Hardware design for cryptographers: Dreams and Reality

Ingrid Verbauwhede

Ingrid.verbauwhede-at-esat.kuleuven.be

KU Leuven, COSIC

Acknowledgements:
Current and past PhD students

KU LEUVEN

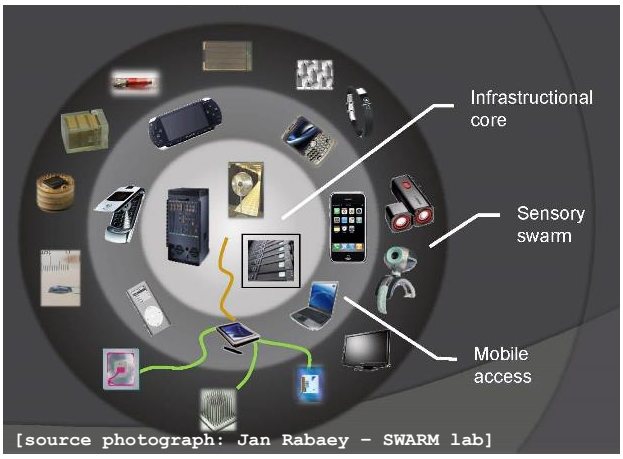
erc

Outline

- Hardware design for cryptographers and information security in general
- Past: focus on efficiency
- Present: focus on efficiency and security (i.e. resistance to side-channel and fault attacks)
- Future: hardware entangled cryptography
  - Physically Unclonable Functions
  - Random number generators

Cyber physical systems

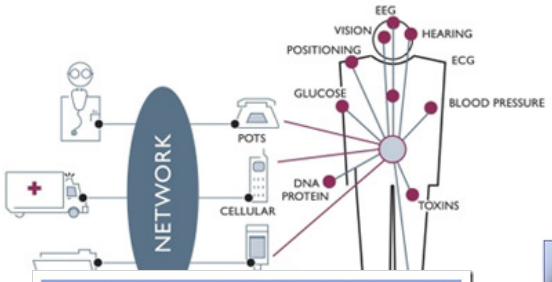
"Networked embedded systems interacting with the environment"

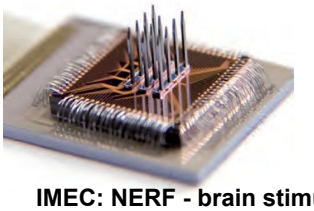


Jan Rabaey, "From batch to interactive to immersion"

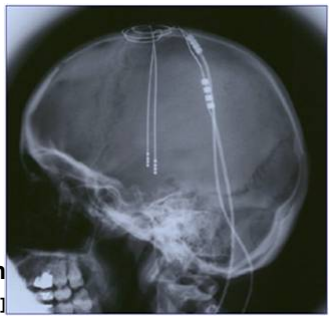
KU Leuven - COSIC | Croatia Summerschool - 3 | June, 2017

Example from E-Health: mobile, networked, interacting with environment





IMEC: NERF - brain stimulant

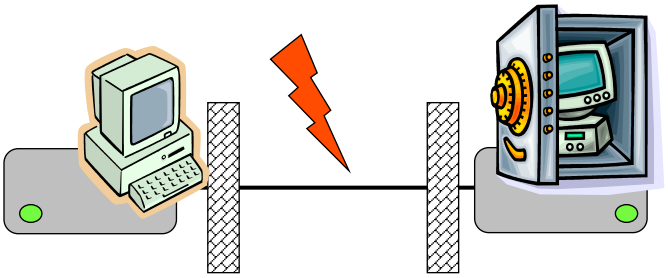


ulation

[Sources: J. Rabaey, National Institutes of Health, Neurology journal]

KU Leuven - COSIC | Croatia Summerschool - 4 | June, 2017

Past: attacker model for computing nodes



Old attack model (simplified view):
-Attack on channel between communicating parties
-Encryption and cryptographic operations in **black** boxes
-Protection by strong mathematic algorithms and protocols

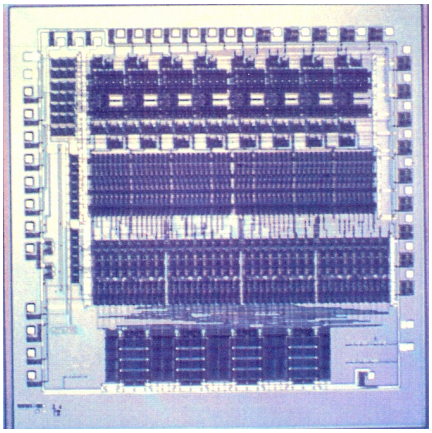
Focus on EFFICIENCY

KU Leuven - COSIC | Croatia Summerschool - 5 | June, 2017

Past: design for efficiency – e.g. DES

Efficiency

- Data Encryption Standard
- Programmable co-processor
- Enc/Dec
- 3DES
- PRNG
- MAC generation
- Modes of operation



[EuroAsic 1991]

KU Leuven - COSIC | Croatia Summerschool - 6 | June, 2017

Next: Power and energy constraint added!

- Power is limited:
  - RFID tags
  - Cooling!!
  - Implanted devices only temperature Δ < 1 °C
- Energy Battery is limited
  - Pace maker battery is not rechargeble
  - One AAA battery is 1300 … 5000 Joule
- **How much crypto in one (micro) Joule ?**

KU Leuven - COSIC | Croatia Summerschool - 7 | June, 2017

Past: efficiency & power - Rijndael

- Rijndael AES evaluation
- Enc + Dec
- 0.18 µm CMOS
- Standard cells
- 2.3 Gbits/sec
- ***Only*** 56 mW
- ***Or 11 Gbits/Joule***

[JSSC 2003]

KU Leuven - COSIC | Croatia Summerschool - 8 | June, 2017

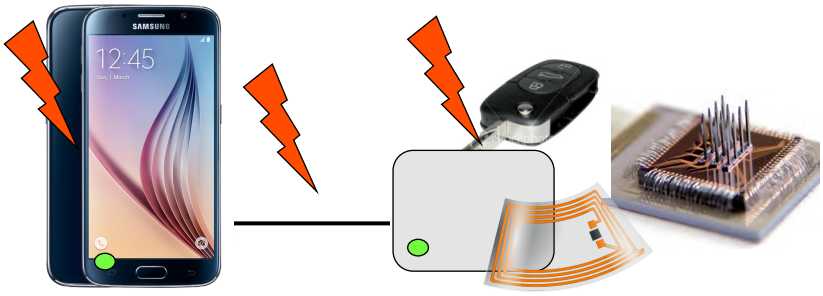
Past: Throughput – Energy numbers

AES 128bit key 128bit data	Throughput	Power	Figure of Merit (Gb/s/W = Gb/J)
180 nm CMOS	3.84 Gbits/sec	350 mW	11 (1/1)
FPGA [1]	1.32 Gbit/sec	490 mW	2.7 (1/4)
Intel ISA for AES	32 Gbit/sec	95 W	0.34 (1/33)
ASM StrongARM [2]	31 Mbit/sec	240 mW	0.13 (1/85)
Asm Pentium III [3]	648 Mbits/sec	41.4 W	0.015 (1/800)
C Emb. Sparc [4]	133 Kbits/sec	120 mW	0.0011 (1/10.000)
Java [5] Emb. Sparc	450 bits/sec	120 mW	0.0000037 (1/3.000.000)

[1] Amphion CS5230 on Virtex2 + Xilinx Virtex2 Power Estimator
[2] Dag Arne Osvik: 544 cycles AES – ECB on StrongArm SA-1110
[3] Helger Lipmaa PIII assembly handcoded + Intel Pentium III (1.13 GHz) Datasheet
[4] gcc, 1 mW/MHz @ 120 Mhz Sparc – assumes 0.25 u CMOS
[5] Java on KVM (Sun J2ME, non-JIT) on 1 mW/MHz @ 120 MHz Sparc – assumes 0.25 u CMOS

KU Leuven - COSIC | Croatia Summerschool - 9 | June, 2017

Current: attacker model for embedded system



Modified Attack Model (also simplified view):
-Attack channel *and* endpoints
-Encryption and cryptographic operations in **gray** boxes
-Protection by strong mathematic algorithms and protocols
-Protection by secure implementation

Need secure implementations not only algorithms

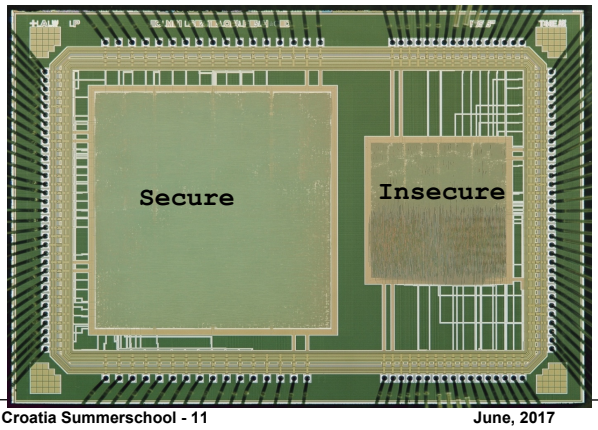
KU Leuven - COSIC | Croatia Summerschool - 10 | June, 2017

Past: AES *with* DPA countermeasures

- AES, 2nd generation
- Regular & secure circuit style (**WDDL)** based implementation
- Standard cells

- 1 Gbit/sec @ 50MHz
- to 3.8 Gbits/sec @ 330MHz
- 50mW unprot
- to 200mW prot

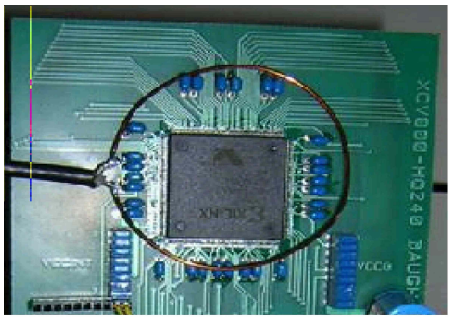
[CHES2005]

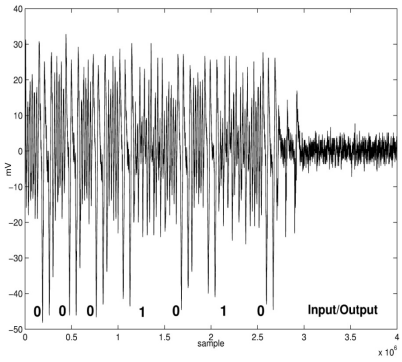


KU Leuven - COSIC | Croatia Summerschool - 11 | June, 2017

Design for efficiency AND security

SEMA attack: Simple Electromagnetic Attack on Elliptic Curve Public Key implementation.



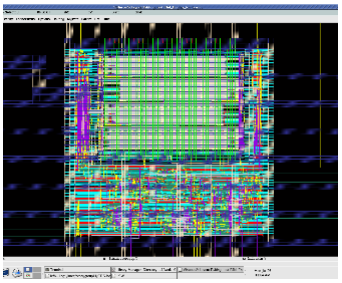


[E. Demulder EUROCON 2005]

KU Leuven - COSIC | Croatia Summerschool - 12 | June, 2017

Low Power, Low Energy Public Key Crypto

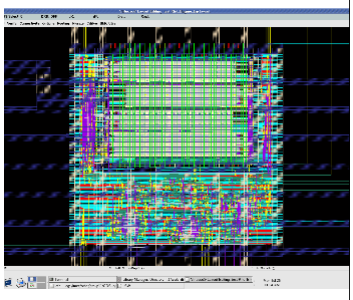
- Goal: public key engine
- Suitable for SWARM, RFID, sensor nodes, IoT, medical devices
- Low Power: cooling - temperature $\Delta < 1$ °C
- Low energy: battery life – 10+ years
- With suitable set of countermeasures



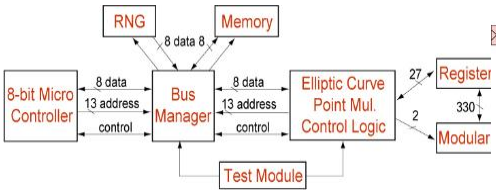
KU Leuven - COSIC | Croatia Summerschool - 13 | June, 2017

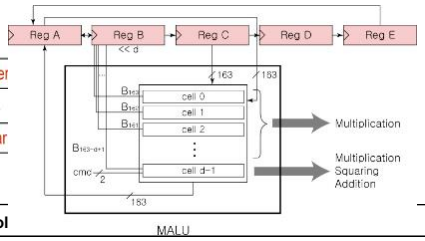
Result

- ECC 163-bit co-processor
  - ECC point multiplications (163 by 4)
  - scalar modular operations (8-bit processor with redundancy)
- 14K gates
- 79K cycles or 158 msec @500 KHz
- **< 5 mJoule** per point mulitplication!



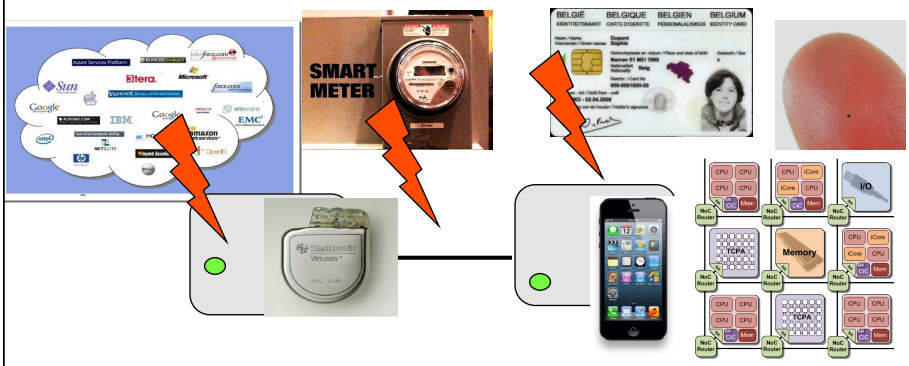
[DAC2011]





KU Leuven - COSIC | Croatia Summerschool

Future: security for immersed system: model?



New Model (also simplified view):

-Attack on the "System"
-Firewalls? there is NO "inside" versus "outside"
-Encryption, trust, security "immersed"
-Devices cooperate to build up trust, multiparty
-All old requirements still stand

Hardware roots of trust

- Moore's law benefits the attacker …
- Secure computation: ala Intel SGX, Cosic/Distrinet Sancus,
- Secure storage: Physically Unclonable Functions
- Random number generation
- Post-quantum secure implementations
- …

PUFs: Dreams and Reality

Ingrid Verbauwhede

Ingrid.verbauwhede-at-esat.kuleuven.be

KU Leuven, COSIC

Acknowledgements:
current: **Jeroen Delvaux, Kent Chuang**
past: Roel Maes, Anthony Van Herrewege

PUF research funded by:

KU LEUVEN

iwt

unique

PUFFIN INFSO-ICT-284833

HINT

HECTOR

Outline

- Ideal PUF
- Reality of PUF

- PUF for authentication
- PUF for key generation
- Is there still research to be done on PUFs?

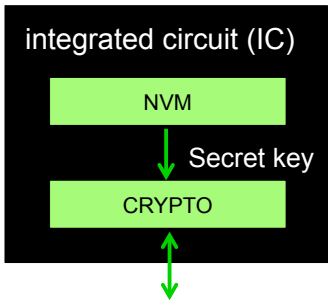
Silicon PUFs – Motivation

A cost-efficient replacement technology for secure non-volatile memory (NVM)

- EEPROM/Flash
- Fuses
- Battery-backed SRAM

Embedded context:

- Physical attacks
- Compatible regular CMOS technology

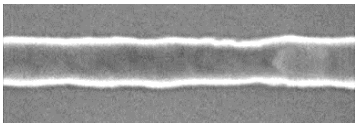


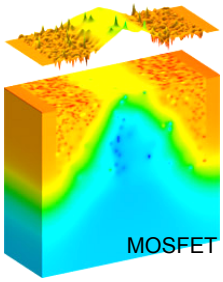
KU Leuven - COSIC | Croatia Summerschool - 19 | June, 2017

Silicon PUFs - Variability

- Silicon Biometrics
- Variability in transistors and interconnect
- In general undesired, except for PUFs
- Random dopant fluctuation
- Line edge/width roughness
- Crucial design challenge with CMOS down scaling (Moore's law)

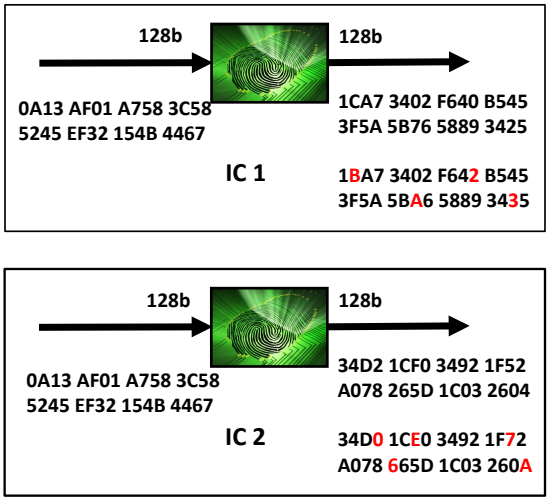
  Pelgrom's law: $\sigma^2 \sim 1/WL$ (Marcel Pelgrom, Dutch engineer)





KU Leuven - COSIC | Croatia Summerschool - 20 | June, 2017

The ideal PUF?



Chip-dependent binary function with noisy output

Evaluation 1

≈ 1-15% noise

Evaluation 2

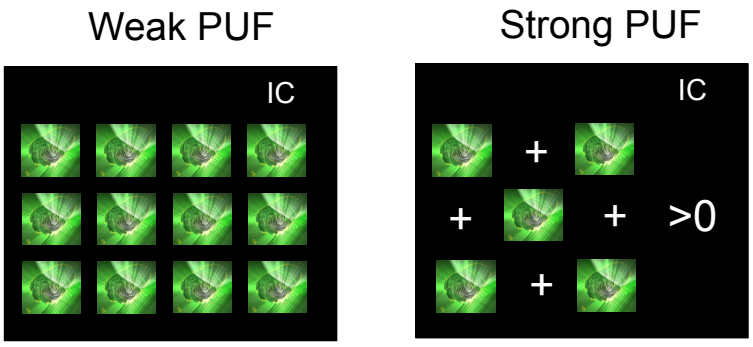
Evaluation 1

Evaluation 2 ≈ 1-15% noise

IDEAL PUF is without noise

PUF (F = Function)

- **Dream 1: IDEAL PUFS don't exist...**
- Two design methodologies for PUF circuits

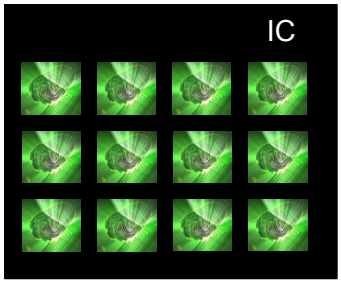


Weak PUF

- An array of identically designed circuit elements
- Each producing 1 (or a few) response bit(s)
- High-quality response bits, i.e., high entropy
- Limited number of bits, e.g., a few 1000s
- (Weak because of limited response size)
- E.g., SRAM PUF, soft-breakdown PUF

- Typical application: key generation

  E.g. 128-bit AES



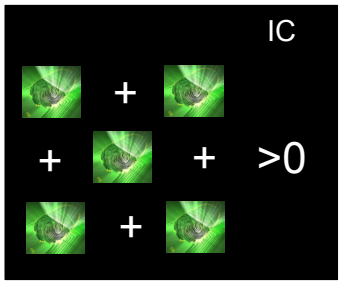
KU Leuven - COSIC | Croatia Summerschool - 23 | June, 2017

Strong PUF

- Finite number of physical building blocks combined with mathematical operations
- E.g., sum of delays, currents, voltages etc.
- Can produce a gazillion of response bits (2^{128}) ➔ Strong
- Low-quality bits: highly correlated, low-entropy

- E.g., arbiter PUF
- Typical application:

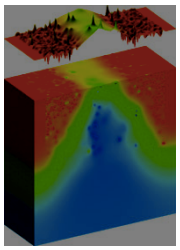
  IC authentication



KU Leuven - COSIC | Croatia Summerschool - 24 | June, 2017

PUF (U = Unclonable)

PUF properties: Unique, Reliable, Unclonable



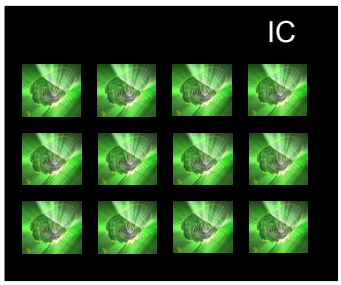
[3D picture TOR]

- It is not feasible to make an exact analog physical clone (a technological constraint)
- But MATHEMATICAL clone
- The main problem is the digital clone:
  - Same black-box challenge – response behavior
  - Internals are different, but does not matter

KU Leuven - COSIC | Croatia Summerschool - 25 | June, 2017

Digital Clone of a Weak PUF

- Corresponds with a simple array read-out
- Applications should not reveal the PUF state
- Typically the case for PUF-based key generation
- Obtaining the PUF response = obtaining the key

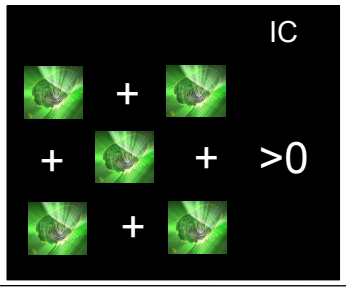


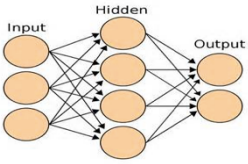
0 1 1 0
1 0 0 0
0 1 0 1

KU Leuven - COSIC | Croatia Summerschool - 26 | June, 2017

Digital Clone of a Strong PUF

- A full CRP read-out might not be feasible
- A gazillion of bits (2^{128}), computionally infeasible
- However, the bits are highly correlated
- Model building, using a small CRP training set
- Machine Learning: Artificial Neural Networks, Evolution Strategies, etc.

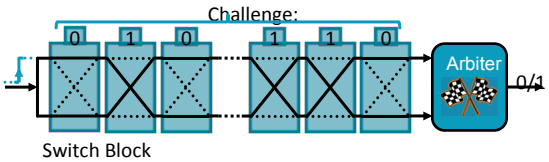


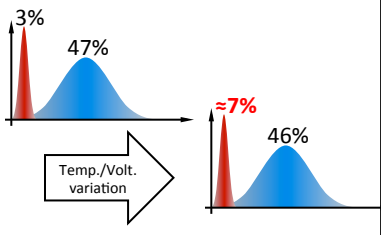


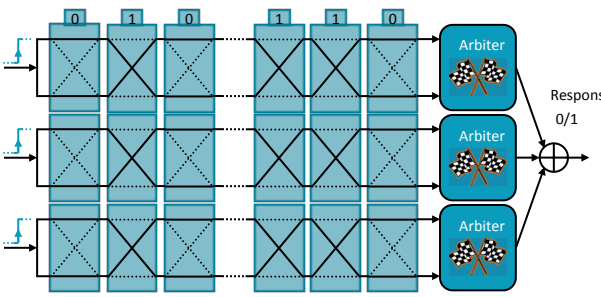
KU Leuven - COSIC | Croatia Summerschool - 27 | June, 2017

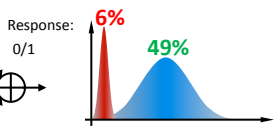
Arbiter PUFs: XOR Variant

- Arbiter PUF: original MIT work
- UNIQUE project result







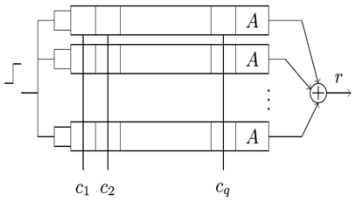


UNIQUE ASIC results

KU Leuven - COSIC | Croatia Summerschool - 28 | June, 2017

Arbiter PUF – XOR Variant

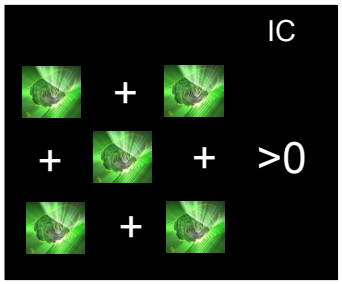
- XOR the response of multiple chains
- More resistant against machine learning
  - # CRPs in training set ↑
  - Training time ↑
- Unfortunately, noise amplification as well
- Lastest results: Becker et al. at CHES 2015



ML Method	CRP Source	Pred. Rate	No. of XORs	CRPs ($\times 10^3$)	Training Time
LR	FPGA	> 99%	3	19.5	51.5 sec
			4	39	139 sec
			5	78	39 min
LR	ASIC	> 99%	3	19.5	26 sec
			4	39	63.5 sec
			5	78	18:09 min

[Ruhrmair, IEEE TIFS 2013]

Dream or future research?

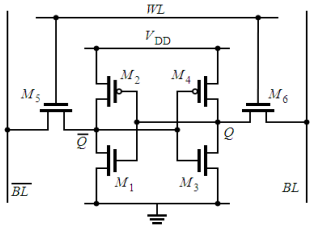


Wish a strong PUF:

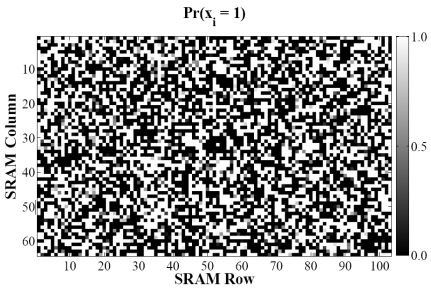
- Finite number of elements
- Gazillion Challenge Response Pairs
- Non-linear combination to resist modeling attacks: ideally cryptographic function
- BUT: noise amplification makes output not useful

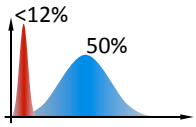
Dream: strong PUF from finite number of elements, resistant to modeling, noise tolerant

SRAM PUF: Basic construction & results

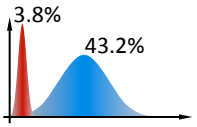


6T CMOS SRAM Cell

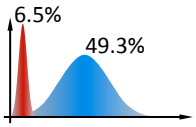




Guajardo et al. 2007, FPGA SRAM temp./volt. var.



Holcomb et al. 2009, Commercial SRAM

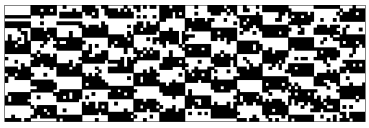


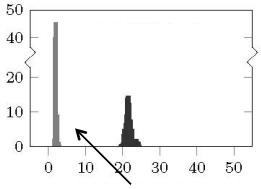
Holcomb et al. 2007, Embedded SRAM

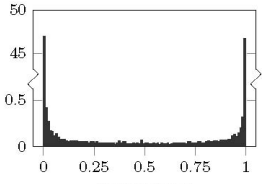
PUF behavior of SRAM in commodity micro-controller

Black box approach (off the shelf micro-controllers)

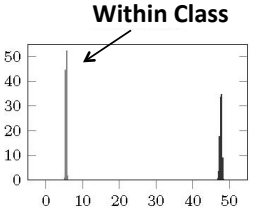
- `PIC16F1825`

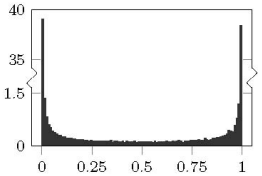






- `STM32F100R8`



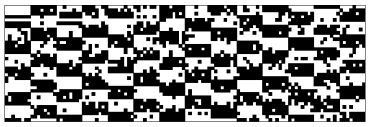


[PhD thesis Anthony VH, PUFFIN]

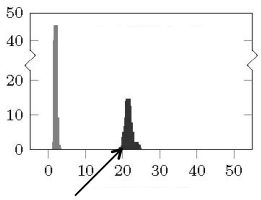
PUF behavior of SRAM in commodity micro-controller

Black box approach (off the shelf micro-controllers)

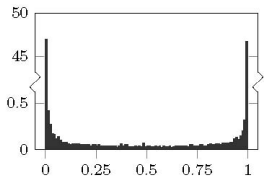
- PIC16F1825



Within and between class HD (%)

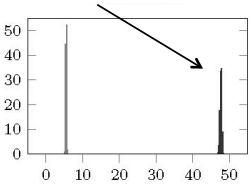


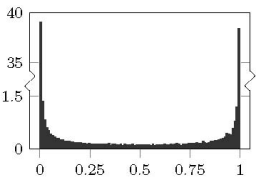
Average bit value (%)



- STM32F100R8

Between Class





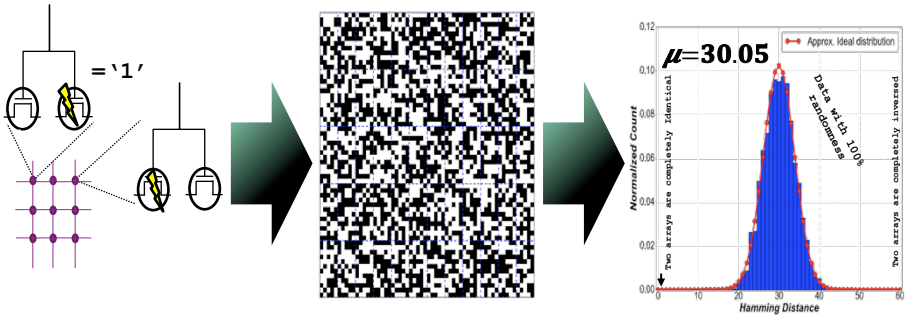
Not yet useful: needs post-processing to create ID or key!

IMEC-COSIC soft breakdown PUF circuits

IMEC Breakdown PUF [patent]

Random Spatial Distribution

Si proven stable PUF



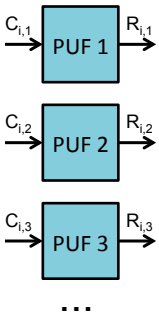
- ✔ Low cost, low power for IoT, reliable, small footprint
- ✔ No trusted third party: Key generation could be by end user
- ✔ Both random key generation & programmable keys

PUF Usage

Strong PUF: Entity authentication

Weak PUF: Key Generation

Challenge/Response (C/R) Identification Basic: Enrollment



1. Generate random challenges $C_{i,j}$ and apply to PUF population

2. Store responses $R_{i,j}$ in CRP database

PUF ID	Challenge	Response
1	$C_{1,1}$	$R_{1,1}$
1	$C_{2,1}$	$R_{2,1}$
1	$C_{3,1}$	$R_{3,1}$
2	$C_{1,2}$	$R_{1,2}$
2	$C_{2,2}$	$R_{2,2}$
2	$C_{3,2}$	$R_{3,2}$
3	$C_{1,3}$	$R_{1,3}$
3	$C_{2,3}$	$R_{2,3}$
3	$C_{3,3}$	$R_{3,3}$
...	...	...

Challenge/Response (C/R) Identification
Basic: (Authenticated) Identification

1. Send ID = 2
2. Pick random stored challenge $C_{i,2}$ for ID=2 and apply to PUF
3. If measured response $R'_{i,2}$ is "close enough" to stored response $R_{i,2}$ then accept
4. Scratch used CRP from database

PUF ID	Challenge	Response
1	$C_{1,1}$	$R_{1,1}$
1	$C_{2,1}$	$R_{2,1}$
1	$C_{3,1}$	$R_{3,1}$
2	$C_{1,2}$	$R_{1,2}$
2	$C_{2,2}$	$R_{2,2}$
2	$C_{3,2}$	$R_{3,2}$
3	$C_{1,3}$	$R_{1,3}$
3	$C_{2,3}$	$R_{2,3}$
3	$C_{3,3}$	$R_{3,3}$
...	...	...

Lightweight Protocols for strong PUFs

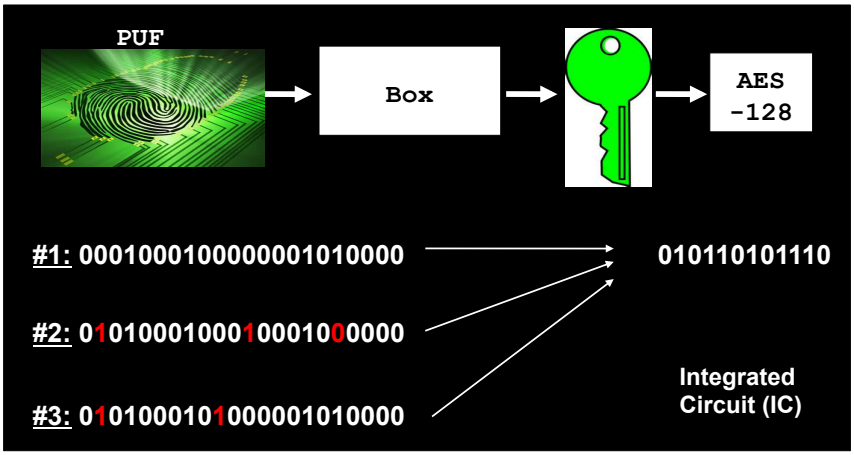
A large-scale study of strong PUF protocols:

„Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible?"

[Delvaux, CHES 2014]
[Delvaux, ACM Comp. Surveys 2015]

		Reference II-A	Reference II-B	Basic	Controlled	Bolotnyy et al.	Öztürk et al.	Hammouri et al.	Kulseng et al.	Sadeghi et al.	Reconfiguration	Reverse FE I	Reverse FE II	Converse	Lee et al. I	Jin et al.	Slender	Xu et al.	He et al.	Jung et al.	Lee et al. II	Noise bifurcation	System of PUFs
resources (#6)	Weak PUF	✓	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	✓
	Strong PUF[1]	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	MTP NVM	×	×	×	×	✓	✓	×	✓	×	✓	×	×	×	✓	✓	×	✓	✓	✓	✓	×	×
	TRNG	×	✓	×	×	×	×	✓	×	✓	×	×	✓	✓	×	×	✓	×	×	~	×	✓	×
	Gen	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×
	Rep	✓	✓	×	×	×	×	×	×	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×
	Crypto (Enc/Hash/MAC)	✓	✓	×	✓	×	×	×	×	✓	×	✓	✓	✓	✓	✓	×	×	×	×	✓	×	×
	PRNG	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
	$\oplus, =?$	×	✓	×	×	×	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×
	$1\times$ interface	✓	✓	×	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
claims	Server authenticity	×	✓	×	×	×	×	×	✓	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×
	Token authenticity	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Token privacy	×	×	×	×	✓	×	×	✓	✓	~	×	×	×	×	✓	×	✓	✓	×	✓	×	×
	Leakage resilience (#2)					×	×		×	✓	~				×	~		×	✓	✓	✓		
	# Authentications	∞	∞	d	d	d	∞	∞	∞	∞	d	∞	∞	∞	d	∞	∞	d	∞	∞	∞	∞	d
evaluation	Noise Robust (#3)	✓	✓		✓	×	~	×	×	✓		✓	✓		×	×	✓	×	×	×	×	✓	~
	Modeling Robust (#4)	✓	✓	×	✓	×				✓	×	✓	✓				~	~				~	×
	PUF Independency (#7)	✓	✓		~					~		×	✓				×					×	
	Server authenticity (#8)		✓						×			~	✓	×	✓	×		×	×	×			
	Token authenticity (#8)	✓			✓				×	✓		~	✓		✓		~		×	×		✓	
	Token privacy (#8)								×	✓									×				
	DoS prevention (#8)	✓	✓		✓	×	×		×	✓	×	✓	✓		×	×	✓		×	×	×	✓	
	Leakage resilience (#8)									✓						×			×	×			
	Scalability[2] (#9)	✓	✓	✓	✓					×		✓	✓			×	✓				✓		

WEAK PUF-Based Key Generation

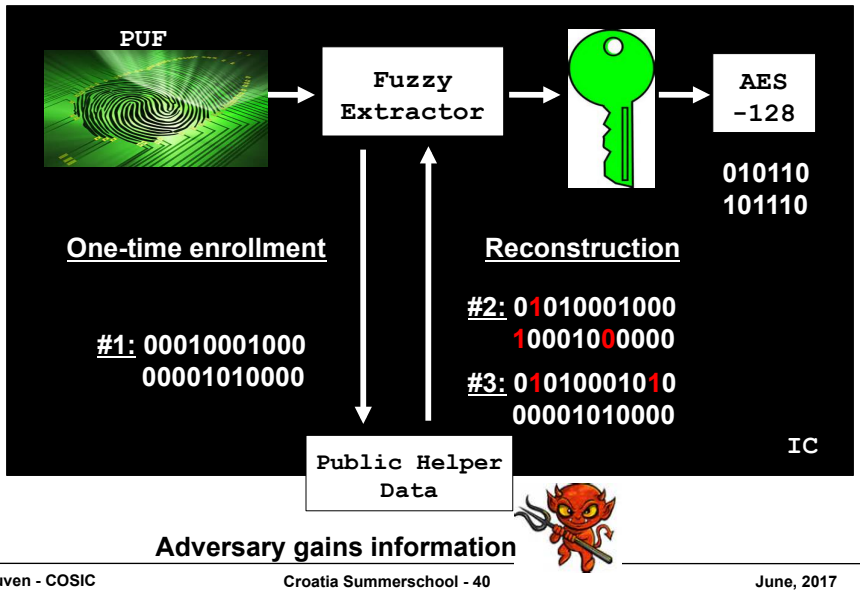


(1) noisy (BER up to 20%)
(2) non-uniform (e.g., more '0' than '1')

(1) stable
(2) uniform

KU Leuven - COSIC | Croatia Summerschool - 39 | June, 2017

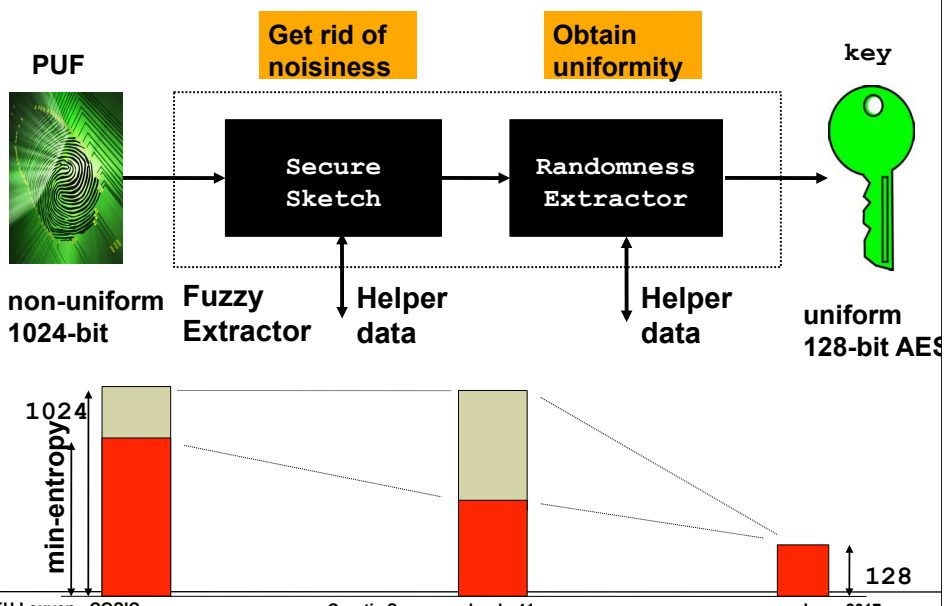
WEAK PUF Key generation with Fuzzy Extractor: Two Phases



Adversary gains information

KU Leuven - COSIC | Croatia Summerschool - 40 | June, 2017

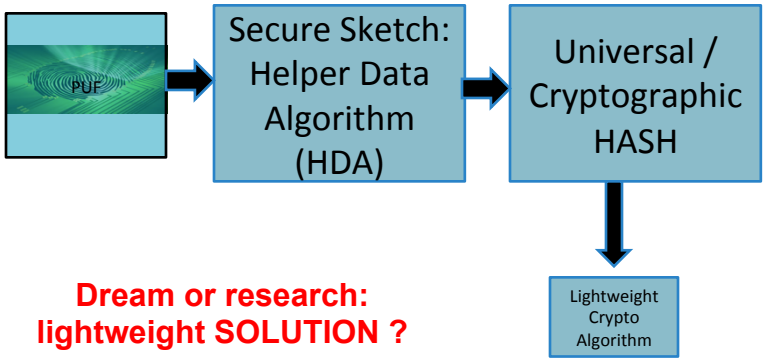
Fuzzy Extractor Min-Entropy Loss



KU Leuven - COSIC Croatia Summerschool - 41 June, 2017

Light weight solution?

- PUF is promised as 'light-weight' key generation for Internet of Things, RFID tags, etc.
- Key generation is larger than lightweight algorithm??



Dream or research: lightweight SOLUTION ?

KU Leuven - COSIC Croatia Summerschool - 42 June, 2017

True Random Number Generator

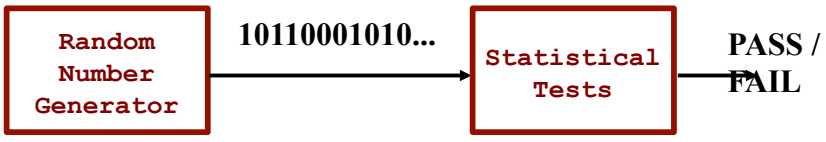
Difficult job!!
Ignored by crypto and masking community

Slide courtesy: Vladimir, Bohan, Josep

HECTOR

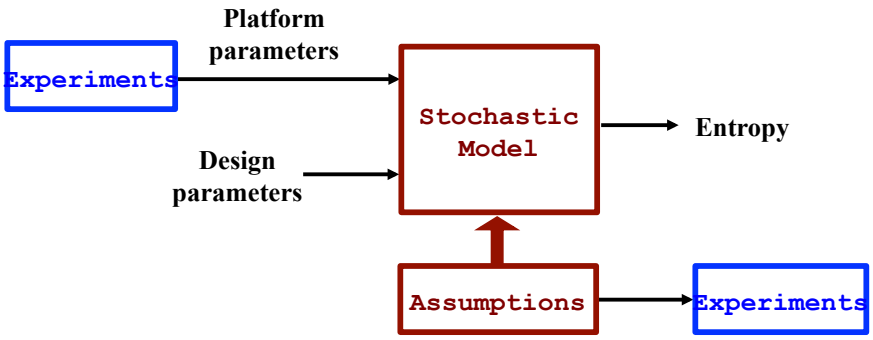
TRNG: the old school

NIST statistical tests:

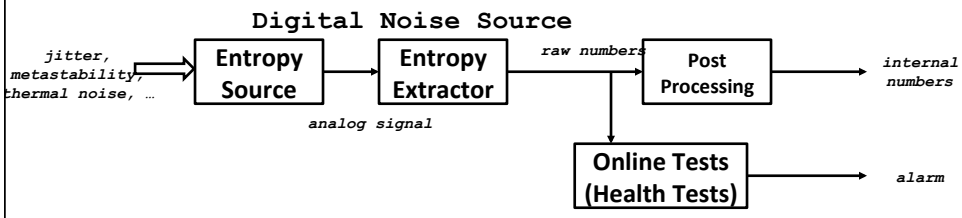


TRNG Design methodology

THE NEW METHOD:



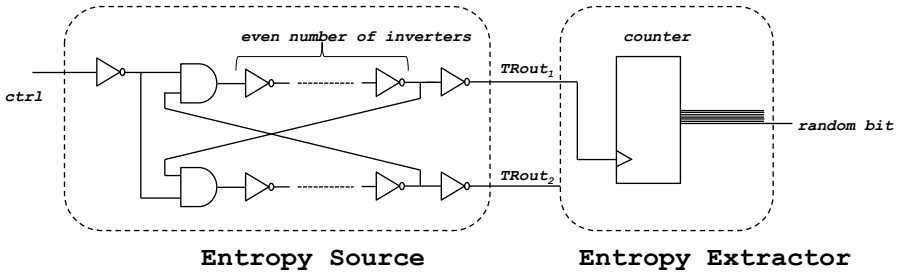
Components of a TRNG



- Source: physical effect with stochastic model
- Entropy extraction: A to D conversion
- Post processing: remove bias, correlation, etc
- Online (Health) tests

Example: TERO based TRNG

- Transition Effect Ring Oscillator – TERO [VD10]
  - Structure similar to RS/$\overline{RS}$ latch
  - Entropy source: oscillatory metastability
  - Entropy extractor: asynchronous counter
    Random bit = LSB of oscillation count

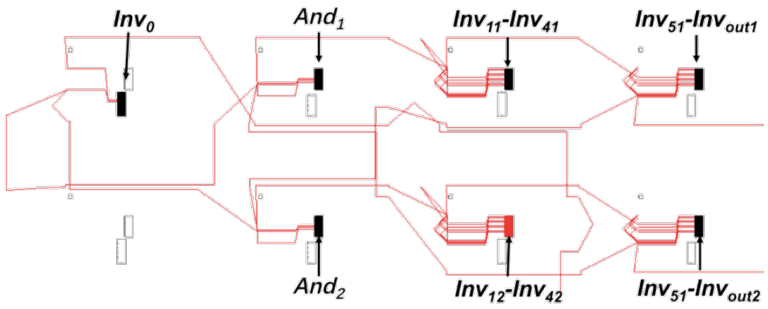


Eeasier said than done …

KU Leuven - COSIC | Croatia Summerschool - 47 | June, 2017

Our TERO implementation

- Atlys Board: Xilinx Spartan-6 LX45 FPGA
- Main challenges:
  - Synthesis optimizations: prevent element removal, reuse, duplication, etc.
  - Placement: direct LUT instantiation, user constraints (UCF)
  - Symmetric routing: manual process (FPGA editor)

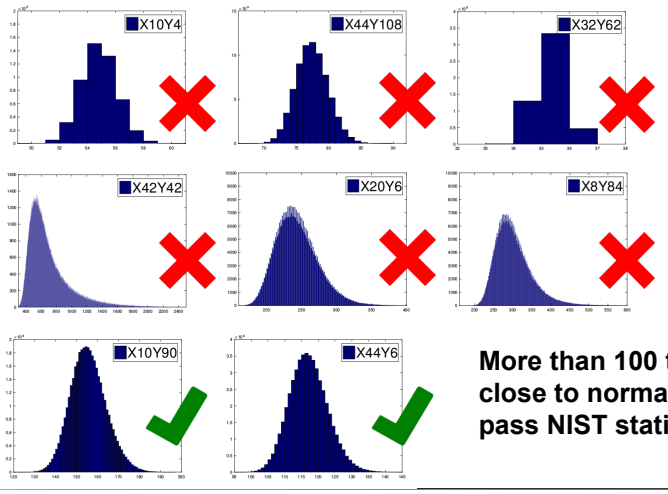


- Position of Inv_0 determines placement of circuit

KU Leuven - COSIC | Croatia Summerschool - 48 | June, 2017

TERO implementation & experiment

- Influence of placement on oscillation occurrence

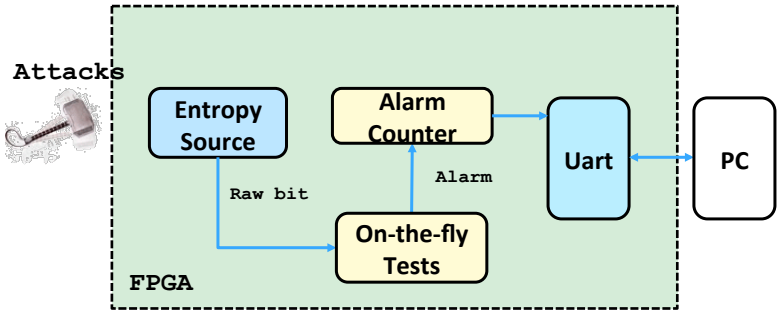


Very few transitions

Statistical defects

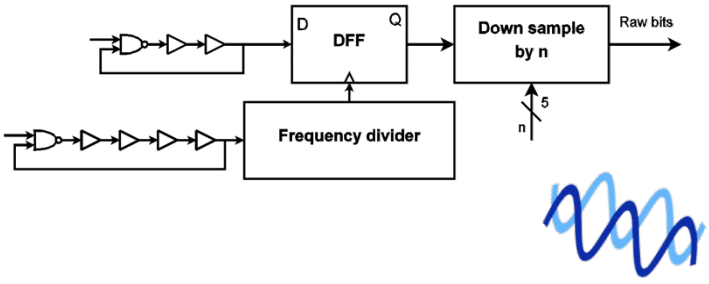
More than 100 transitions, close to normal distribution, pass NIST statistical tests

TOTAL: Lightweight on On-the-fly Attack detection



On the fly tests are TRNG specific

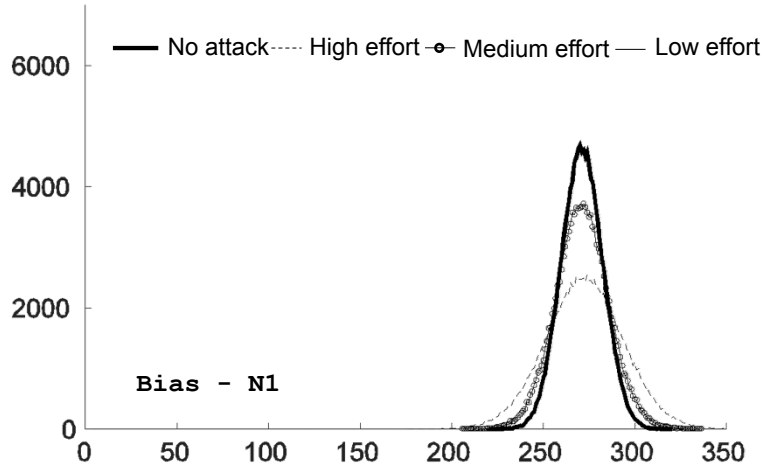
Case study: Elementary TRNG



Over sampling attack

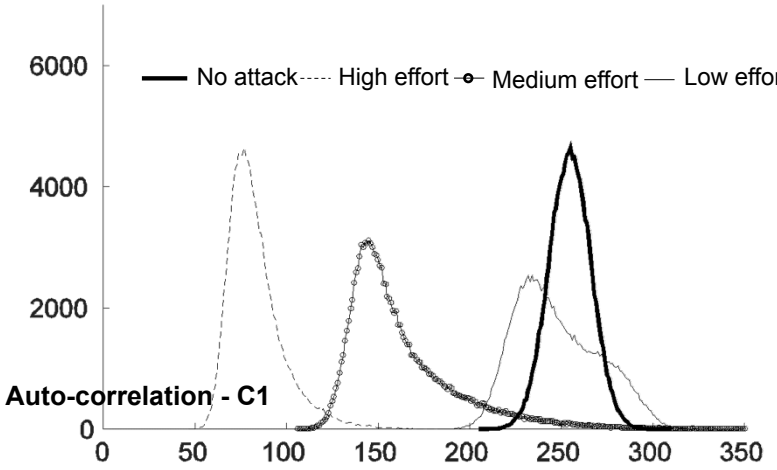
KU Leuven - COSIC | Croatia Summerschool - 51 | June, 2017

Case study: Elementary TRNG



KU Leuven - COSIC | Croatia Summerschool - 52 | June, 2017

Case study: Elementary TRNG



Challenge 1: select correct statistical feature
Challenge 2: develop light weight on-the-fly monitor for it

KU Leuven - COSIC | Croatia Summerschool - 53 | June, 2017

Conclusions

- Efficient algorithms and arithmetic is only start
- HW efficiency and side-channel resistance equally important
- Hardware roots of trust:
  - Physically Unclonable Functions
  - Random Number Generation
  - Secure trusted computation
  - Secure storage
  - Post-quantum secure, side-channel attack resistant

European Research Council
Established by the European Commission

KU Leuven - COSIC | Croatia Summerschool - 54 | June, 2017