GDR SoC SiP

PUF and Trojans

Delay PUF overview

27 Novembre 2012

Jean-Luc Danger

Table of Contents

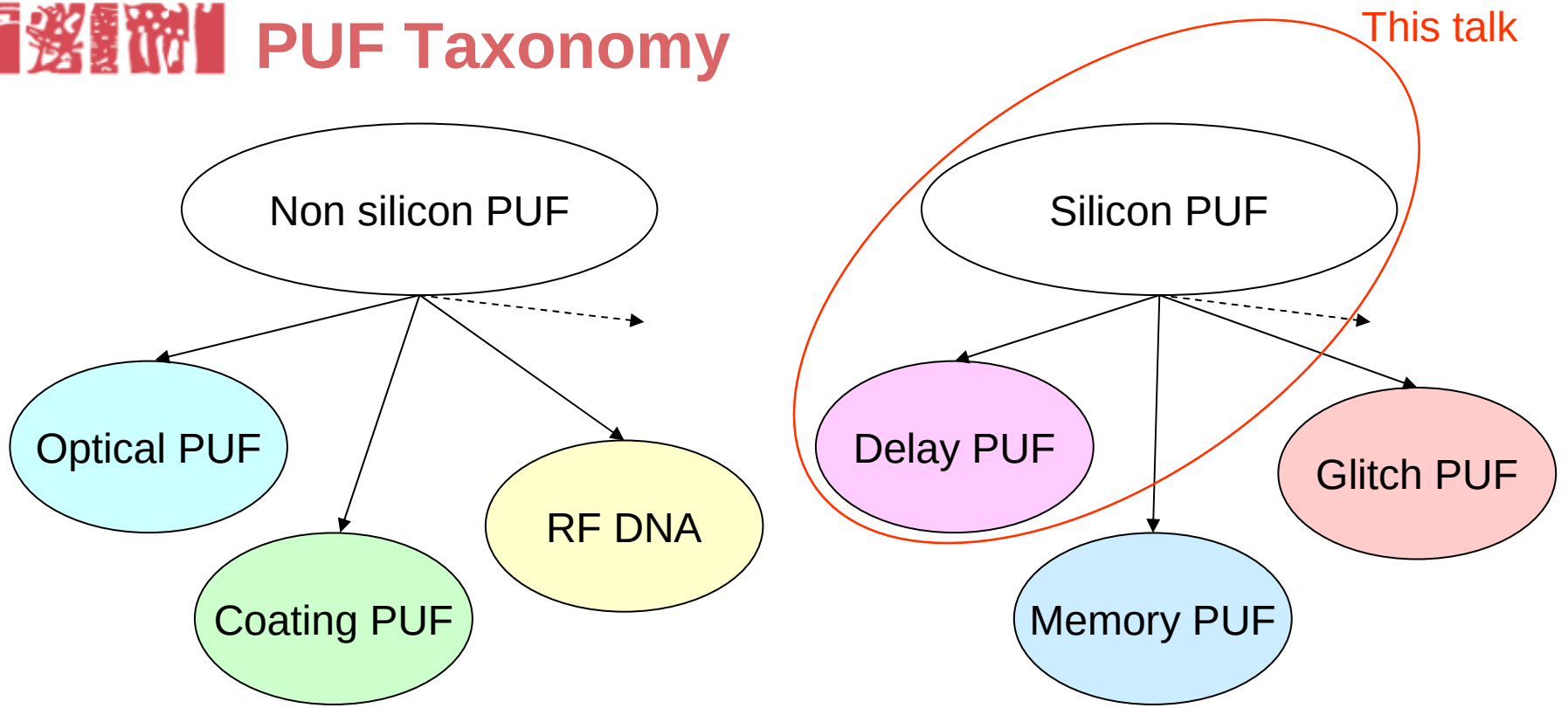
PUF Concept

- **Function returning a signature of the device**
  - Unclonable : not a mathematical function but
  - Physical function linked to material randomness
  - Introduced by Pappu in 2001
    - Optical PUF : Ravikanth S. Pappu. Physical One-Way Functions. PhD thesis, Massachusetts Institute of Technology, March 2001.
- **Basic applications**
  - Lightweight authentication
    - Challenge-Response Pair (CRP) Protocol
  - Private Key generation
- **Phases of use**
  - Enrollment (to do once)
  - Measurement or reconstruction

PUF properties

- **Uniqueness**
  - Each circuit has a unique signature
- **Steadiness**
  - The PUF response is always the same, whatever the noise and environment
- **Security**
  - Mathematically unclonable and unpredictable
  - Not sensitive to physical attacks (invasive, side-channel, fault injection)
- **Cost**
  - Not only the core but
  - Extra structure to make it steady and secure

PUF Taxonomy



Ravikanth S. **Pappu**. Physical One-Way Functions. PhD thesis, Massachusetts Institute of Technology, March 2001

Blaise **Gassend**, Dwaine E. Clarke, Marten van Dijk, and Srinivas Devadas. "Silicon physical random functions". In ACM Conference on Computer and Communications Security, pages 148–160, 2002.

Tuyls P., Schrijen G.J., Skori B., Van Geloven J., Verhaegh N., Wolters, R.: "Read-proof hardware from protective coatings". In: Cryptographic Hardware and Embedded Systems Workshop, LNCS, vol. 4249, pp. 369–383. Springer, 2006

Su Y., Holleman J., Otis B.: "A 1.6pj/bit 96% stable chip-id generating circuit using process variations". In:. ISSCC 2007. Digest of Technical Papers. IEEE, pp. 406-611, 2007

Gerald **DeJean** and Darko Kirovski. Rf-dna: Radio-frequency certificates of authenticity. In *CHES 2007, 9th International Workshop,Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *LNCS*, pages 346–363. Springer, 2007.

Daisuke **Suzuki** and Koichi Shimizu. 2010. The glitch PUF: a new delay-PUF architecture exploiting glitch shapes. In *Proceedings of the* CHES'10. Springer-Verlag, Berlin, Heidelberg, 366-382

Other PUF classification

- **Intrinsic vs non-intrinsic [1][2] , intrinsic if:**
  - Measurements are internal
  - Randomness comes from the manufacturing process
- **Strong vs weak [2] , strong if:**
  - Many challenges and
  - No possibility to build a model

(1). Jorge **Guajardo**, Sandeep S. Kumar, Geert Jan Schrijen, and Pim Tuyls. FPGA Intrinsic PUFs and Their Use for IP Protection. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 63–80. Springer, 2007.

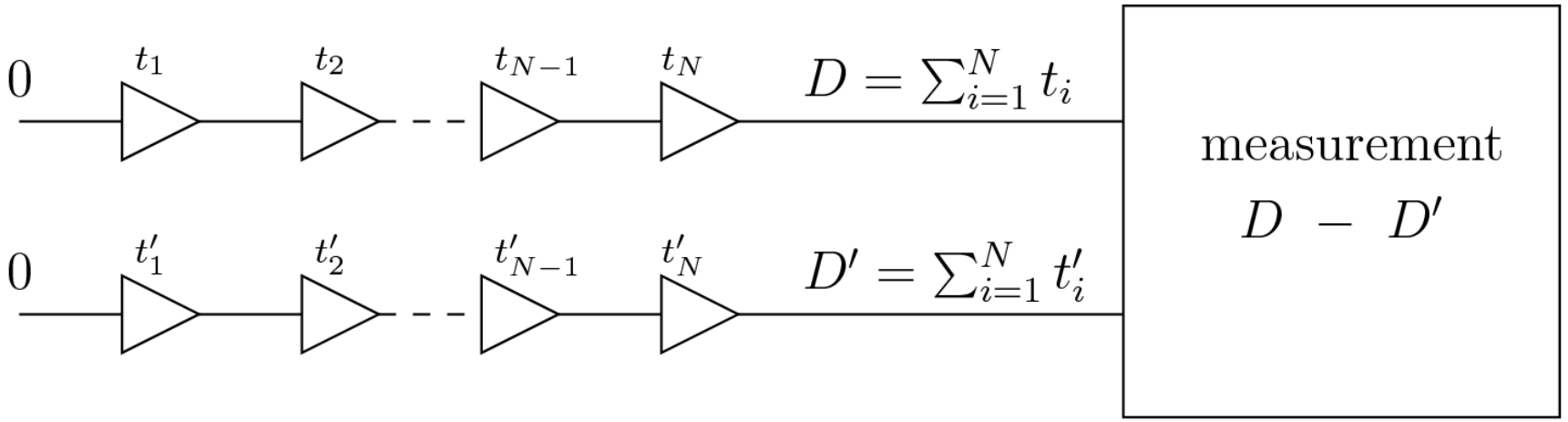
(2) R. **Maes.** *Physically Unclonable Functions: Constructions, Properties and Applications*. PhD thesis, KU Leuven, 2012.

SILICON PUF structures

- **Main Principles**
  - Delay measurement : **Delay PUF**
  - Memory state : **Memory PUF**
  - Propagation of glitches : **Glitch PUF**

Delay PUF

❑ Principle: Differential Delay measurement



Blaise **Gassend**, Dwaine E. Clarke, Marten van Dijk, and Srinivas Devadas. “Silicon physical random functions”. In ACM Conference on Computer and Communications Security, pages 148–160, 2002.

Delay PUF

- **Pros**
  - Good uniqueness
  - No technology constraints
  - Many challenges with controled delay elements
- **Cons**
  - Effort at P/R for a perfect balance
    - Of the two delay lines
    - Of the measurement element
  - Sensitive to Machine Learning attack
    - To Build the PUF model from a set of Challenge-Response
    - Rührmair et al. : Modeling Attack by Logistic regression*
  - Sensitive to noise and environment

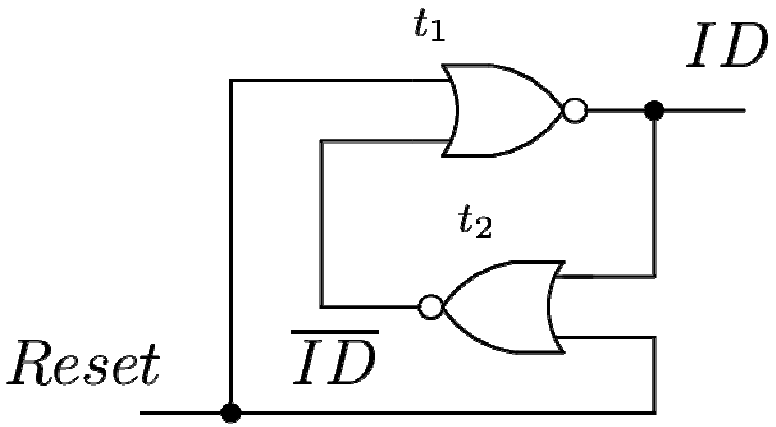
* Ulrich Rührmair, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. “Modeling attacks on physical unclonable functions”. In Proceedings of the 17th ACM

Memory PUF

More details given in the Talk of **Vincent Van der Leest** from INTRINSIC-ID

Principle

- Convergence towards a steady state from an unstable state :
  - Metastable
  - Power on



What happens when Reset goes to ‘0’ ?

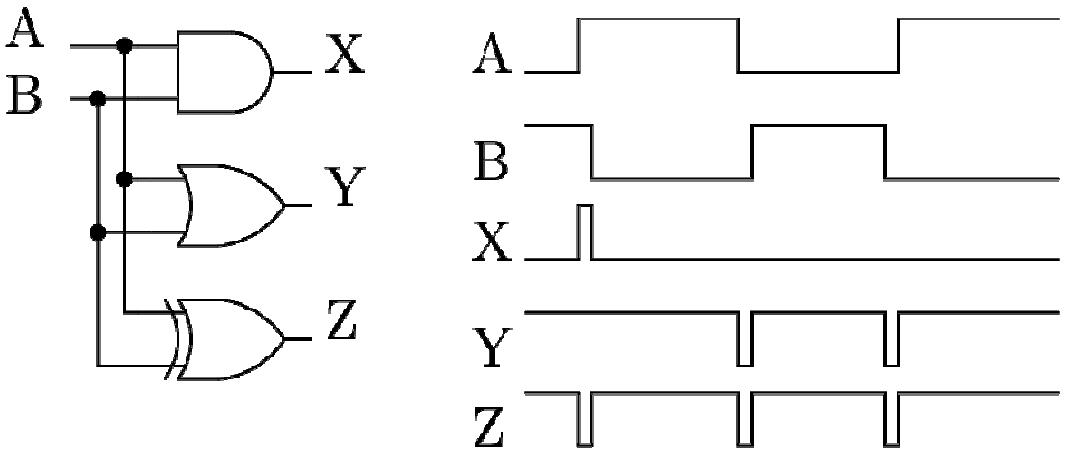
Su Y., Holleman J., Otis B.: “A 1.6pj/bit 96% stable chip-id generating circuit using process variations”. In:. ISSCC 2007. Digest of Technical Papers. IEEE, pp. 406-611, 2007

Memory PUF

- **Pros**
  - Good uniqueness
  - Implementable in any technology with
    - Non initialized SRAM
    - DFF, latches
    - Bus keepers
  - No ML attack
- **Cons**
  - Few challenges
  - Sensitive to noise and environment

Glitch PUF

- **Exploits the glitches of a non-linear Boolean function**



- **Main drawback**
  - Glitches hard to extract (lot of buffers + DFF)

Daisuke **Suzuki** and Koichi Shimizu. 2010. The glitch PUF: a new delay-PUF architecture exploiting glitch shapes. In *Proceedings of the* CHES'10. Springer-Verlag, Berlin, Heidelberg, 366-382

Brief comparison

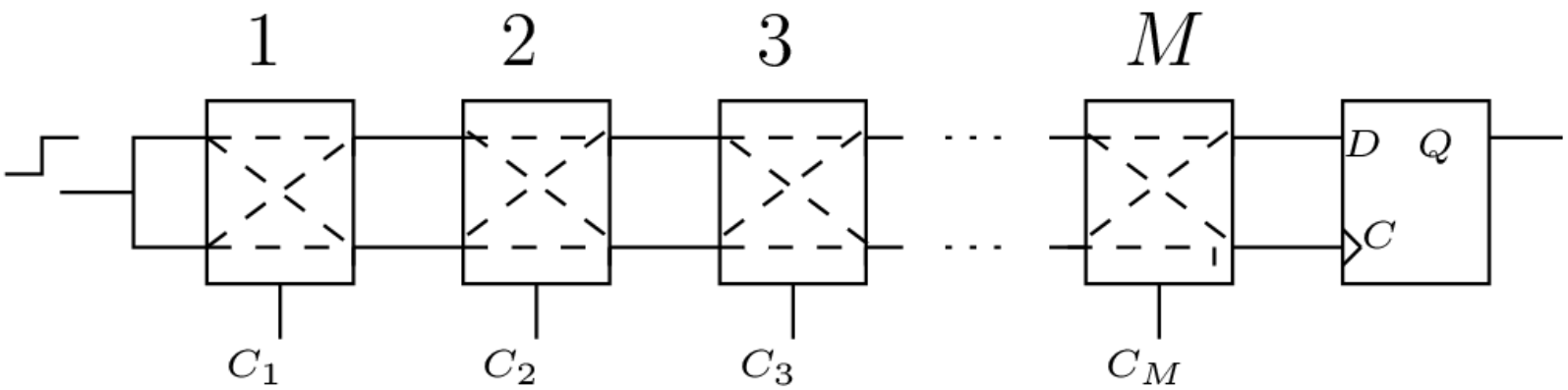
	Delay PUF	Memory PUF	Glitch PUF
Pros	• Unique • Many challenges • Implementable in any technology	• Unique • Implementable in DFF or non intialized memory	• Unique
Cons	• Sensitive to modeling attack • Needs effort at P/R • Not steady	• Few challenges • Not steady	• Not yet mature • Need complex hardware to extract glitches • Not steady

Table of Contents

- PUF overview
- Delay PUF structures
- Security and reliability

Delay PUF: Arbiter PUF

- **The first silicon PUF (Gassend et al.)**

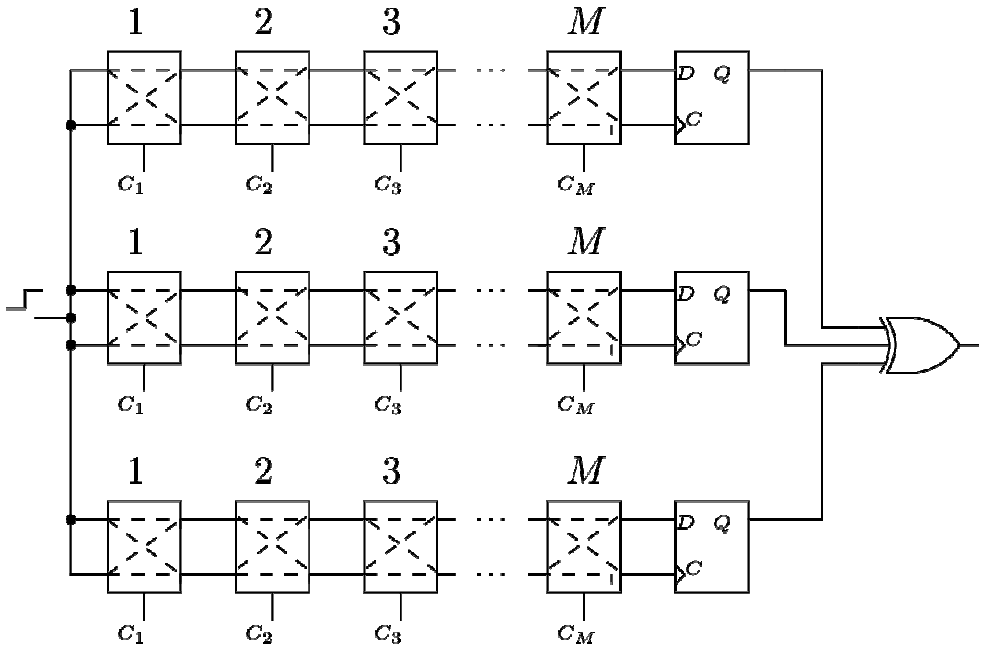


- Special care needed at P/R
- Many derivatives to enhance security
  - XOR , Lightweight PUF, FF-PUF

B. Gassend, D. Lim, D. Clarke, M. Van Dijk, and S. Devadas. Identification and authentication of integrated circuits. Concurrency and Computation: Practice & Experience, 16(11):1077–1098, 2004

XOR arbiter PUF

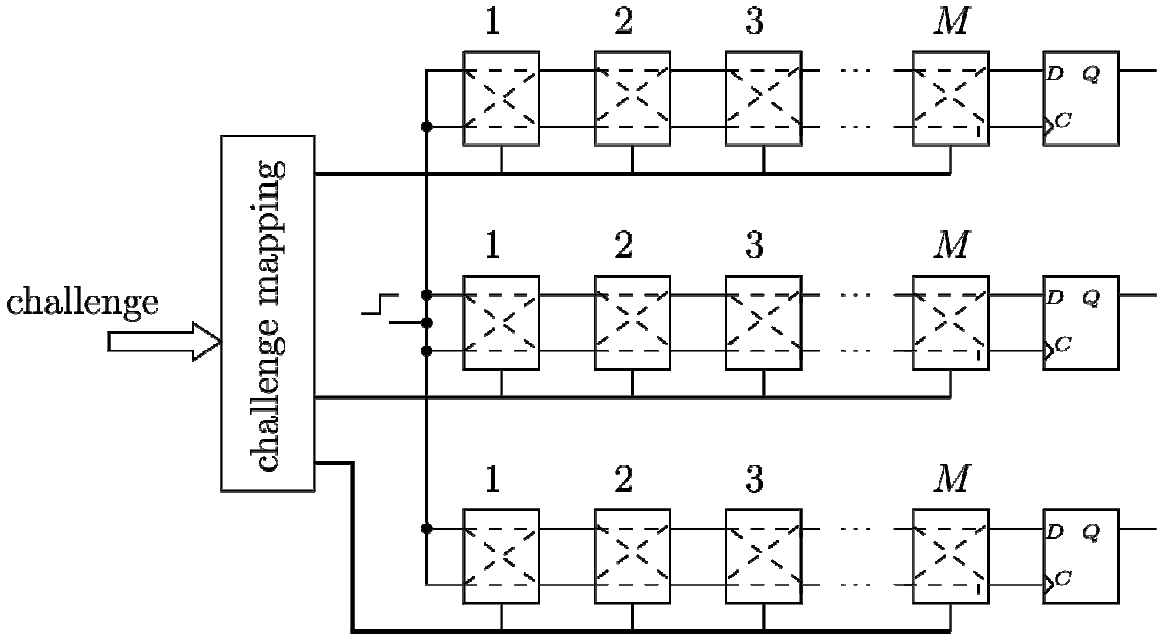
- **Proposed by Suh et al. to avoid ML attack**
  - N Arbiter PUF Xored



G. Edward Suh and Srinivas Devadas. “Physical unclonable functions for device authentication and secret key generation”. In DAC, pages 9–14, 2007.

Lightweight secure PUF

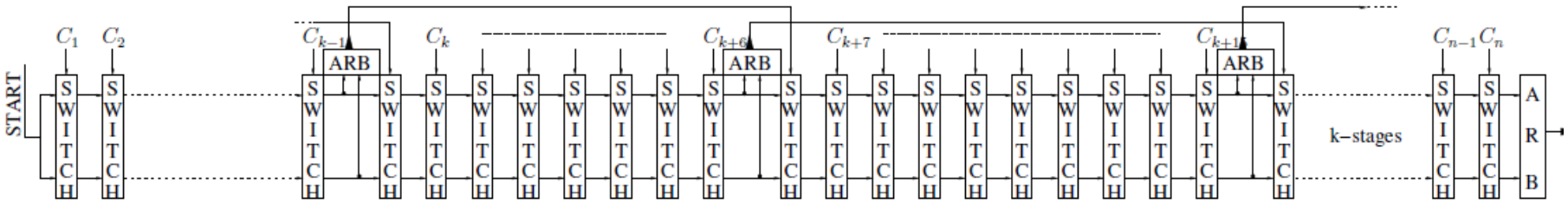
- **Proposed by Majzoobi et al. to increase robustness**
  - N arbiter PUF with specific challenge mapping



Mehrdad Majzoobi, Farinaz Koushanfar, and Miodrag Potkonjak. “Lightweight secure pufs”. In Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, ICCAD ’08, pages 670–673, Piscataway, NJ, USA, 2008. IEEE Press.

Feed-Forward PUF

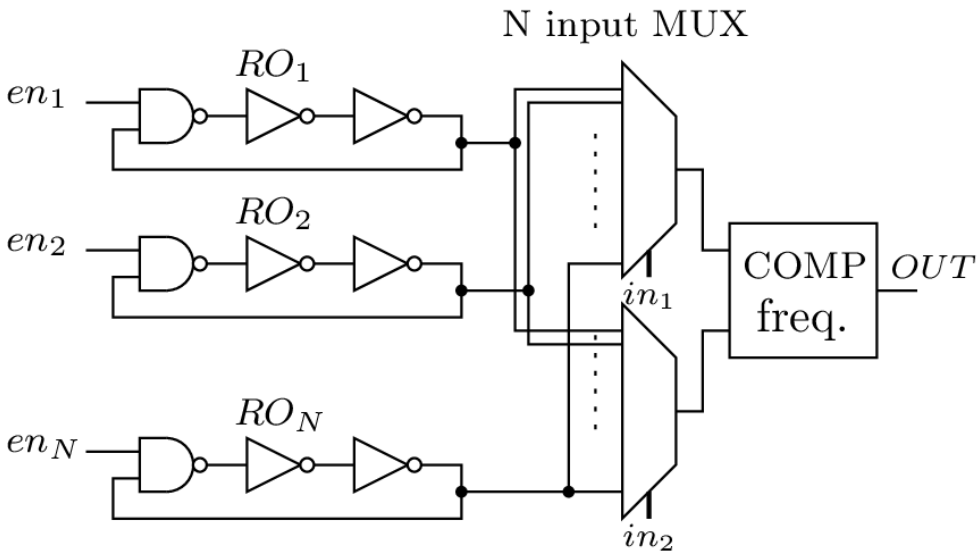
- **Proposed by Gassend et al. to fight ML attacks**
  - Some challenge bits are generated by intermediate arbiters



B. Gassend, D. Lim, D. Clarke, M. Van Dijk, and S. Devadas. “Identification and authentication of integrated circuits”. Concurrency and Computation: Practice & Experience, 16(11):1077–1098, 2004.

Ring Oscillator PUF

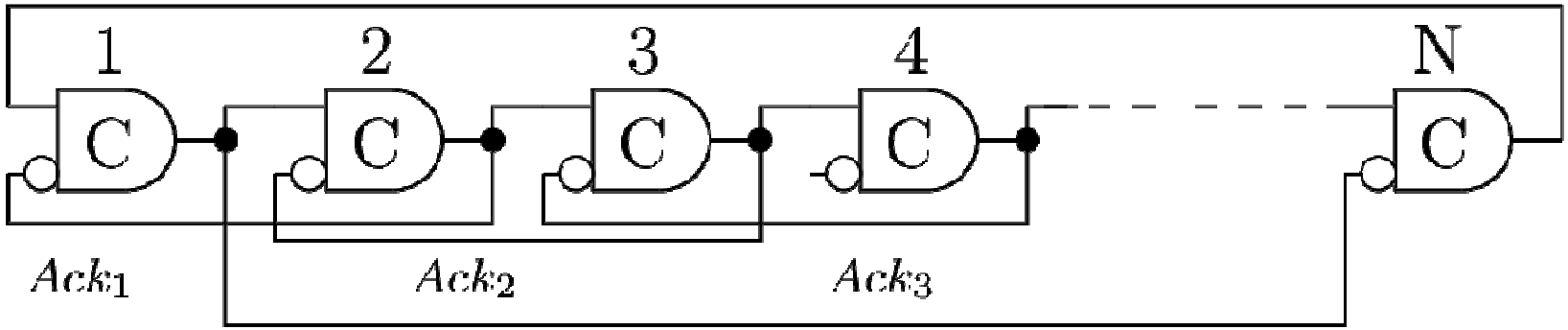
- **Introduced by Suh et al**
  - Identical Ring Oscillators are compared pairwise



G. Edward Suh and Srinivas Devadas. “Physical unclonable functions for device authentication and secret key generation”. In DAC, pages 9–14, 2007.

ASYNC PUF

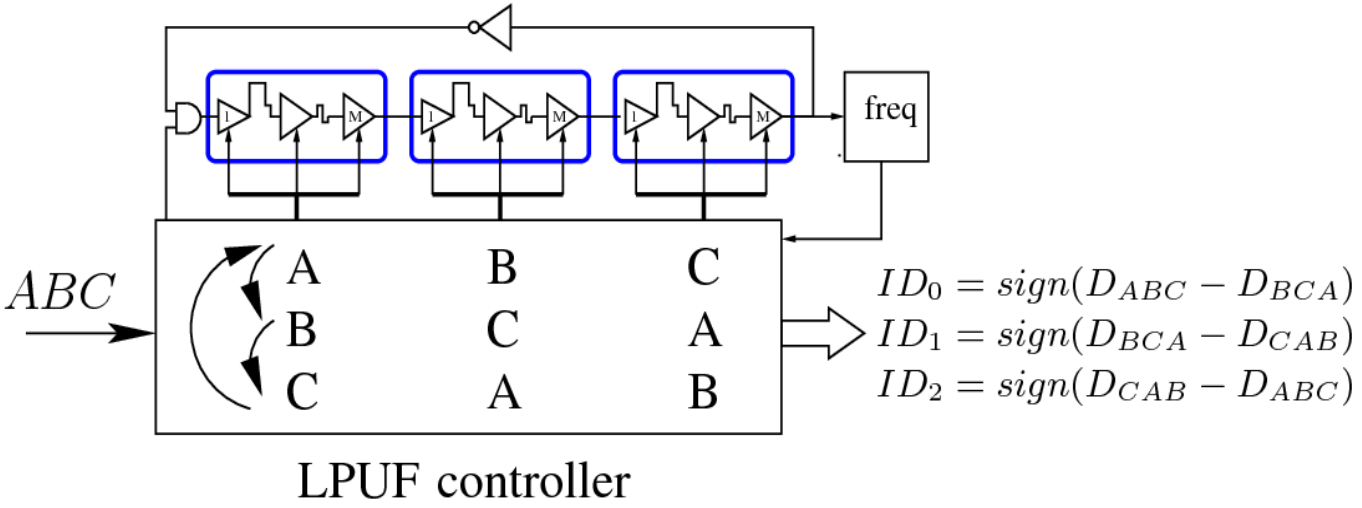
- **RO-PUF with better stability of the RO**
  - Self-synchronization (by C-element) limits the jitter propagation which accumulates in a classical ring oscillator



J. Murphy, A. Dziech, A.Czyżewski, "Asynchronous Physical Unclonable Functions ASYNC PUF", Multimedia Communications, Services and Security; Krakow 2012

Loop PUF

- **Multidimensionnal measurements (N>2)**
  - Many more challenges : very « strong » PUF
- **Easy to design**
  - Copy and paste the chain N times



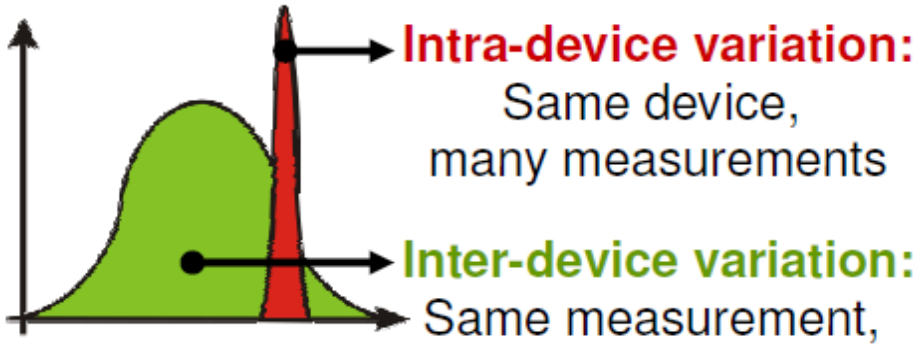
Zouha Cherif, Jean-Luc Danger, Sylvain Guilley et Lilian Bossuet, (2012), An Easy-to-Design PUF based on a Single Oscillator: the Loop PUF, "DSD", Izmir.

Table of Contents

- PUF overview
- Delay PUF structures
- Security and reliability

PUF Reliability (or steadiness)

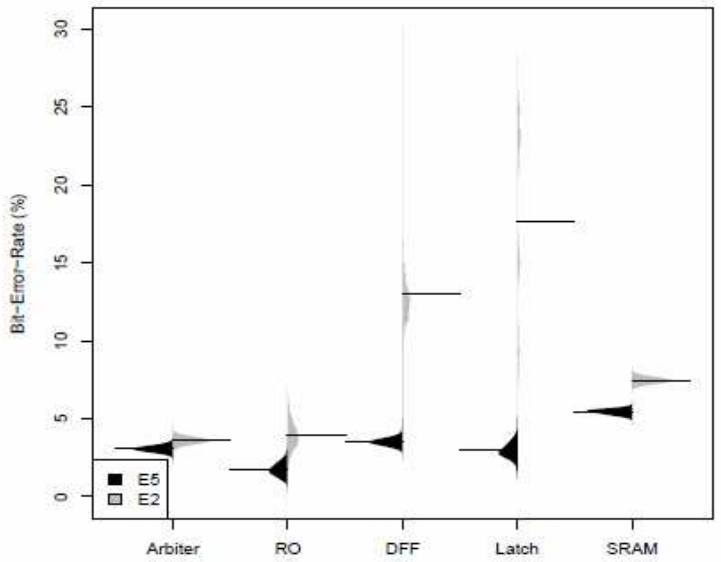
- **Intra and inter variation**
  - PUF sensitive to
    - Noise
    - Environment T°C, Vdd
    - Attacks



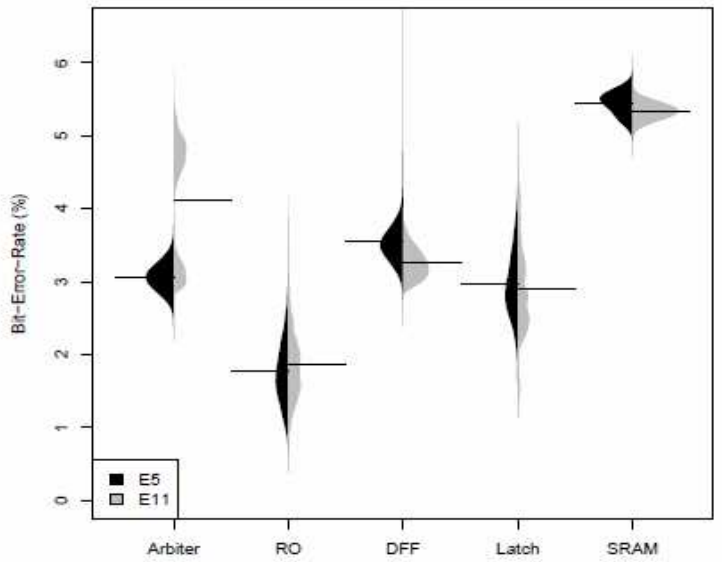
- **Need a correction circuit to enhance the reliability**

PUF reliability

Results from the UNIQUE European project



(a) Bit error rates at +25 °C (test case E_5, black) and at −40 °C (test case E_2, gray)

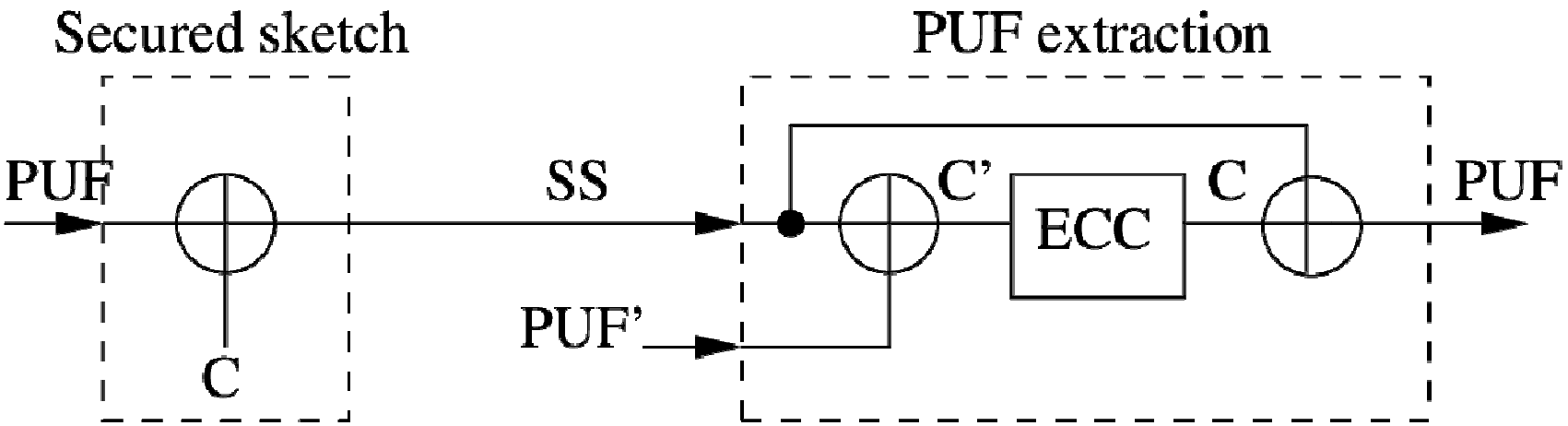


(b) Bit error rates with active core off (test case E_5, black) and active core on (test case E_{11}, gray)

Katzenbeisser, S., Kocabas, Ü., Rožić, V., Sadeghi, A.R., Verbauwhede,I.,Wachsmann, C.: PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon. In: CHES 2012. Springer (2012)

Enhancing the steadiness

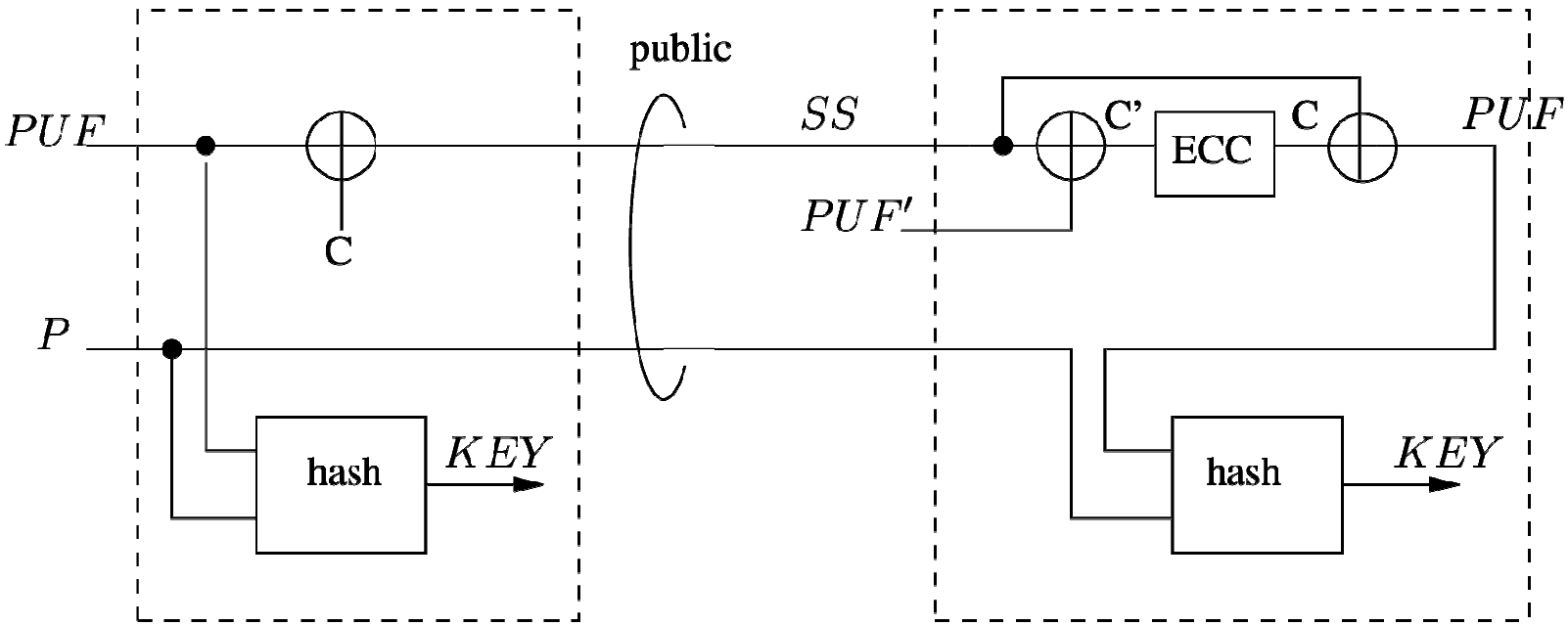
- **Secured sketch: Use of a witness and Error correcting code**



Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”. SIAM J. Comput., 38(1):97–139, 2008.

Reliable Key generation

- **Fuzzy extraction**
  - Key extracted by means of Secure Sketch and Hash function



PUF Attacks 1/2

- **Brute force**
  - To save every Challenge/Response (CRP)
  - Physical access to the PUF is required
- **Replay**
  - Sniffing CRPs and play them back
- **Modeling attack (or Machine Learning attack)**
  - Take advantage of relationships between the challenge / response
  - Methods based on machine learning to build a model by trial and error
  - Set of CRP needed to train ML algorithm
  - Very powerful to attack delay-based PUF

ML attack on delay PUFs

- **Modeling Attacks by Machine Learning (Rührmair et al)**
  - Logistic Regresion technique : success rate
    - Arbiters
      - ✓ 99.9% using 18K CRPs in **0.6 sec**. (64 taps)
    - XOR Arbiter
      - ✓ 99% using 12K CRPs in **3 min 42 secs** (4 XOR, 64 taps).
    - Lightweight Arbiters
      - ✓ 99% using 12K CRPs in **1 hour and 28 mins** (4 XORs, 64 taps).
    - Feed-forward Arbiters
      - ✓ 99% using 5K CRPs in **47 mins and 7 secs** (7 FF, 64 taps).
    - Ring Oscillators
      - ✓ 99% using 90K CRPs (1024 bit value)¤.

PUF Attack 2/2

- **Side-Channel**
  - Mainly focus on the Fuzzy extractor (1)
    - Simple Power Analysis has been carried out on a FE with error correcting code using conditional branches.
    - Template attacks have been implemented on error correcting codes (w/o conditional branches)
- **Could target the RO-based PUFs (2)**
  - The frequency can be lock on external EM carrier injection (rather Fault injection attack than side-channel)

(1) Karakoyunlu, D.; Sunar, B.; , "Differential template attacks on PUF enabled cryptographic devices," *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on* , vol., no., pp.1-6, 12-15 Dec. 2010

(2) François Poucheret, « Injections Electromagnétiques : Développement d'Outils et Méthodes pour la Réalisation d'Attaques Matérielles », Thèse soutenue le 23 novembre au LIRMM

Countermeasures

- **Brute Force Attack**
  - Too long : For a (n, k)−PUF (n input bit, k output bit) : 2^n query and 2^n * k bits memory.
- **Replay attack**
  - Protocol normally forbid to reuse played Challenge
  - Impossible in the case of generating internal secret
- **ML attack**
  - Cipher the challenges or the responses, as the adversary needs both.
  - Cryptography is generally present near the PUF
- **Side-Channel Attack**
  - FE : Masking (as ECC is linear)

Conclusions

- **PUF is an elegant solution to generate an identification**
  - Unique Signature generated by the device itself
- **But need extra hardware**
  - To enhance the steadiness
    - Secure Sketch with ECC
  - To enhance the security
    - protection against SCA and modeling attacks (for the delay PUF)
- **And can be costly**
  - Because of extra Hardware for security and steadiness