ECCTD 2020

Hardware-Intrinsic Security with Printed Electronics for Identification of IoE Devices

Alexander Scholz
MERAGEM
Offenburg University of Applied Sciences
&
Karlsruhe Institute of Technology
Germany

Outline

I. Introduction

- What is a Physical Unclonable Function (PUF) ?
- Printed Electronics (PE)
- PE‘s capabilities as security feature

II. Background

- Hybrid PUF architecture core circuit
- Hybrid PUF addressing methods
- Security assessment on hybrid PUF

III. Results

- Identifiability of hybrid PUF
- Identifiability of hybrid PUF – Results
- Identifiability of hybrid PUF – Comparison

IV. Conclusion and Outlook

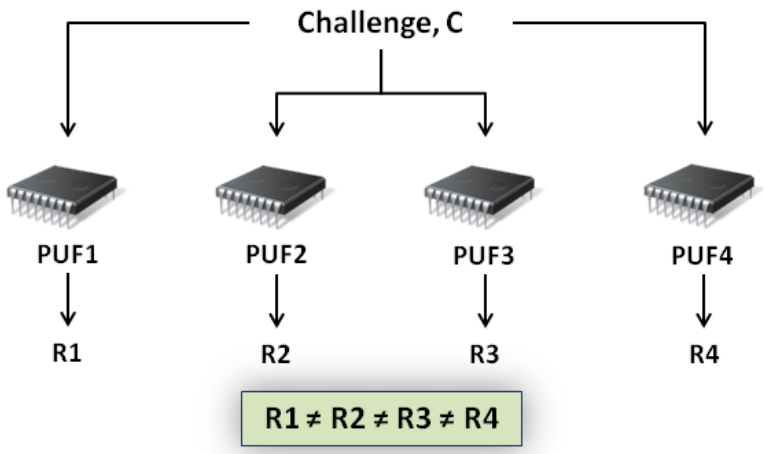
I. What is a Physical Unclonable Function (PUF)?

A Physical Unclonable Function (PUF) is a function that outputs a device-specific response by extracting its intrinsic physical characteristics […].

– Hori, Yohei et al. [1] –

Requirements on PUFs

- Challenge – Response mechanism: $R = f(C)$
- Easy to evaluate in short time
- Hard to characterize with limited resources
- Hard to reproduce



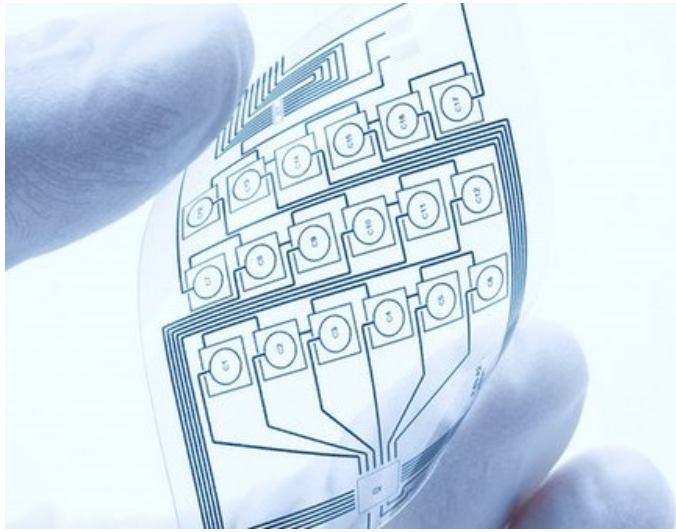
Source: http://rijndael.ece.vt.edu/puf/background.html

Source: http://www.davidcrozier.co.uk/tag/unclonable/

I. Printed Electronics (PE)

Table 1: Comparison between silicon-based electronics with printed electronics

Performance parameters	Silicon-based electronics	Printed electronics
Operating speed	Very high (~GHz)	Low (~kHz)
Integration capabilities	Large-scale integration	Low-scale integration
Form factors	Rigid, partially flexible	Flexible substrates, large area
Production site	Centralized	Decentralized



© Shawn Hempel – Shutterstock
Source:https://www.azonano.com/article.aspx?ArticleID=3697

„Complementary use of traditional silicon based circuits with printed electronics“ [2]

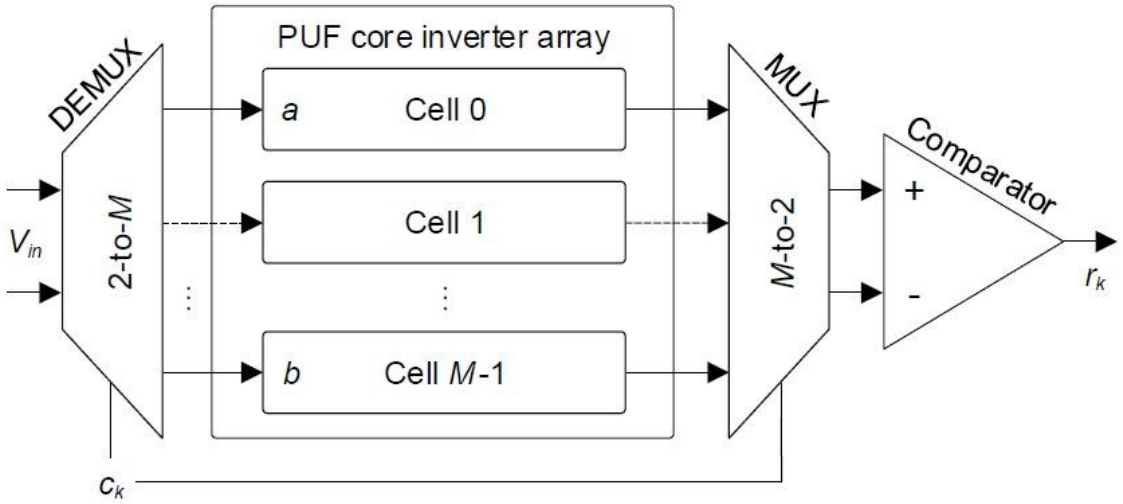
I. PE‘s capabilities as security feature

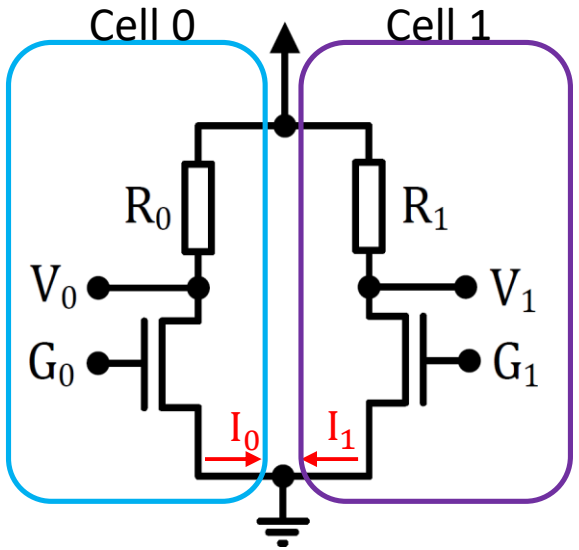
- Smart systems require for authentication and encryption
  - Security begins on the hardware level
- Exploit inherent variability in printed active devices as security feature in form of a PUF
  - Manifold possibilities in materials and substrates
  - Supply chain „root of trust“ due to decentralized manufacturing

II. Hybrid PUF architecture core circuit

Addressable RTL inverter array

- Arbitrary inverter input and output selection
- Digital bit generation based on pair-wise inverter output voltage comparison





II. Hybrid PUF addressing methods

Possible Hybrid PUF addressing methods for challenge-response pair (CRP) generation:

1.) Re-addressing:

- All inverter address combinations, except recurrend or reversed addresses are allowed → Increased response bit width, reduced entropy

$$L_{\mathrm{ra,max}} = \frac{M(M-1)}{2}$$

2.) Differential Addressing:

- Each inverter address is ony used once → Limited response bit width, high entropy

$$L_{\mathrm{da,max}} = \frac{M}{2}$$

II. Security assessment on hybrid PUF

Intra Hamming distance (intra-HD)

(mean value)

$$\mu_{\text{intra}} = \frac{1}{T}\sum_{t=1}^{T}\frac{HD(R_{ref,n}\ ,\ R'_{n,t})}{L}$$

The intra-HD is a measure of the reproducibility of the PUF responses.

- **Reliability metric**
- **Theoretical best value for μ_{intra} is 0**

Inter Hamming distance (inter-HD)

(mean value)

$$\mu_{\text{inter}} = \frac{2}{N(N-1)}\sum_{i=1}^{N-1}\sum_{j=i+1}^{N}\frac{HD(R_i\ ,\ R_j)}{L}$$

The inter-HD is a measure of the uniqueness of the PUF responses.

- **Uniqueness metric**
- **Theoretical best value for μ_{inter} = L/2**

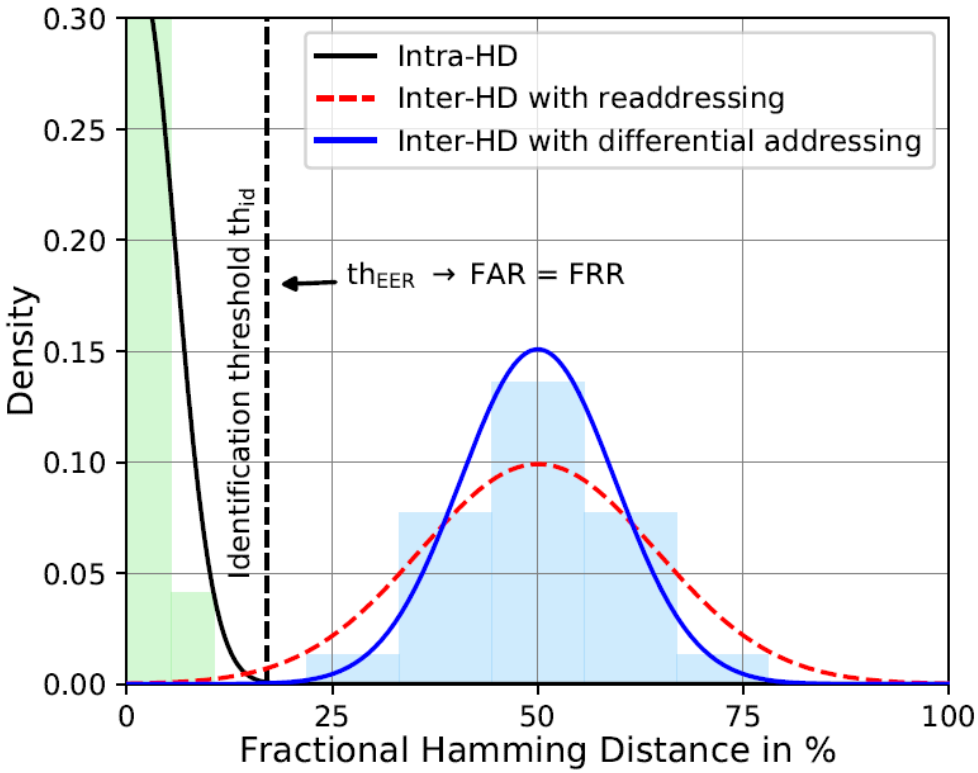
III. Identifiability of hybrid PUF

- Investigation of both addressing types – based on Monte Carlo (MC) simulation of 150 hybrid PUF cores with a L=28-bit response
- Calculate μ_{intra} and μ_{inter} with associated probability density function (PDF)

➢ Set identification threshold (th_{id}), calculate False-Acceptance-Rate (FAR), False-Rejection-Rate (FRR), and Equal-Error-Rate threshold (th_{EER})

$$\text{FAR} = \int_{0}^{\text{th}_{\text{id}}} P_{\text{inter}}(x)\ dx$$

$$\text{FRR} = \int_{\text{th}_{\text{id}}}^{L} P_{\text{intra}}(x)\ dx$$



III. Identifiability of hybrid PUF - Results

Table 2: Performance evaluation of hybrid PUF based on addresing method

Addressing method	Inverter	Bits	Intra-HD		Inter-HD		Threshold @overlapp			Threshold @EER	
	M	L	μ_{intra} (%)	σ_{intra} (%)	μ_{inter} (%)	σ_{inter} (%)	th_{id} (%)	FAR (lg)	FRR (lg)	th_{EER} (%)	FAR/ FRR (lg)
Re-addressing	8	28	1.50	4.46	50.02	14.37	14.29	-2.21	-2.68	13.07	-2.32
Differential	56	28			50.01	9.43	-	-	-	17.08	-3.61

III. Identifiability of hybrid PUF - Comparison

Table 3: Comparison of hybrid PUF performance metrics with other works

PUF type	Intra-HD	Inter-HD	FAR (lg)	FRR (lg)	Ref.
	μ_{intra} (%)	μ_{inter}(%)			
This work	1.50	50.01	-3.61	-3.61	-
Pseudo-LSFR	2.72	62.73	-2.96	-3.05	[3]
SRAM-PUF	-	-	-4.01	-4.03	[4]
PUF sensor	7.16	31.00	-6.04	-6.02	[5]
RO-PUF	1.53	49.60	-6.06	-6.20	[6]

IV. Conclusion and Outlook

Conclusion:

- PE is capable to enable hardware-based security and establish „root of trust“ in supply chains
- PE-based hybrid PUF shows capability for identification
- First assessment of identifiability for novel material devices

Outlook:

- Reduce FAR and FRR in future works due to novel hardware architectures
- Software-sided optimization of FAR & FRR by means of binning techniques and error correction codes

References

[1] Hori, Yohei, et al. „Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs." Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on. IEEE, 2010.

[2] Chang Joseph S. et. al „A Circuits and Systems Perspective of Organic/Printed Electronics: Review, Challenges and Contemporary and Emerging Design Approaches“ IEEE Journal on Emerging and Selected Topics In Circuits And Systems, Vol. 7, No. 1. March 2017

[3] Y. Hori, H. Kang, T. Katashita, and A. Satoh, “Pseudo-lfsr puf: A compact, efficient and reliable physical unclonable function,” in 2011 International Conference on Reconfigurable Computing and FPGAs. IEEE, 2011, pp. 223–228.

[4] Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott, and D. C. Ranasinghe, “Detecting recycled commodity socs: Exploiting aging-induced sram puf unreliability,” arXiv preprint arXiv:1705.07375, 2017

[5] H. Ma, Y. Gao, O. Kavehei, and D. C. Ranasinghe, “A puf sensor: Securing physical measurements,” in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017, pp. 648–653

[6] R. Maes, Physically unclonable functions: Constructions, properties and applications. Springer Science & Business Media, 2013

Thank you for your attention!

Questions?

E-Mail: alexander.scholz@hs-offenburg.de
alexander.scholz2@kit.edu