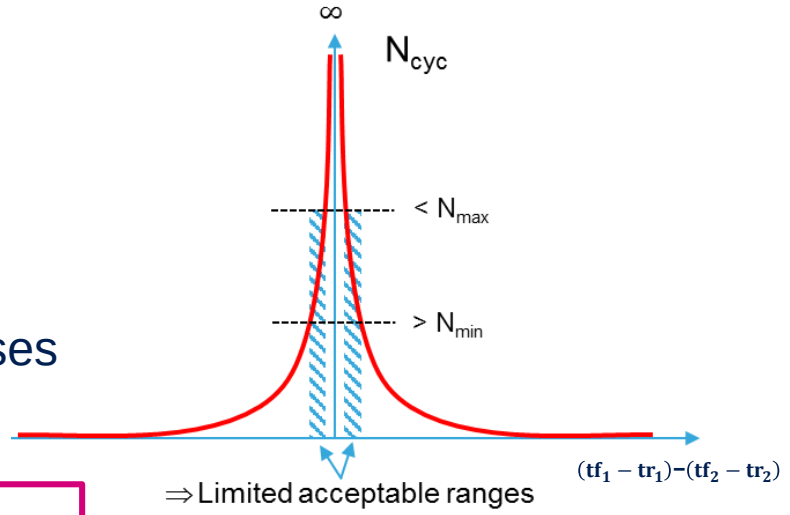


- Electrical modelling allows to predict the number of oscillations in the absence of noise (N_{cyc}):

$$N_{cyc} = \frac{P_0 - Pmin}{(tf_1 - tr_1) - (tf_2 - tr_2)}$$



- The random bit is the parity value of the number of generated pulses.
  - High N_{cyc} => Low Throughput
- Entropy is carried by the noise accumulated along the successive pulses
  - High N_{cyc} => High Entropy



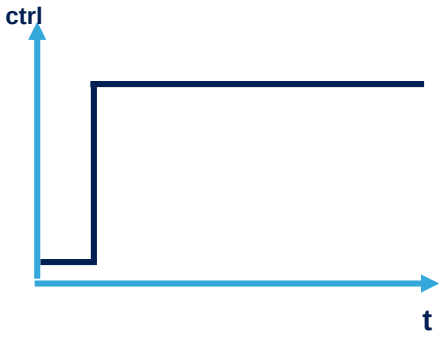
REMINDER

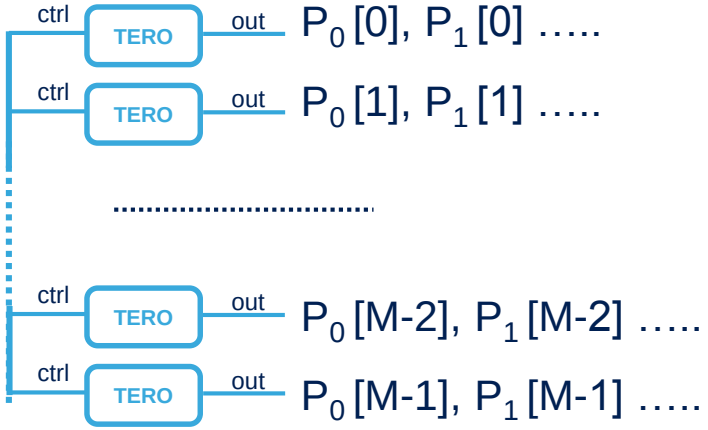
- tf_1, tr_1, tf_2, tr_2 are (slightly) impacted by:
  - The regularity of the stacks and the doping variations of the materials.

life.augmented

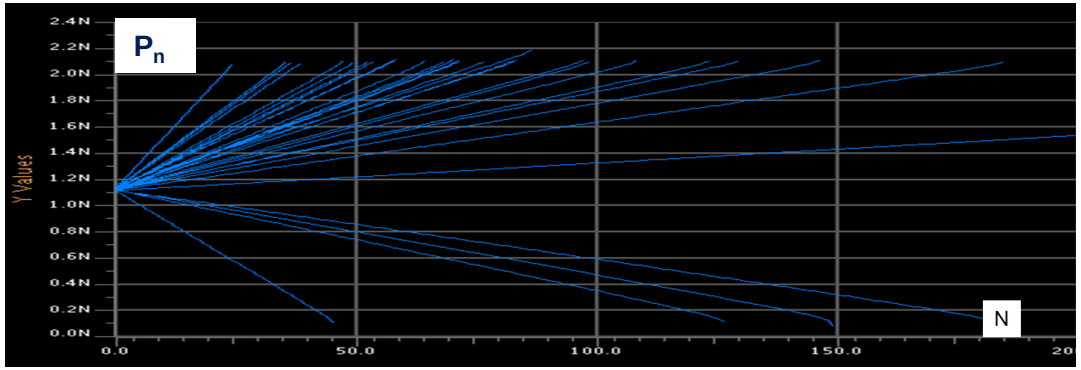
The Effect at TRNG Level

- TEROs are composed of non homogeneous transistors
- The experiment:





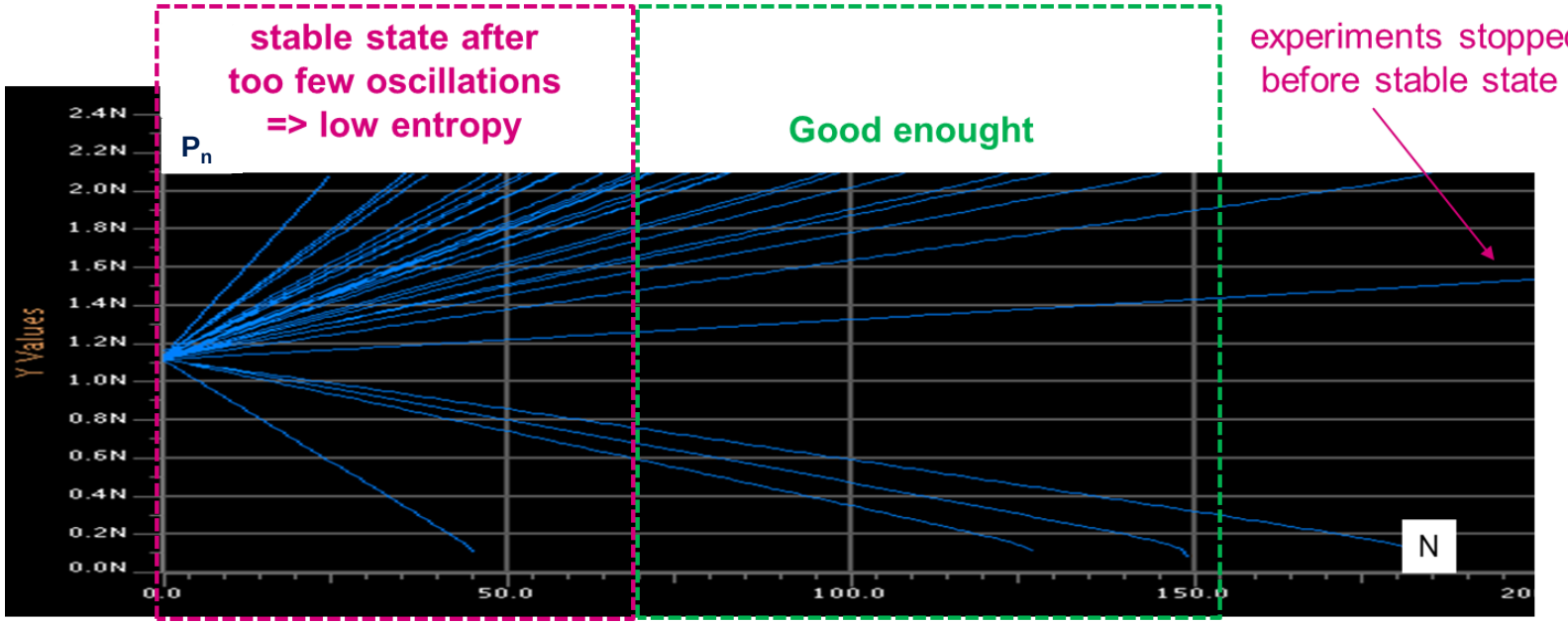
- The results:



life.augmented

The Effect at TRNG Level

- The results:



- Low entropy or throughput in more than 50% of the manufactured ICs
  - => verdict for TERO based TRNG:

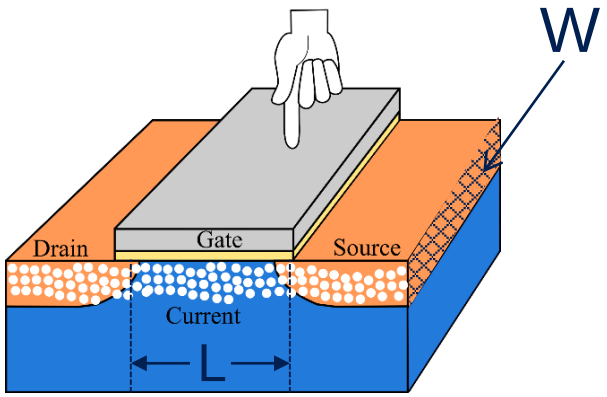
too sensitive to manufacturing variations

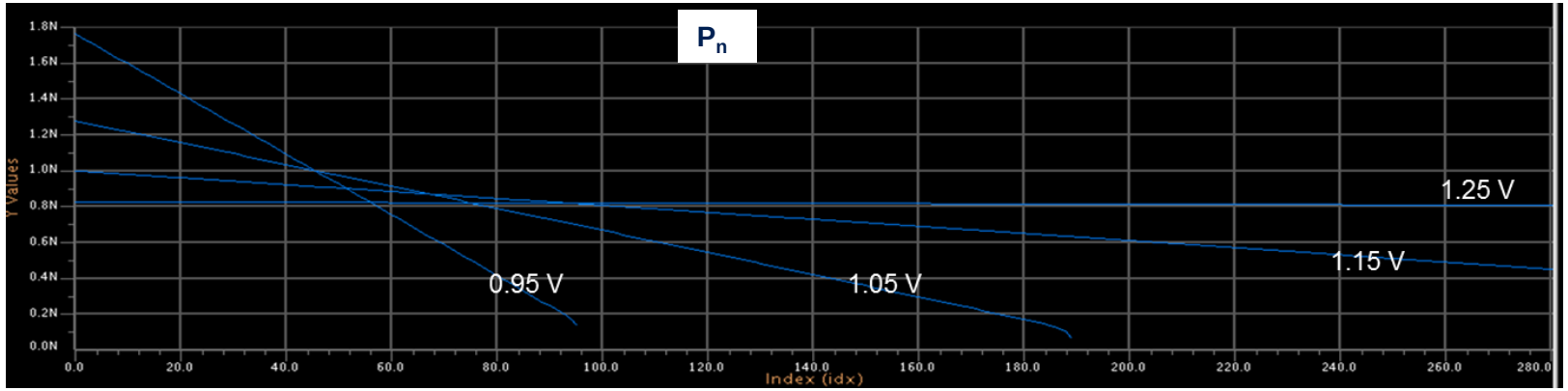
Study of the Voltage Supply Influence

TRNG Behavior & Voltage Variations

- Electrical parameters of the transistor are impacted by:
  - The voltage supply.
  - The temperature.

$$I_{DS} = \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot \frac{(V_G - V_{TH})}{2}$$





- Voltage variation lower than 10 % => non negligible entropy variations

  => verdict for TERO based TRNG:

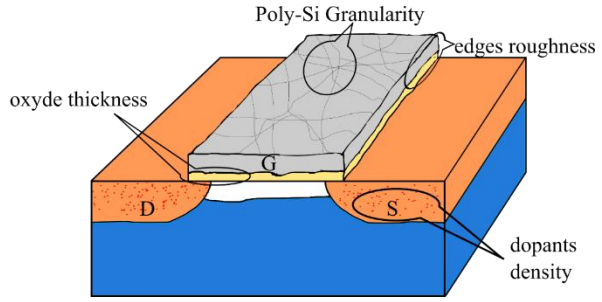
  too sensitive to voltage supply variations

life.augmented

First Conclusions

- Manufacture an IC is a set of complex, precise, long and expensive to set up processes
  - Fortunately we manufacture in parallel

- Tailored for mass production => Low unitary cost
- Master factors impacting the TRNG behavior is a key point for an IC manufacturer such as manufacturing process variations:
  - To avoid TRNG flaws in nominal conditions
  - Detectable with design phase simulations



- The voltage supply and the temperature are also studied factors.
  - To guarantee enough entropy in the IC range of usage conditions
- Allows us to evaluate the industrialization of TERO for next generations TRNGs.
- The TRNG behavior can also be maliciously impacted by environmental factors: Perturbation attacks

→ Next section

Study of Malicious Manipulations

Malicious Manipulations

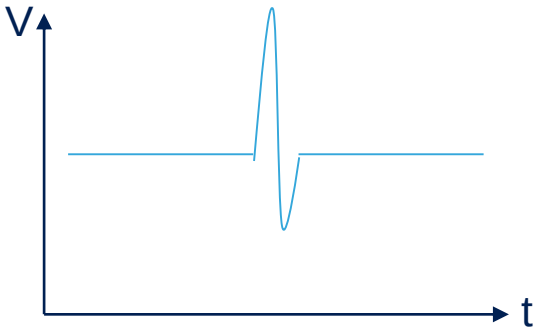
Perturbation attacks are generating and exploiting faults in embedded systems

Non or semi-invasive active HW attacks (if chip-package needs to be removed)

- Identify source capable of generating exploitable faults
  - Glitches on power-supply or clock, EM perturbation, Laser shot, etc.

FI

- Disturb normal IC behavior & exploit resulting faults
  - Skip CPU instructions → bypass software checks, change execution flow, etc.
  - Alter product configuration bits (Ex: lifecycle state)
  - Fault in crypto processing (Ex: Differential Fault Analysis or “Safe-Error” attacks)
  - Influence / bias random number generators

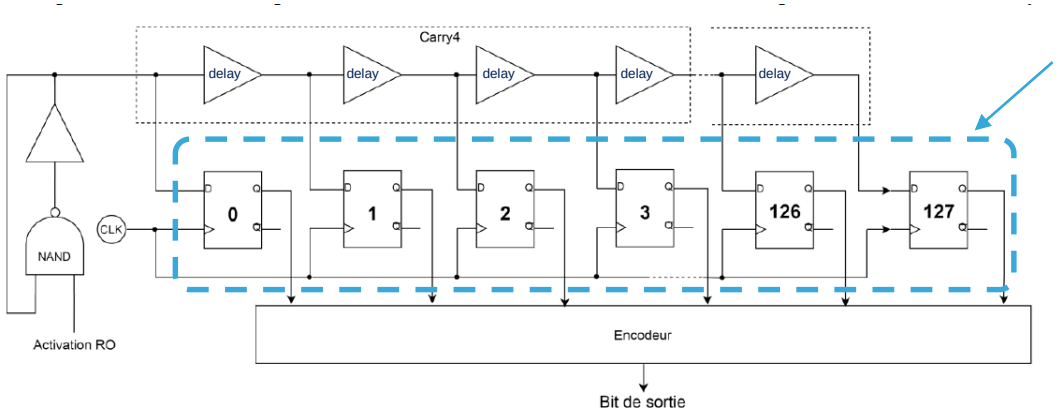


The DC-TRNG

- The DC-TRNG is a fully digital TRNG introduce in [RYBV15]
- Entropy is carried by the phase noise of a ring oscillator

- The phase noise digitization is performed by a « chronophotograph » technique
  - Implemented using a sampled delay chain

- An encoder transform the chronophotograph into a random bit.



DFF	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0

Is the DC-TRNG vulnerable against EM pulsed perturbations ?

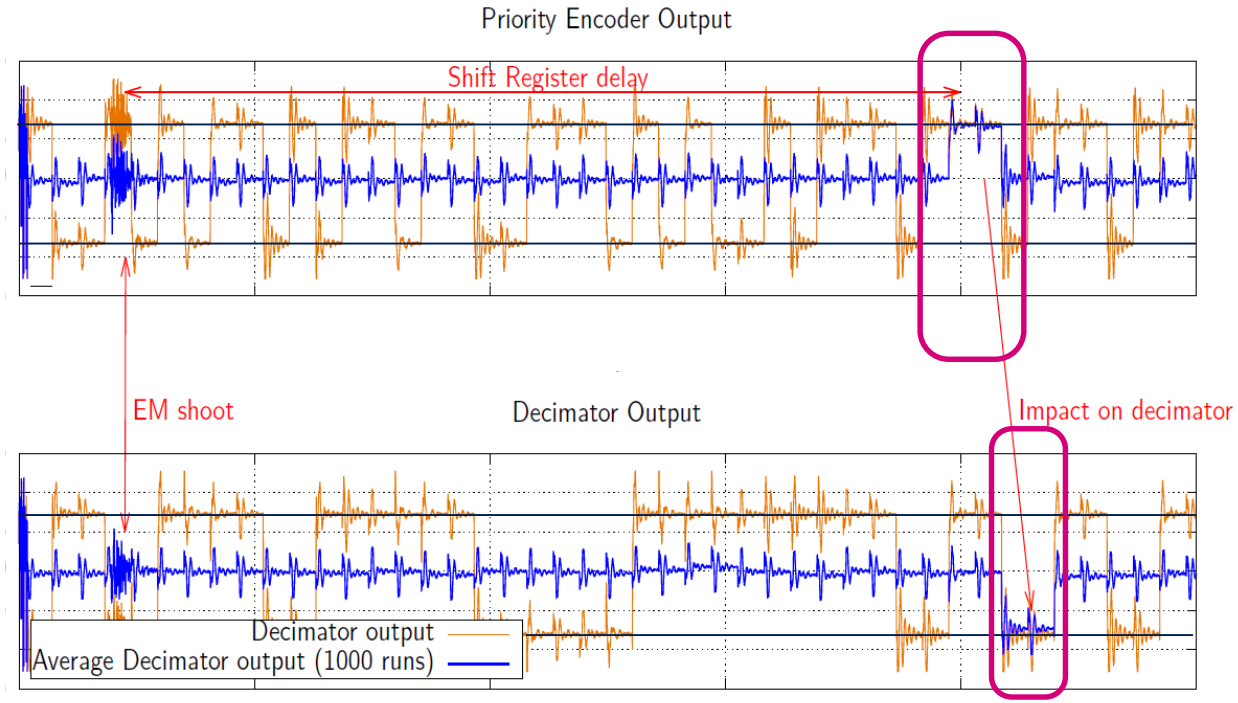
life.augmented

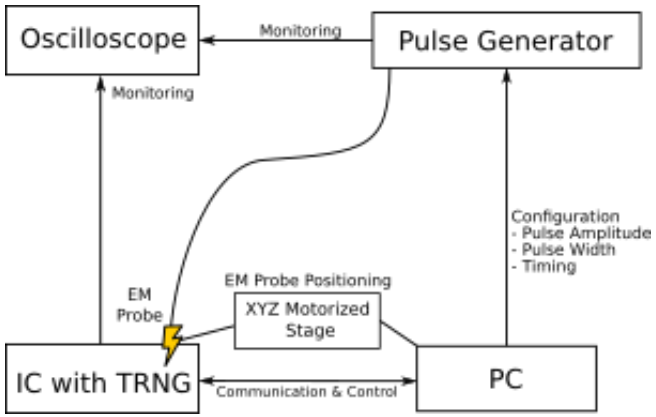
[RYBV15] Vladimir Rozic, Bohan Yang, Wim Dehaene, and Ingrid Verbauwhede, Highly efficient entropy extraction for true random number generators on fpgas

Malicious Manipulation of DC-TRNG

- We generate a pulsed electromagnetic field above the IC during the generations of random numbers

- We verify the presence of simple statistical defects:
  - e.g.: mono-bit, poker …





- After a pulse, we observe: two consecutives stuck at 1

- Is this attack decrease the security level ?
  - The time between 2 pulses is 500 µs for a high end pulser
  - 1 random bit is generated each 25 µs

- **In the worst case 1% of the bit can be manipulated**

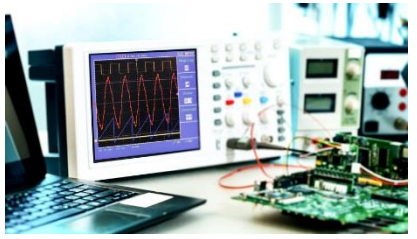
life.augmented

Conclusions

- Our goal is to develop by anticipation what will be needed by ST product divisions in 3-5 years
  - Security IP blocks (HW or SW)
  - Architectures
  - Expertise



- Leveraging the most advanced research activities & funneling them into commercial products, helping improve security of products in the field
- For TRNG IPs, we continuously analyze promising TRNGs proposed in the literature :
  - against variations of **manufacturing process** (e.g.: TERO TRNG)
  - against variations of **power supply** (e.g.: TERO TRNG)
  - against variations of **temperature**
  - against classical **physical attacks** (e.g.: DC TRNG)




- Works done in concertation with national / private certification agencies to improve the standards and share compatibles roadmaps

Thank You

life.augmented