KU LEUVEN

COSIC



Hardware: an essential partner to cryptography

IACR Distinguished Lecture
Prof. Dr. Ir. Ingrid Verbauwhede
KU Leuven, COSIC

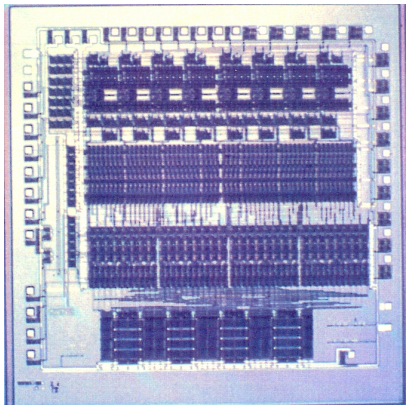
erc

Eurocrypt 2022 – June 1 2022

Slide acknowledgement: All past and present PhD students!

Background

- MS Micro-electronics with MS thesis on analog circuits, moved to digital for PhD
- my **very** first conference was **EUROCRYPT**
- "Security Considerations in the design and implementation of a new DES chip"



- Goal: link security and cryptography to hardware design, provide new research challenges

KU LEUVEN

Outline

- Position of cryptography in the design of embedded systems
  - Root of trust & secure composition
- Cryptography relies on hardware because it needs:
  - Performance (see DES chip)
  - Secure implementation: protection against side-channel, fault attacks
  - Secure key storage
  - Quality random number generators
- Challenges for crypto to work on
- Conclusions

3

KU LEUVEN

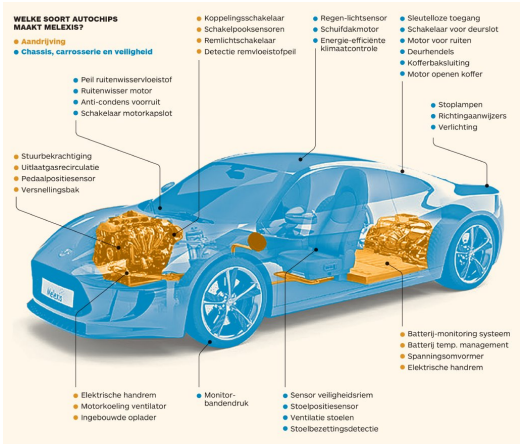
NEXT GENERATION EMBEDDED SYSTEMS

4

KU LEUVEN

Automotive

"Networked embedded systems interacting with the environment"



Today 58 Melexis chips in TESLA Model Y,
170 Melexis chips in Mercedes EQS

[De Tijd, February 2, **2022**]



- Networked → secure, authenticated communication, low latency
- Embedded → compact (no external memory), cheap, no batch processing
- Interacting with environment →
  - LOW latency
  - Compact
- Resistant to attacks

5

KU LEUVEN

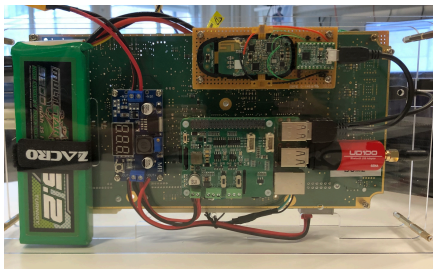
How to evaluate security? Where to start?



Tesla Model X key fob (2020)
https://youtu.be/clrNuBb3myE

Tesla Model S key fob (2018)
https://youtu.be/aVlYuPzmJoY

[Lennert Wouters, COSIC]



Passive Keyless Entry and Start System:

- Wireless challenge response system
- No Mutual authentication (model S)
- Weak crypto (model S)
- Secure element, but problems with protocol (model X)
- Off the shelf radios and components

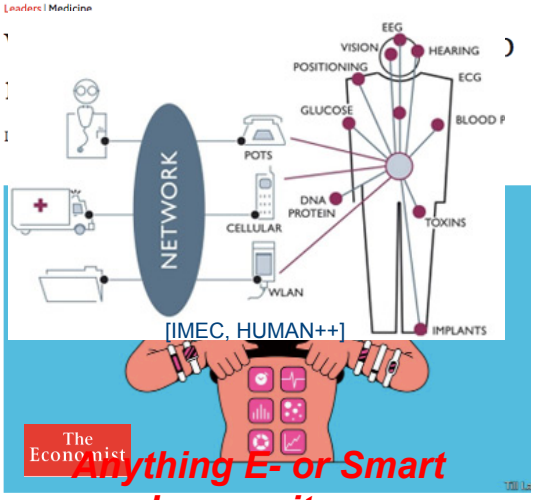
6

KU LEUVEN

Internet of Everything – IOT – Industry4.0 - E-…

- Internet of things
- E-health, e-commerce
- E-voting, e-…
- Smart grid
- Big data





Anything E- or Smart needs security

KU LEUVEN

TRUST AND TRUST BOUNDARIES

8

KU LEUVEN

Trust Definition

Trust (R. Anderson in "Security Engineering", after NSA):

- "Trusted system or component is one whose failure can break the security policy, while a trustworthy system or component is one that won't fail."

Trust (Trusted Computing Group):

- "An entity can be trusted if it always behaves in the expected manner for the intended purpose."

Loosely stated: if trusted system or component fails, then bad things can happen.

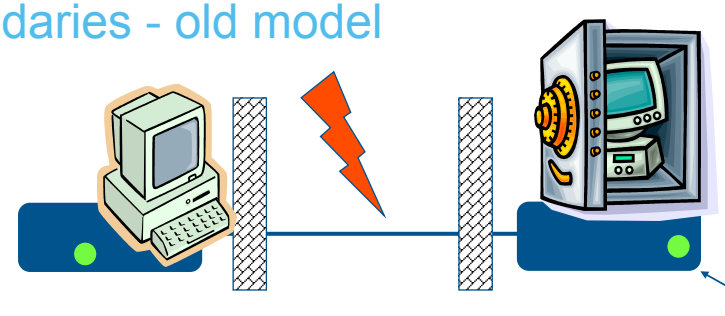
Goal of security: **minimize** what needs to be trusted

How does cryptography fit in this context?

9

KU LEUVEN

Trust boundaries - old model



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

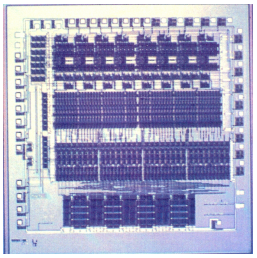
Focus on efficiency

10

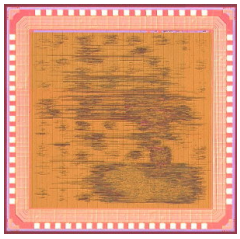
KU LEUVEN

DES, AES, ECC, SABER dedicated ASICs

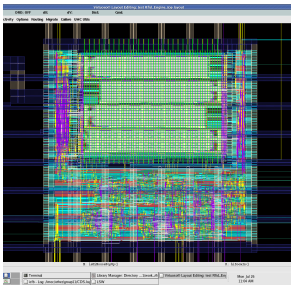
- Performance: what is feasible, throughput, latency, power (cooling), energy (battery lifetime) etc.



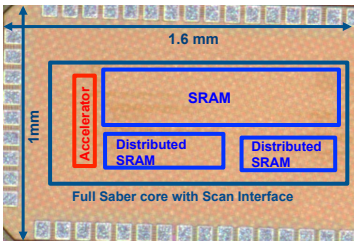
DES



Rijndael



ECC



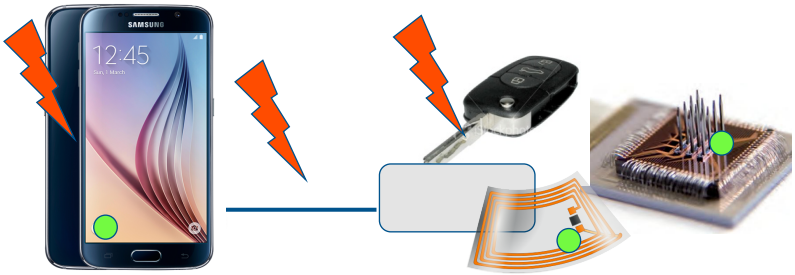
Saber

- Next: light weight crypto, FHE, …

11

KU LEUVEN

Trust boundaries – current model



Current attack model (simplified view):

- Attack on channel between communicating parties and on components!
- Encryption and cryptographic operations in **gray** boxes
- Protect by strong mathematic algorithms and protocols
- Protect by secure implementations

Need secure implementations not only algorithms!

12

KU LEUVEN

Side-channel and fault attacks

- Many types of side-channel analysis
  - Power, Electro Magnetic (EM), Time,
  - Micro-architectural side-channel: cache, transient execution attacks
- Many types of fault or active attacks:
  - EM, laser, clock, voltage glitch, etc.
- Local or remote
- Combined attacks

13

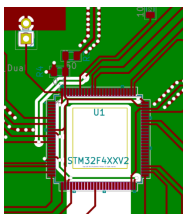
KU LEUVEN

Measurement methods

Contact power measurements:
-shunt resistors
-current probes

Cost: 150- 5000€

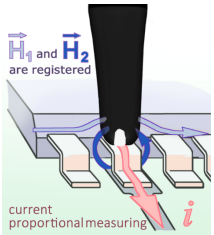
Freq: kHz – MHz range



Contactless power measurements:
-EM probes

Cost: 2000 - 25000€

Freq: kHz – GHz range

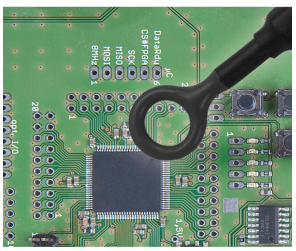


[picture credit: Langer]

EM measurements:
-EM probes

Cost: 2000 - 25000€

Freq: kHz – GHz range

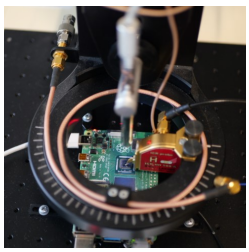


[picture credit: Langer]

Local EM measurements:
-EM probes

Cost: >50000€

Freq: MHz – GHz range



KU LEUVEN

Research challenges for cryptography

- Goal: introduce new research topics, improve existing ones

- Challenge 1: masking is hard in practice
- Challenge 2: masking is expensive
- Challenge 3: Possibilities of PUFs
- Challenge 4: Random number generation
- Challenge 5: new hardware challenges

15

KU LEUVEN

IMPLEMENTATION CHALLENGE - SIDE CHANNEL ATTACKS:

MASKING IS HARD

16

KU LEUVEN

Countermeasure: masking

- Types of masking
  - Boolean
  - Arithmetic
  - Inner product
  - Threshold
  - …

All start from similar leakage MODEL: Shares leak independently

All require randomness

- Two experiments:
  - Symmetric key: AES masking on micro controllers
  - Public key: Post-quantum masking of lattice based encryption

17

KU LEUVEN

Masking in practice is HARD

- Experiment: first order SW masked AES evaluated for:
  - Side-channel leakage
  - Timing
  - Randomness requirements

Paper title	Published venue	masking method
Provably Secure Higher-Order Masking of AES	CHES 2010	boolean
Higher order masking of look-up tables	Eurocrypt 2014	boolean
All the AES You Need on Cortex-M3 and M4	SAC 2016	boolean
Consolidating Inner Product Masking	Asiacrypt 2017	inner product
First-Order Masking with Only Two Random Bits	CCS-TIS 2019	boolean
Side-channel Masking with Pseudo-Random Generator	Eurocrypt 2020	boolean
Detecting faults in inner product masking scheme	JCEN 2020	inner product
Fixslicing AES-like Ciphers	TCHES 2021	boolean

[A. Becker, L. Wouters, Cosade 2022]

18

KU LEUVEN

Results [Cosade 2022]

- Key recovery with first order attack
- Incorrect TRNG instantiations
- Benchmarking issues
- Software bugs

Paper title	Published venue	masking method
Provably Secure Higher-Order Masking of AES	CHES 2010	boolean
Higher order masking of look-up tables	Eurocrypt 2014	boolean
All the AES You Need on Cortex-M3 and M4	SAC 2016	boolean
Consolidating Inner Product Masking	Asiacrypt 2017	inner product
First-Order Masking with Only Two Random Bits	CCS-TIS 2019	boolean
Side-channel Masking with Pseudo-Random Generator	Eurocrypt 2020	boolean
Detecting faults in inner product masking scheme	JCEN 2020	inner product
Fixslicing AES-like Ciphers	TCHES 2021	boolean

19

KU LEUVEN

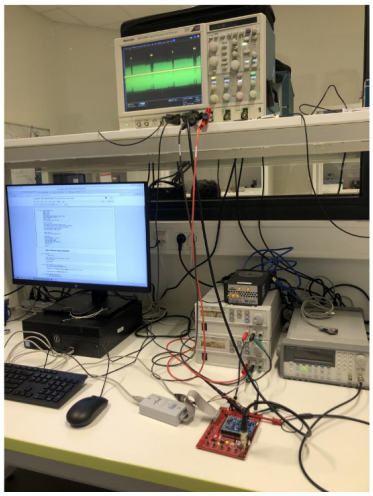
Correlation Power Analysis (CPA)

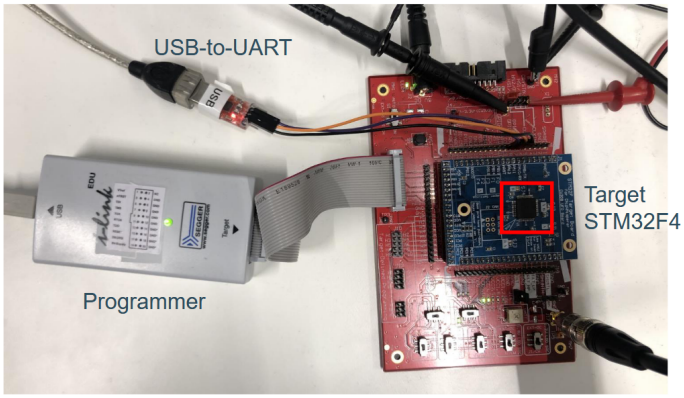
- All implementations compiled using given makefile
- Only inserted triggers
- Textbook first order CPA:
  - SBOX in or output
  - Hamming Weight leakage, or single bit when bitsliced
  - 20k traces
- No claims about the mathematical concepts or proofs

20

KU LEUVEN

Set-up in the lab





21

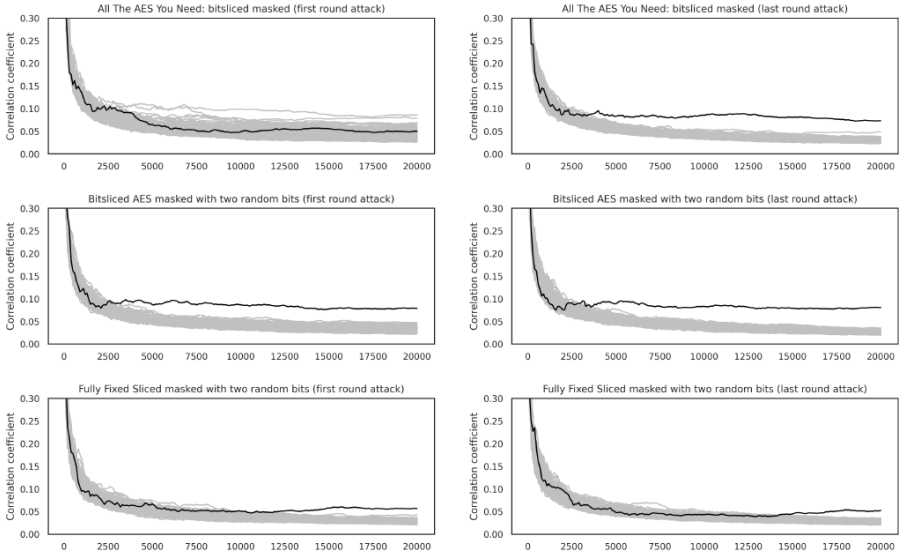
KU LEUVEN

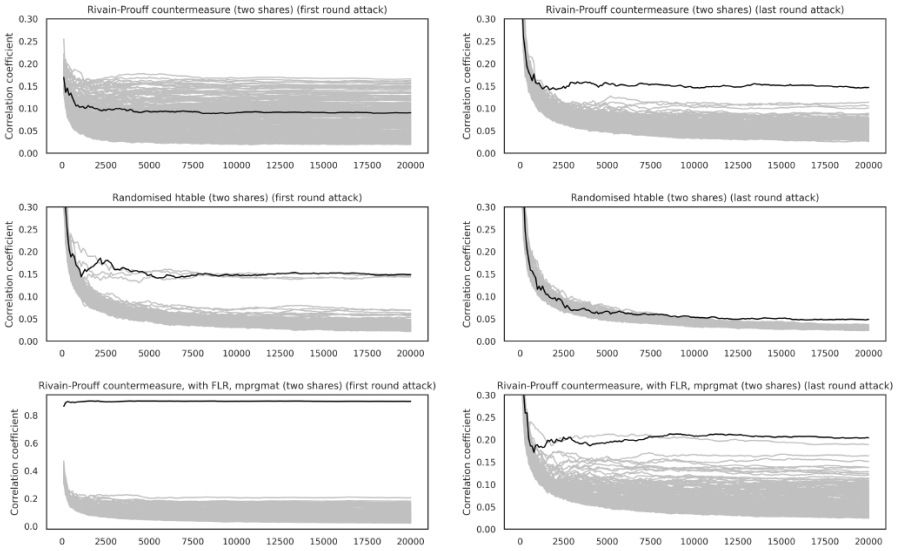
CPA results

AES Key recovery:
- Byte by byte
- correct byte stands out

to 255 other options

X-axis: number of samples
Y-axis: correlation coef





For more details see COSADE 2022

KU LEUVEN

Cause: violation of assumptions

- Assumption: shares leak independently
- Leakage caused by the microcontroller breaks this assumption
  - Assume share A is in r0
  - Move share B into r0 (and overwrite share A)
  - Information on A ⊕ B is leaked!
- Complex processors: transient execution
- Compiler optimizations
- Coupling through power and ground network
- Below 60nm CMOS ‘static’ leakage

KU LEUVEN

IMPLEMENTATION CHALLENGE - SIDE CHANNEL ATTACKS:

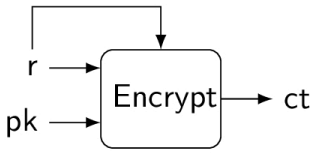
MASKING IS EXPENSIVE

25

KU LEUVEN

Lattice Based Post-quantum crypto (NIST)

- KEM = key generation, encapsulation, decapsulation
- CCA secure: Fujisaki – Okamoto transformation
- Similar for
  - Kyber
  - Saber

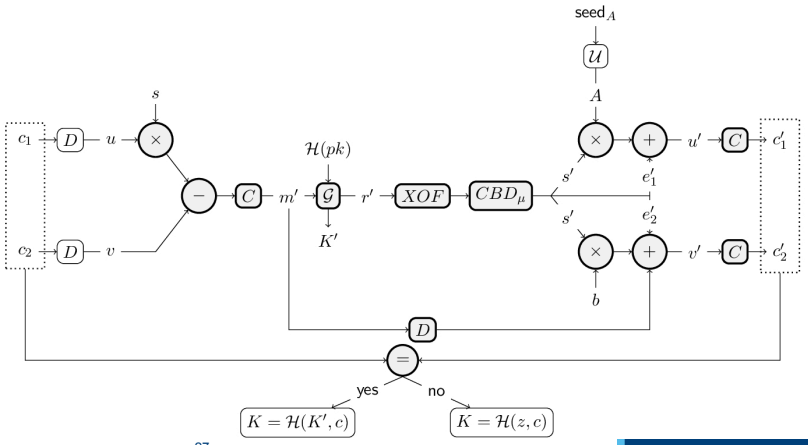


26

KU LEUVEN

Cost of decapsulation

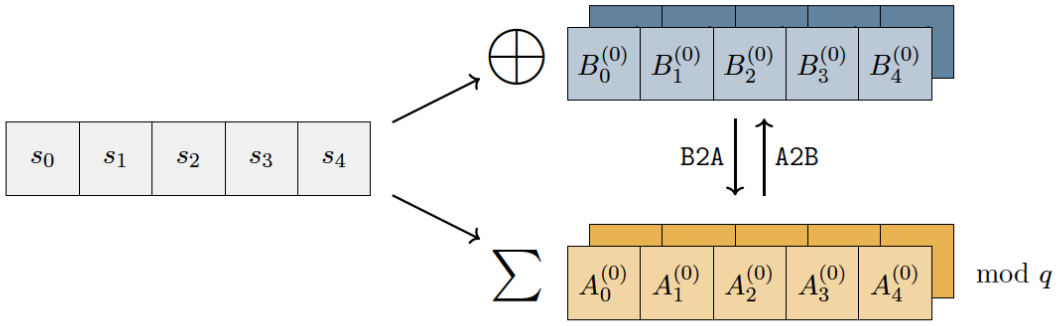
- Expensive parts: multiplication, hash, sampling
- Saber vs Kyber
  - Very similar
  - Power of two q= 2^{13} vs q= 3329
  - MLWR vs MLWE
    implicit vs explicit error addition



27

KU LEUVEN

Arithmetic and Boolean masking



Conversion is: Arithmetic to Boolean (A2B) or Boolean to Arithmetic (B2A)

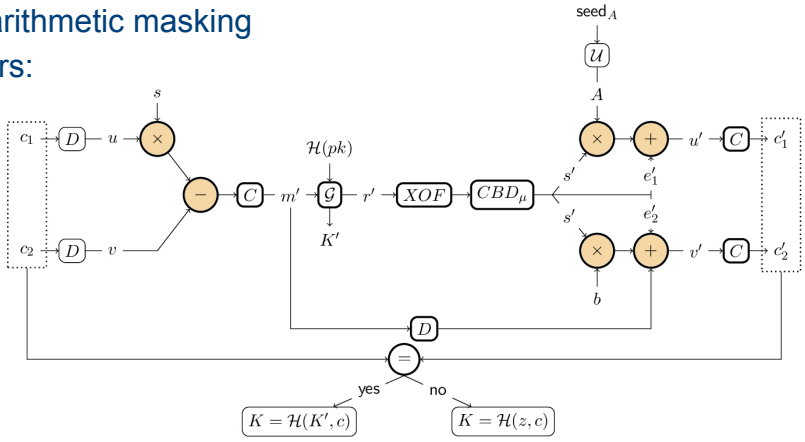
28

KU LEUVEN

Polynomial arithmetic

- Easy to protect with arithmetic masking
- Small overhead factors:
  - 1.7 to 2.0 (n=2)
  - 2.96 (n=3)

n = sharing factor



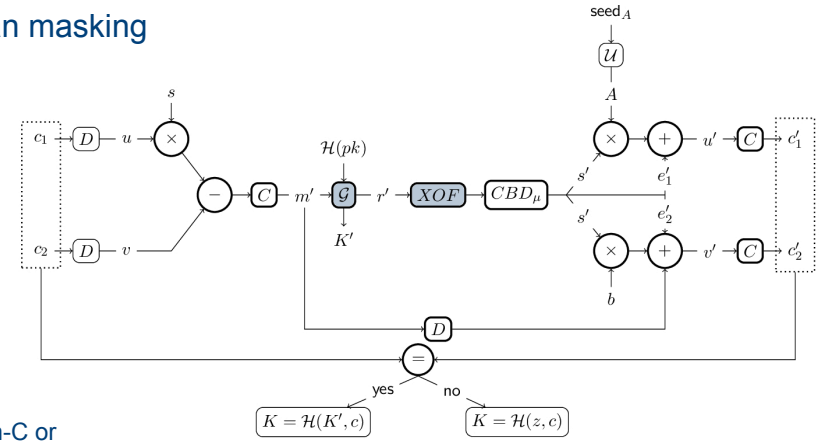
[BGR+21, BDK+21]

KU LEUVEN

SHA-3

- Protected with Boolean masking

- Overhead factors
- 5.9 to 9.26 (n = 2)
- 73.1 (n=3)



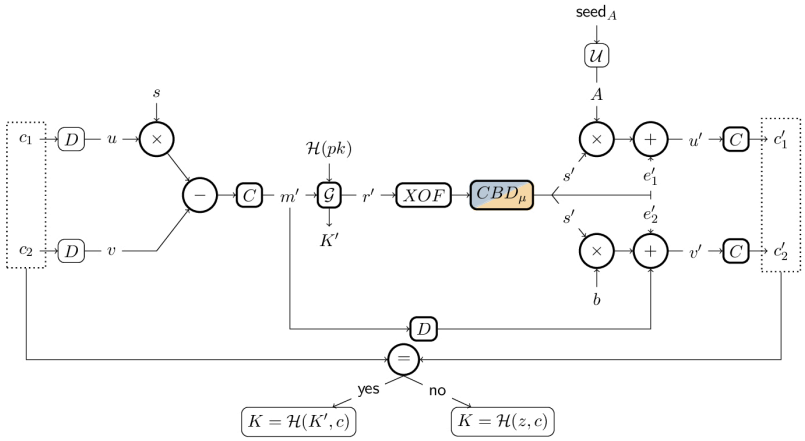
Depends if you compare to plain-C or optimized assembly

[Boolean masking: BDPVA10,BBD+16]

KU LEUVEN

Centered Binomial sampling

- Mix of A2B and B2A
- Expensive!
- Etc.



31

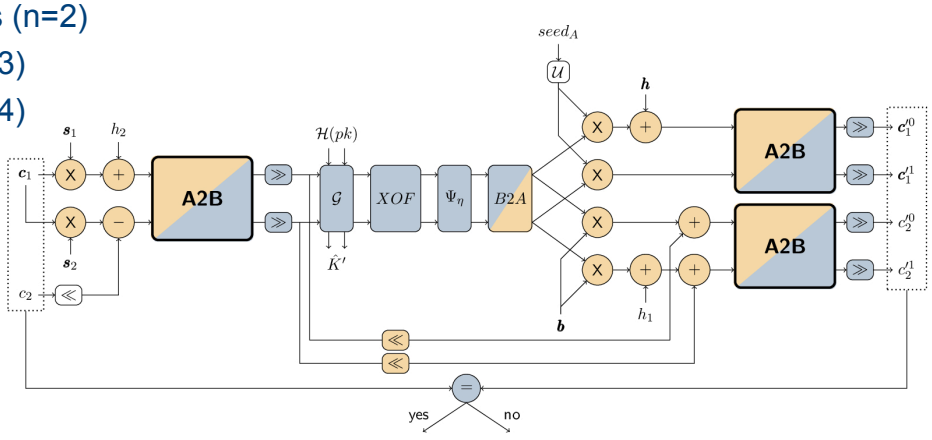
KU LEUVEN

One A2B conversion cost (Saber)

Requires bit-slicing

- 55-61 K cycles (n=2)
- 172-206 K (n=3)
- 302-365 K (n=4)

+ randomness



[ABV22, BC22]

32

KU LEUVEN

Masking is expensive

CPU cycles x1000 / Scheme	Unmasked	1st order n=2	2nd order n=3	3rd order n=4
Saber	773	3,011 (1x)	5,534 (1x)	8,591 (1x)
Kyber [2]	804	7,716 (2.56x)	11,880 (2.14x)	16,715 (1.94x)
COST	**1x**	**3.9x – 9.6x**	**7.2x – 14.8x**	**11.1x – 20.8x**
Random bytes		**12 KB**	**42 KB**	**90 KB**

- Unmasked Kyber/Saber similar cost
- Masked Kyber more expensive vs Saber
  - Power of two
  - Rounding vs error sampling
- Masking is expensive AND requires randomness

Platform: ARM Cortex M4
Framework: PQM4
Compiled: arm-none-eabi-gcc
Version: 9.2.1

33

KU LEUVEN

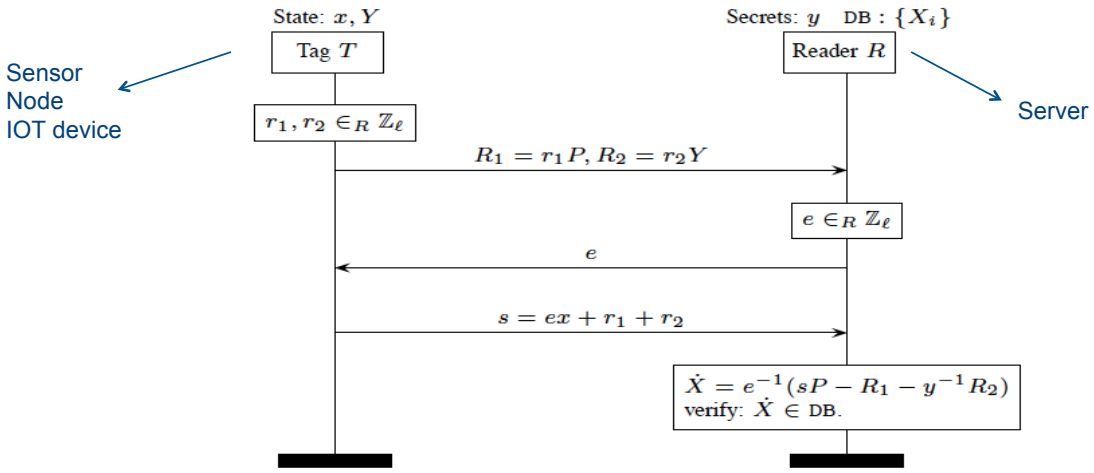
CHALLENGE 3: RANDOMNESS

TRUE RANDOM NUMBER GENERATION
PHYSICALLY UNCLONABLE FUNCTIONS (PUFS)

34

KU LEUVEN

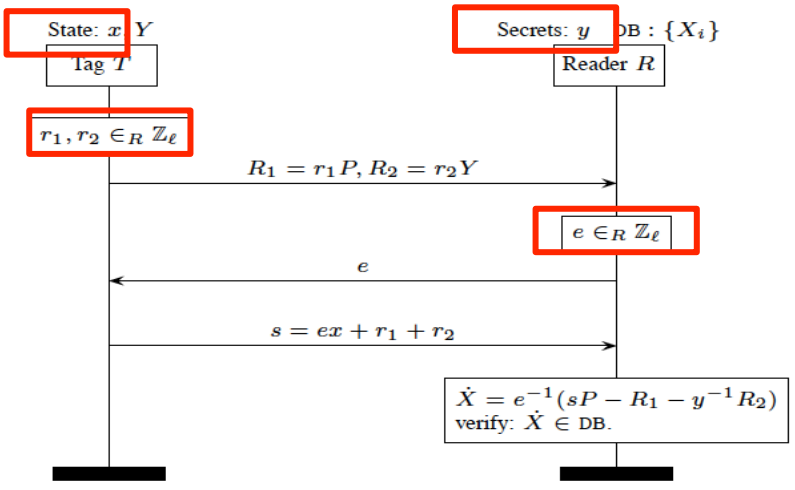
How the crypto protocol paper sees it:



Source: J.Hermans, et al., "Proper RFID Privacy: Model and Protocols," IEEE Trans on Mobile computing, 2014

KU LEUVEN

Protocol relies on secrets and random numbers

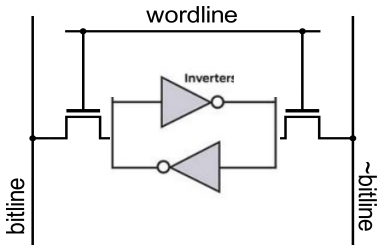


Source: J.Hermans, et al., "Proper RFID Privacy: Model and Protocols," IEEE Trans on Mobile computing, 2014

KU LEUVEN

Two ends of randomness

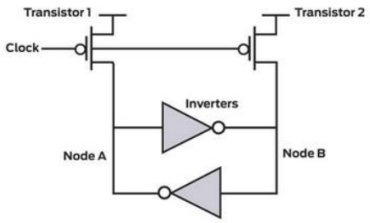
- Fixed randomness, stable over time



Physically Unclonable Function

Used: secret key
Challenge: time varying noise

- Randomness changing over time



True Random Number Generation

Used: freshness
Challenge: fixed noise

37

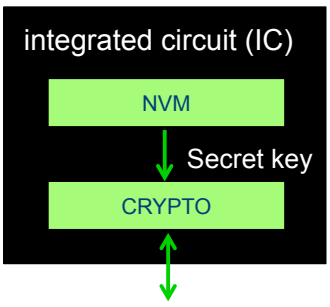
KU LEUVEN

Fixed randomness - Silicon PUFs

Purpose: CHEAP unique key or ID generation

Replacement for more expensive secure non-volatile memory (NVM)
- EEPROM/Flash
- Fuses
- Battery-backed SRAM

Embedded context:
- Physical attacks
- Constraints on cost and resources

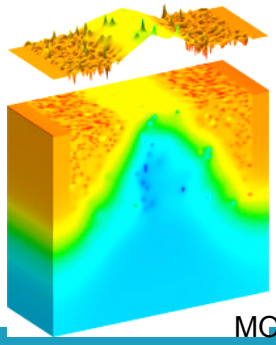


[J. Delvaux]

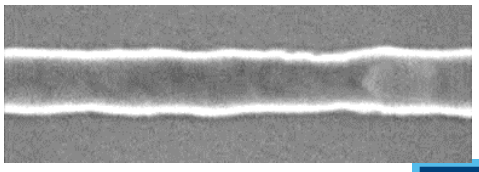
KU LEUVEN

Variability is inherently presented in ICs

- Variability in transistors and interconnect
- In general undesired – except for PUFs
- Random dopant fluctuation
- Line edge/width roughness



MOSFET



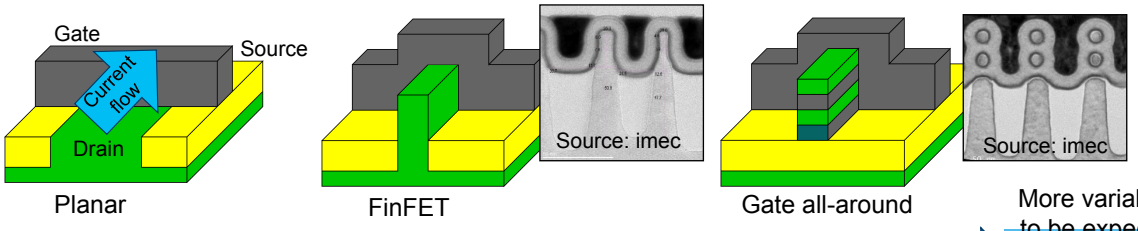
Interconnect

KU LEUVEN

39

More opportunities brought by scaling

- Even more challenging to manufacture identical devices in scaled technologies
  - Moore's Law
  - 40nm → 28nm →16nm → 7nm → ...
- More variability comes from:
  - More processing steps, new materials
  - Decreased size (e.g. 2nm difference → **5%** in 40nm and **30%** in 7nm)



Planar FinFET Gate all-around

More variability to be expected

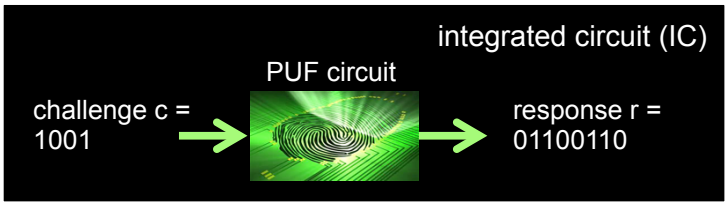
Transistor design roadmap

KU LEUVEN

40

Model: PUF (F = Function)

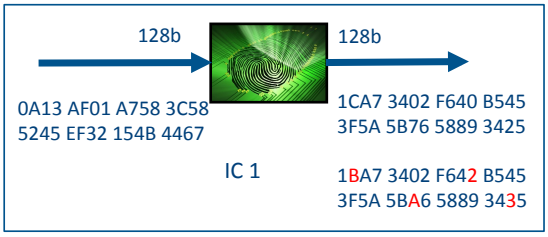
- Binary input & binary output
  - Therefore, easy of integration with other systems
  - Input = challenge; output = response
  - **C**hallenge-**R**esponse **P**airs (CRPs)
  - Easy to evaluate

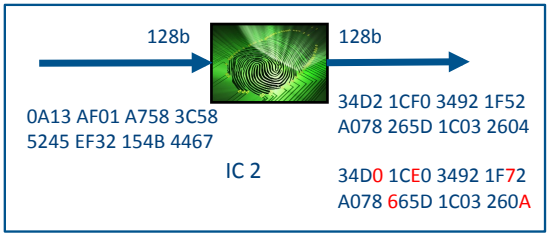


[J. Delvaux]

KU LEUVEN

The almost ideal PUF





Chip-dependent binary function with noisy output

Evaluation 1

≈ 1-15% noise

Evaluation 2

Evaluation 1

Evaluation 2 ≈ 1-15% noise

Unique
Unpredictable
Unclonable
Intrinsic
Tamperproof
Stable
…

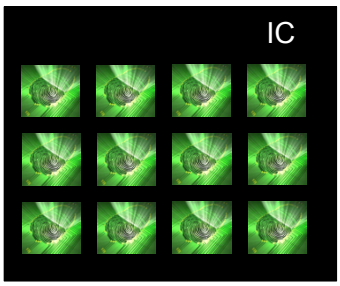
IDEAL PUF is without noise

KU LEUVEN

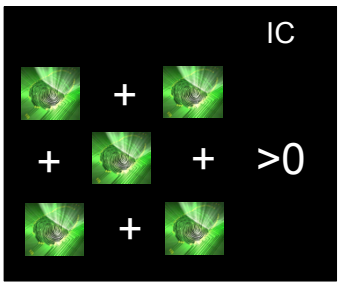
PUF (F = Function)

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

Key PUF



Authentication PUF



[J. Delvaux]

KU LEUVEN

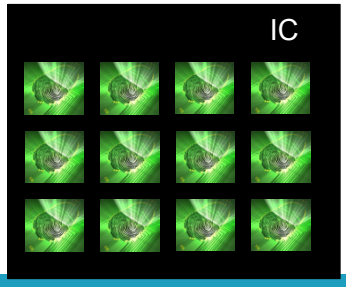
Key Generation PUF (aka weak) = 1 output

- 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
- E.g., SRAM PUF

BADLY chosen terminology

- Typical application: key generation

E.g. 128-bit AES



[J. Delvaux]

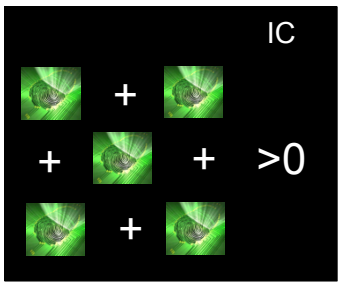
KU LEUVEN

Authentication PUF (aka Strong)

- Mathematical operations
- E.g., sum of delays, currents, voltages, frequences etc.
- Can produce a gazillion of response bits (2^{128})
- Low-quality bits: highly correlated, low-entropy, mostly broken

BADLY chosen terminology

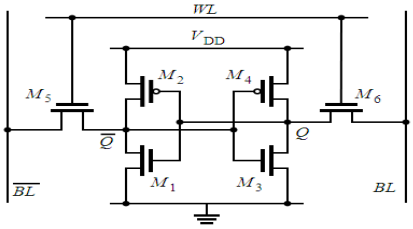
- E.g., arbiter PUF
- Typical application:
- IC authentication



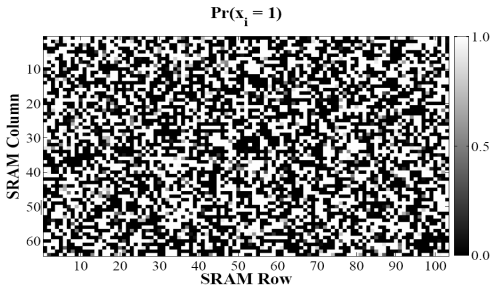
[J. Delvaux]

KU LEUVEN

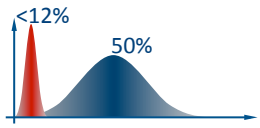
Key (Weak) SRAM PUF: Basics



6T CMOS SRAM Cell



Statistics:
- INTER distance between different PUFs
- INTRA distance between multiple readings same PUF



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

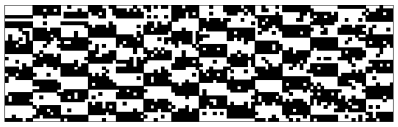
46

KU LEUVEN

PUF behavior of SRAM in commodity micro-controller

Black box approach (off the shelf micro-controllers)

- PIC16F1825

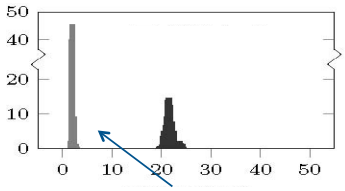


- STM32F100R8

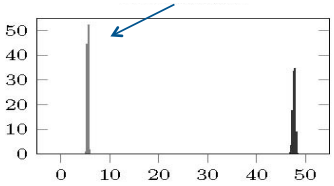


[PhD Anthony VH]

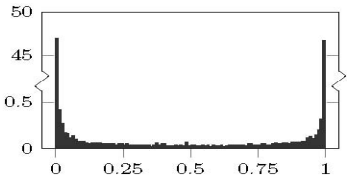
Within and between class HD (%)

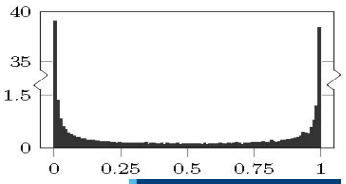


Intra



Average bit value (%)





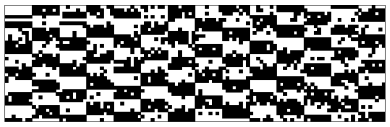
47

KU LEUVEN

PUF behavior of SRAM in commodity micro-controller

Black box approach (off the shelf micro-controllers)

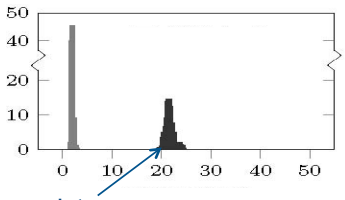
- PIC16F1825



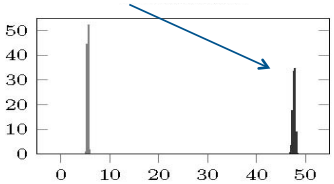
- STM32F100R8



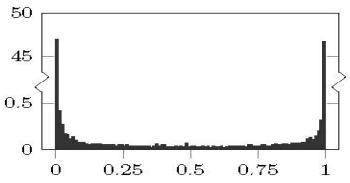
Within and between class HD (%)

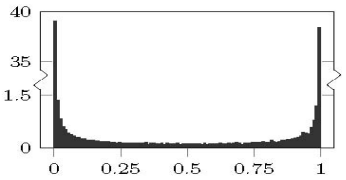


Inter



Average bit value (%)



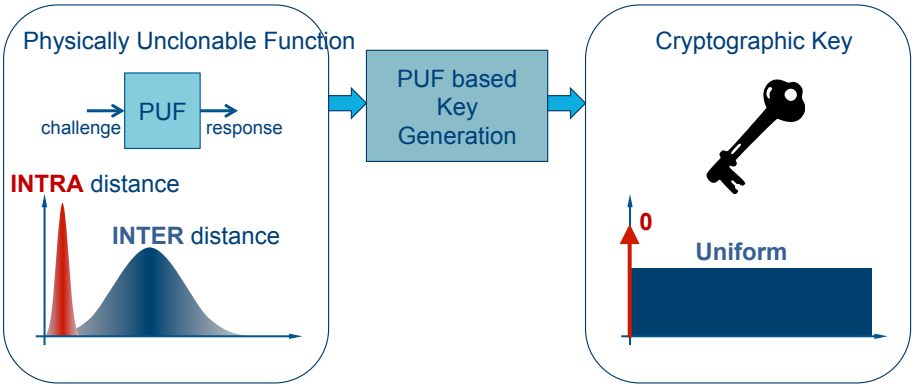


Needs post-processing to create key!

48

KU LEUVEN

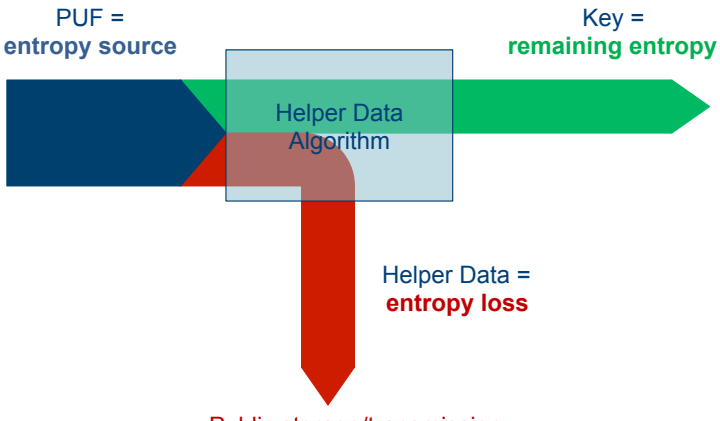
Cryptographic Key Generation: Basic Goals



KU LEUVEN

Cryptographic Key Generation: Entropy flow

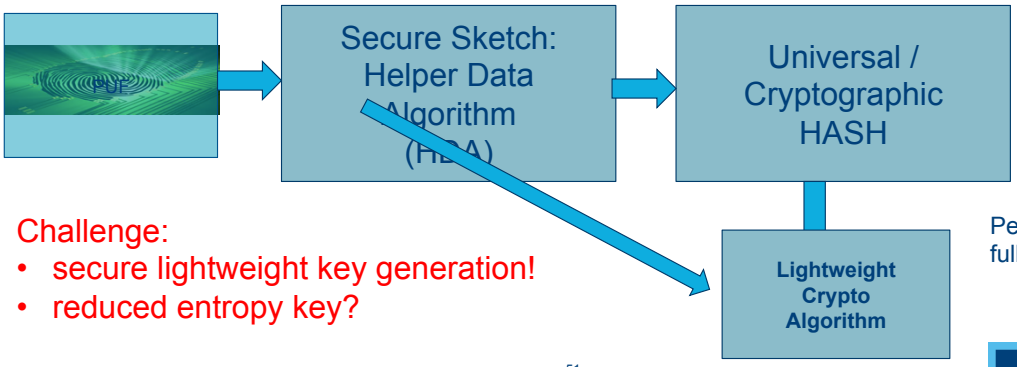
- Entropy is a measure for the "secrecy" of a value
  i.e., the uncertainty an adversary has about the value



KU LEUVEN

Light weight solution

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



Challenge:
- secure lightweight key generation!
- reduced entropy key?

Perfect 128 bit full entropy key

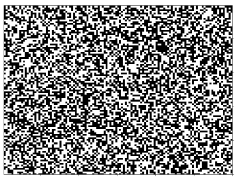
51

KU LEUVEN



CHALLENGE 4: COST OF TRUE RANDOM NUMBERS

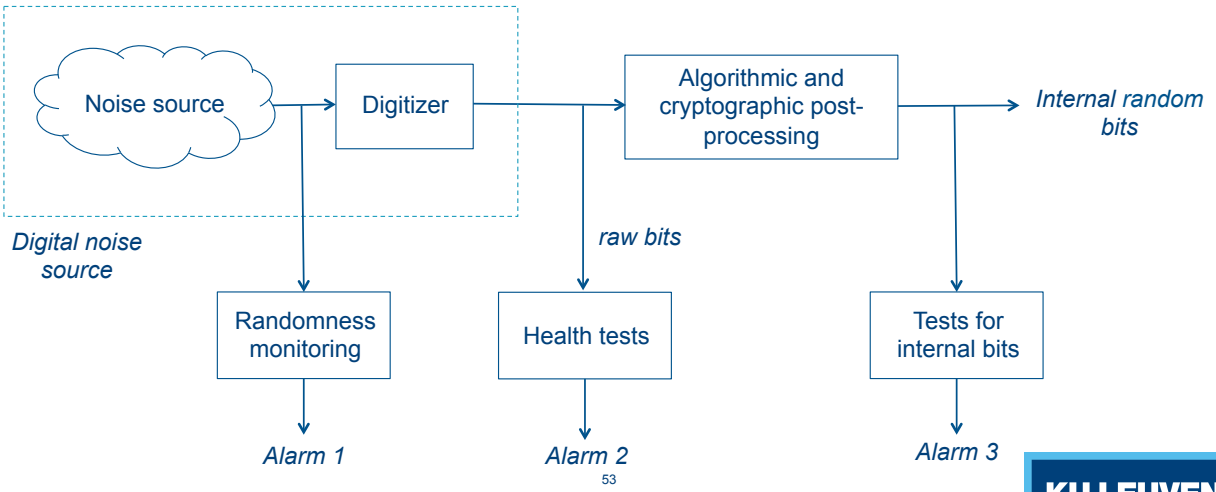
DESIGN AND ATTACKS ON TRNGS



52

KU LEUVEN

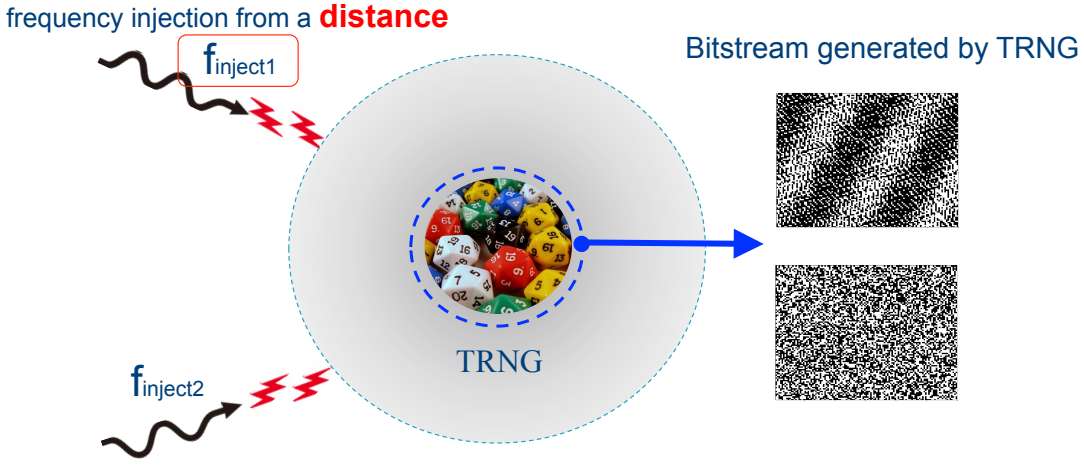
Architecture: True Random Number Generator



53

KU LEUVEN

IEMI: Intentional Electro Magnetic Injection

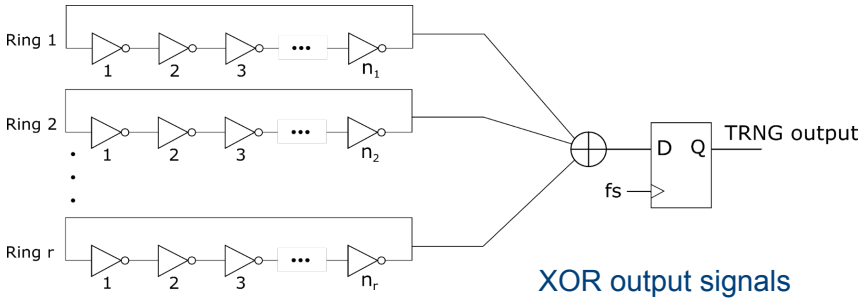


Goal: suppress jitter of Ring Oscillators

54

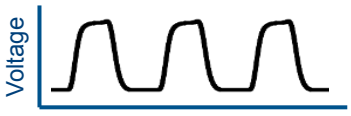
KU LEUVEN

Basic structure of RO-based TRNG



XOR output signals
sampled at arbitrary frequency

The output signal of an RO



55

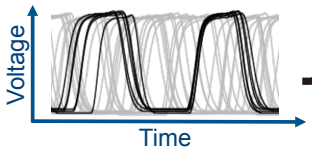
KU LEUVEN

Suppression of ROs' jitter

Jitter : variations in the transition timing of an RO in the time domain

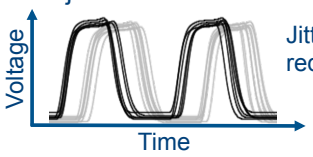
Normal RO

Non-locked state



$f_{inject1}$

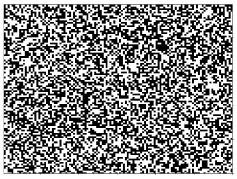
Inject Continuous Wave (CW)



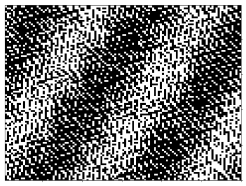
Jitter is reduced.

locked state

Normal TRNG output



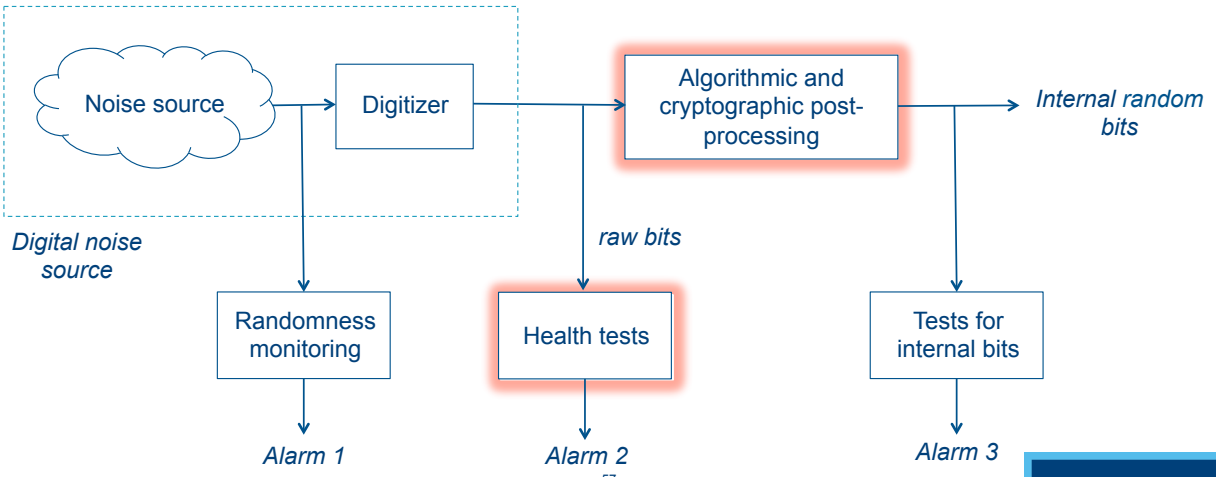
introduce CW to reduce randomness



56

KU LEUVEN

TRNG Tests and post processing

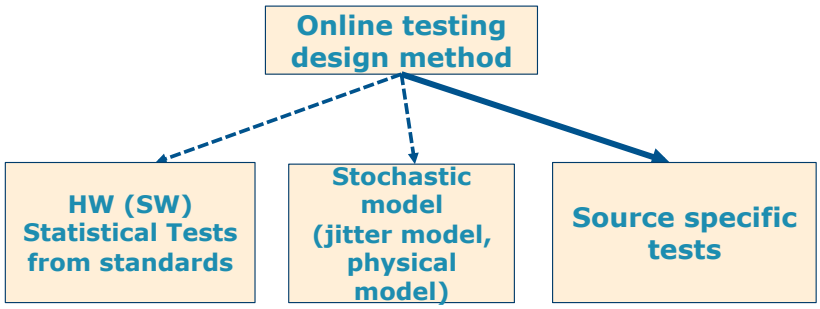


GERMAN BSI, AIS-31 or US NIST SP800-B/C

57

KU LEUVEN

Online tests: options



Challenges:

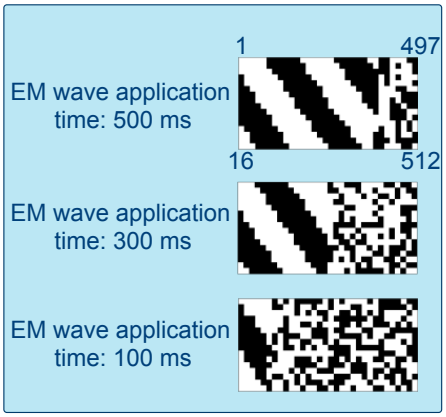
- Low latency
- Release data before it has been checked? Health bit?
- Memory requirements?

58

KU LEUVEN

Remote injection

- Countermeasure = bias detection counters
- Attacker tries to stay below the detection radar by manipulating inject on/off



59

KU LEUVEN

Conclusions – lessons learned

- "Provable secure masking" does not mean secure: theory and practice are different.
  - Practical evaluation in the lab of theoretical security is a must
  - Papers should include artifact evaluation.
- Masking and especially higher order masking are expensive, orders of magnitude
  - Less stringent, more realistic models
  - Reduce randomness requirements
  - Work with less perfect keys and less perfect random requirements
  - Trade-off security versus entropy in the key or random numbers

60

KU LEUVEN

Future work

- Performance: implement Fully Homomorphic Encryption
  - E.g. BASALISC presentation during FHE workshop
  - Take advantage of novel compute architectures
    - Multi-core, heterogeneous multi-core, combined CPU - FPGA
- Side-channel secure by design?
  - Resistant against combined fault/side-channel/micro-architectural attacks
  - Take into account new leakage models
- Take advantage of inherent variations in silicon technology
  - Fixed randomness: ID's or PUFs
  - Variable randomness: TRNG, approximate computing

61

KU LEUVEN

THANK YOU!

QUESTIONS?

Acknowledgements: All current and past PhD students,

62

KU LEUVEN

In operation and test – demo – back-up



https://www.youtube.com/watch?v=ajrYPRczMc0

63

KU LEUVEN