Daniele Lombardi

Exploiting Physical Unclonable Functions to secure resource-constrained devices

Tutor: Prof.ssa Valentina Casola

Cycle: XXXVII

Year: Third

itee PhD
information technology
electrical engineering

Candidate's information

- MSc degree: **Computer Engineering**
- Research group/laboratory: **RFI / SecLab**
- PhD start date: **01.01.2022 - 31.12.2024**
- Scholarship type: **None**
- Research fellowship, founded by: **Rete Ferroviaria Italiana S.p.A.**
- Periods abroad: **Visiting at Laboratoire TIMA - Université Grenoble Alpes (26.05.24 - 29.07.24 / 28.08.24 - 12.10.24)**
- Scientific/Industrial Collaborations:
  - **Rete Ferroviaria Italiana S.p.A.**

Summary of study activities

- **First Year**
  - Courses on virtualization technologies, and statistical data analysis
  - Seminars on security issues and critical systems
  - Design and Prototyping of critical systems
- **Second Year**
  - Seminars on security and PUFs-based solutions
  - Attendance at conferences/event:
    - 9th IEEE International Workshop on Advances in Sensors and Interfaces (IWASI 2023)
    - 14th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2023)
    - PUF-enabled Security Challenge (CSAW'23), **selected as finalist**
  - Designing lightweight security solutions based on Physical Unclonable Functions
  - Design and Prototyping of critical systems
- **Third Year**
  - Course on industrial embedded system design
  - Attendance at conferences/event:
    - International Conference on Availability, Reliability and Security (ARES'24)
  - Design and Prototyping of critical systems
  - Methodologies for the assessment of PUFs quality metrics
  - Adoption of PUFs in virtual environments

Research area(s)

- **Main Research Area**:
  - *Securing resource-constrained devices by PUFs* (A1)*
    - *Assessment of the quality of PUFs (Ch1)*
    - Designing lightweight solutions to security problems (*Ch2*)
- **Others:**
  - *Design of critical systems* (A2)
    - Non-intrusive testing of critical real-time systems for generic platforms;
    - Mechanisms of redundancy in 2x2oo2 systems;
    - Interrupts management to improve system predictability

***PhD Thesis**

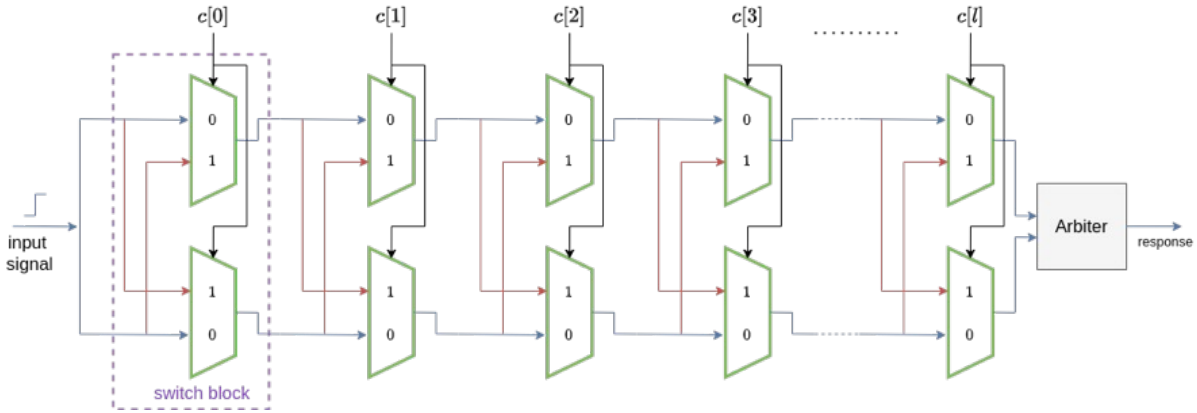
Physical Unclonable Functions

- **Physical Unclonable Functions** are special integrated circuits, with unique physical characteristics, caused by random imperfections, introduced during the manufacturing process.

- From a mathematical perspective:

$$\theta : C \rightarrow R,\ C \in \{0, 1\}^m \text{ and } R \in \{0, 1\}^n$$

- To assess the **goodness** of an implementation there are **quality metrics** such as:
  - *Uniformity*
  - *Bit-aliasing*
  - *Reliability*
  - *Uniqueness*



PhD thesis overview

Problem

- PUFs are emerging as one of the most promising **hardware security primitives**, enabling the resolution of problems such as forgery, authentication, key management, and root of trust on *devices with **limited** resources*. However, their adoption is slowed down by a number of **challenges**, including:

P1: Lack of data (C1)

P2: Resource-inefficient applications (C2)

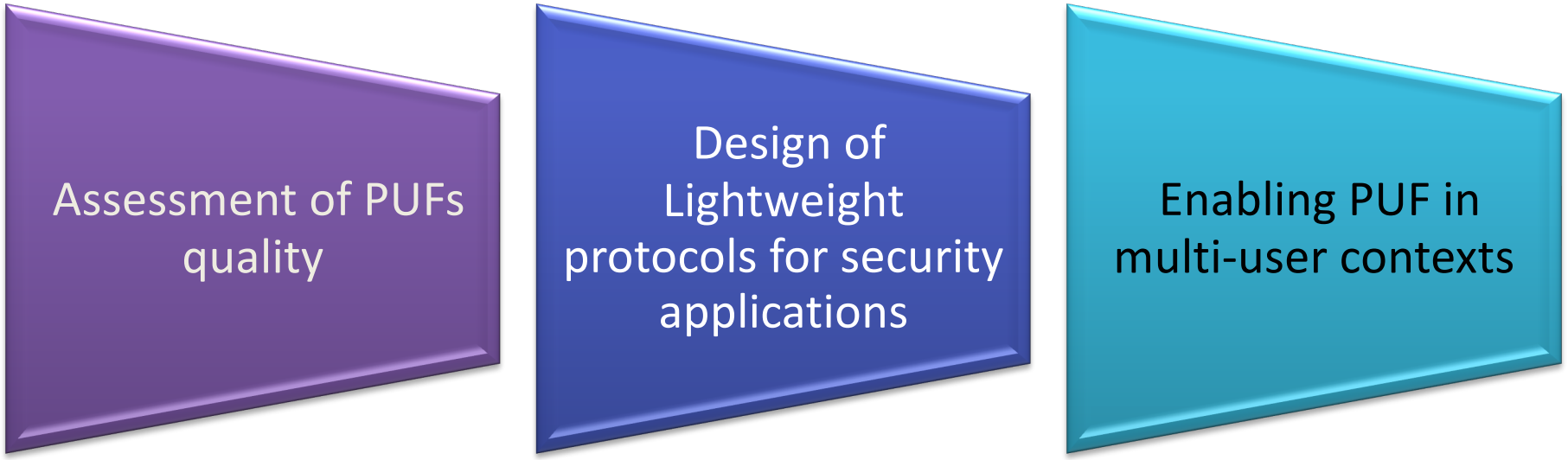
P3: Suitability in multi-users contexts (C2)

PhD thesis overview

Objective

- Systematic development of flexible tools and methodologies to support the design and evaluation of security applications based on the adoption of PUFs.

Methodology



Contribution 1:
Assessment of PUFs quality

Problem

Characterizing a PUF implementation on a large scale is a **costly activity** in terms of: implementation **time**; **economic** costs; implementation **complexity**. Moreover, this activity does not allow researchers to focus solely on implementation aspects of new proposals.

State of the Art

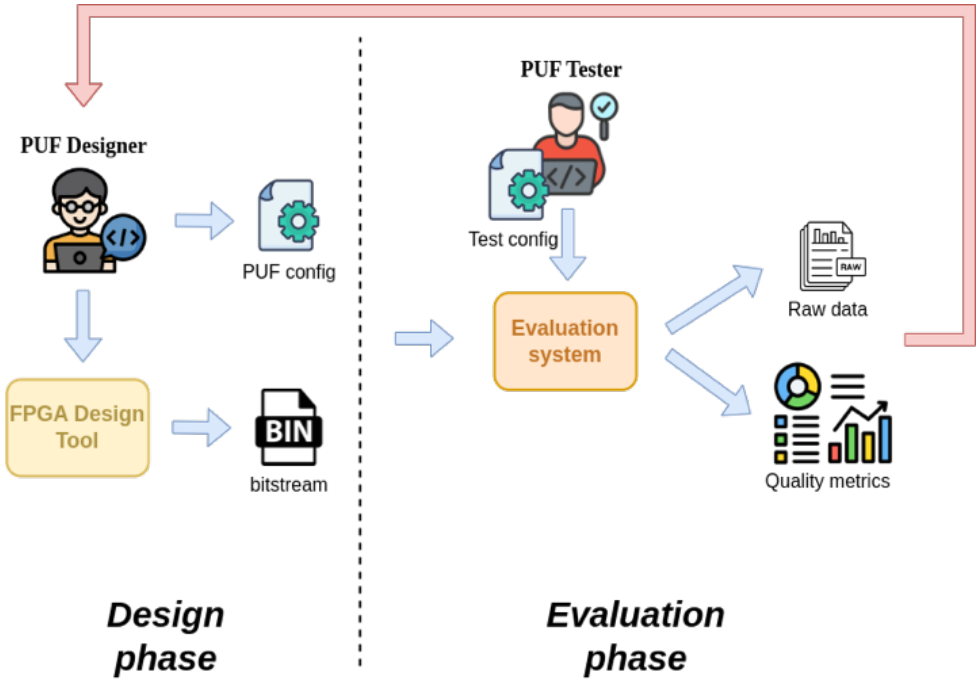
- Many new PUF proposals are characterized by insufficient data
- Existing large-scale PUFs evaluation systems are:
  - poorly scalable (hard to maintain)
  - targeted for specific implementation (not reusable)
    - do not allow for comparison of different implementations

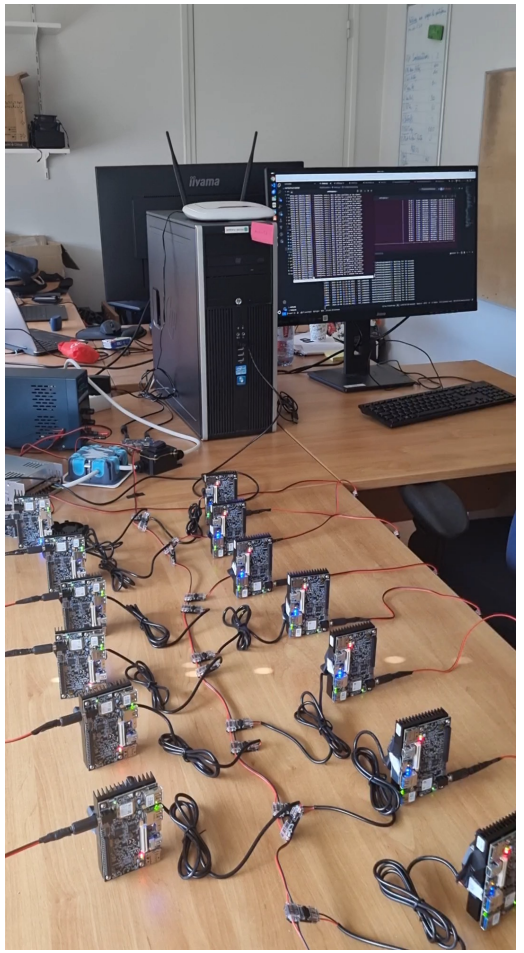
Assessment of PUFs quality

Contribution

SPECTRE[1] allows the large-scale characterization of generic PUFs synthesized on FPGA technology, offering several advantages:

- to develop new PUFs with an **hardwareless** approach;
- easy **scalability** of the number of devices;
- **flexibility**, test any PUF on FPGA.





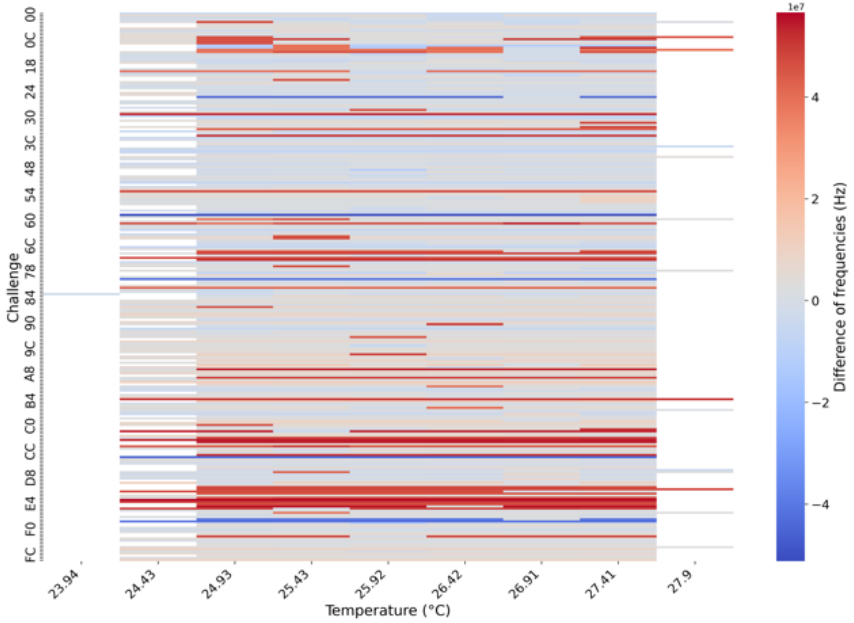
[1] *On the large-scale characterization of FPGA-based Physical Unclonable Functions – D. Lombardi, M. Barbareschi, V. Casola, E. Vatajelu, G. Di Natale*

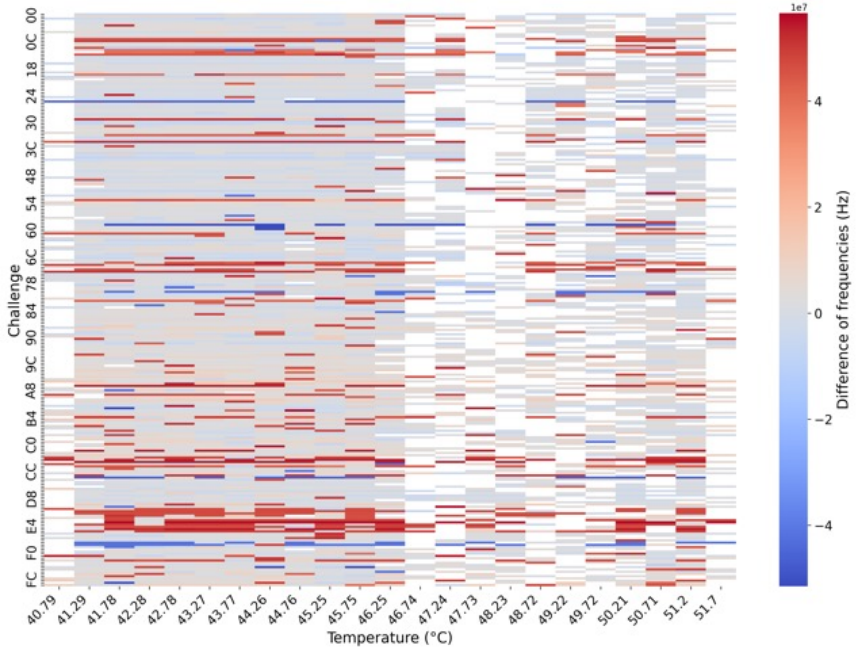
Assessment of PUFs quality

Results

The tool was tested with 7 different PUF implementations, helping to identify:

- which PUF metrics to improve;
- which FPGA locations offer better metrics;
- the correlation between temperature rise and oscillation frequency variation in RO-PUFs.





- The tool successfully supported the development of a new PUF: **one-LUT PUF[2]**

[2] *A One-LUT Physical Unclonable Function on AMD FPGAs - F. Ferrandino, D. Lombardi, A. Cilardo.*

Contribution 2:
Design of Lightweight protocols for security applications

Problem

Securing resource-constrained devices (e.g IoT devices), by guaranteeing authentication, integrity and confidentiality of exchanged data, considering:

- Their limited storage capacity;
- Their limited computational capability;
- Heterogeneity of architectures;
- High number of devices

State of the Art

- Classical approaches based on asymmetric cryptography are not suitable because they are computationally burdensome
- Some solutions rely on pre-installed keys on vulnerable NVM memories.
- Other solutions in literatures are declared lightweight but are not transparently evaluated on all possible metrics.

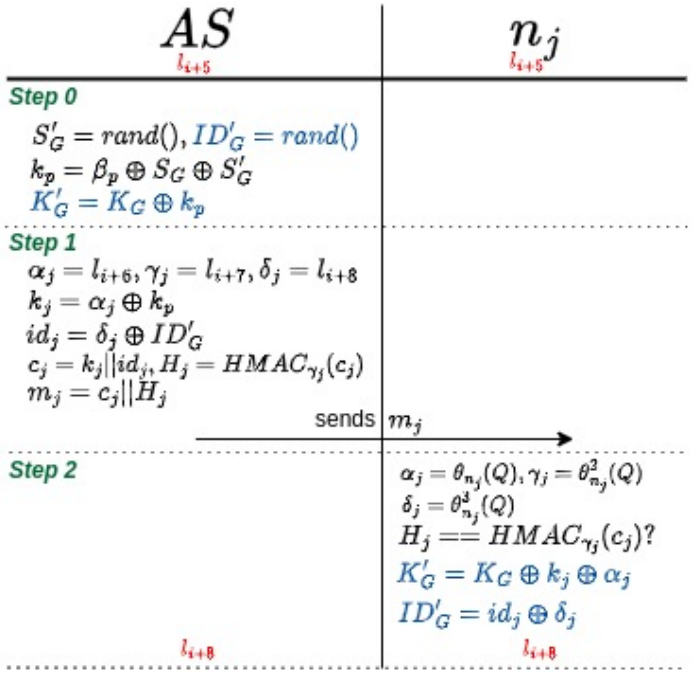
Lightweight protocols for security applications

Contribution

- **Design a family of solutions** [3, 4, 5, 6] characterized by:
  - Low overheads;
  - Use of innovative and safe primitives (PUF);
  - Use of simple operations (XOR);
- **Compare** the proposals with existing solutions w.r.t.
  - Computiational costs;
  - Comunication costs;
  - Scalability;
  - Execution times;
  - Security analysis.

$$K_G = \bigoplus_{j=1}^{N_G} \beta_j \oplus S_G$$

Group key composition



[3] *A Lightweight PUF-based Protocol for Dynamic and Secure Group Key Management in the IoT - M. Barbareschi, V. Casola, A. Emmanuele, D. Lombardi*

[4] *Lightweight Secure Keys Management Based on Physical Unclonable Functions - M. Barbareschi, V. Casola, D. Lombardi*

[5] *On the adoption of PUF for key agreement scheme in Internet of Things - M. Barbareschi, V. Casola, A. Emmanuele, D. Lombardi.*

[6] *Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions - M. Barbareschi, V. Casola, D. Lombardi.*

Lightweight protocols for security applications

Results

- Experimental results conducted on ESP8266 boards show that group key management protocols with a centralized, decentralized approach perform better than existing

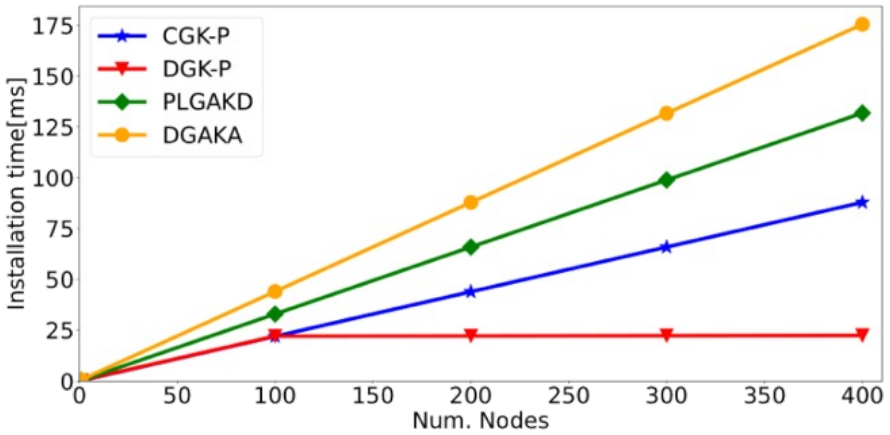
	Installation (μs)	Join (μs)	Revoke (μs)
CGK-P	990	483	692
DGK-P	1450	$880^{\dagger}$ / 483	$1151^{\dagger}$ / 483
[16]	2130	818	$2130^{\dagger}$ / 1243
[17]	1910	766	1255

† times obtained by devices belonging to the subgroup that triggers the update

Execution Times

	Installation	Join	Revoke
CGK-P	$2 \cdot N_G$	1	$N_G - 1$
DGK-P	$2 \cdot N_{LV} \cdot (N_l + 2)$	$N_{LV} + 2$	$N_{LV} + N_l$
[17]	$3 \cdot N_G$	1	t
[16]	$2 \cdot N_G$	1	$N_{LV} + N_l - 2$
[18] v.1	$4 \cdot N_G$	n.s.	n.s.
[18] v.2	$2 \cdot N_G$	n.s.	n.s.
[19]	$4 \cdot N_G$	n.a.	n.a.

Communication costs



Execution Times (Installation)

Contribution 3:
Enabling PUFs in multi-user context

PUF in multi-user contexts

Problem

- The current PUF model **cannot** be directly used to establish **trust relationships** with applications running on the same device, since each of them could impersonate the others by exploiting the same PUF circuit. Furthermore, if one application is compromised, all the others are compromised, as they can no longer guarantee their security properties.

State of the Art

- Virtualization techniques of security primitives are based on TPM (V-TPM)
- V-TPM solutions are designed for the Cloud and would not be easily integrated at the Edge (scarce resources)
- There are no PUF-based solutions

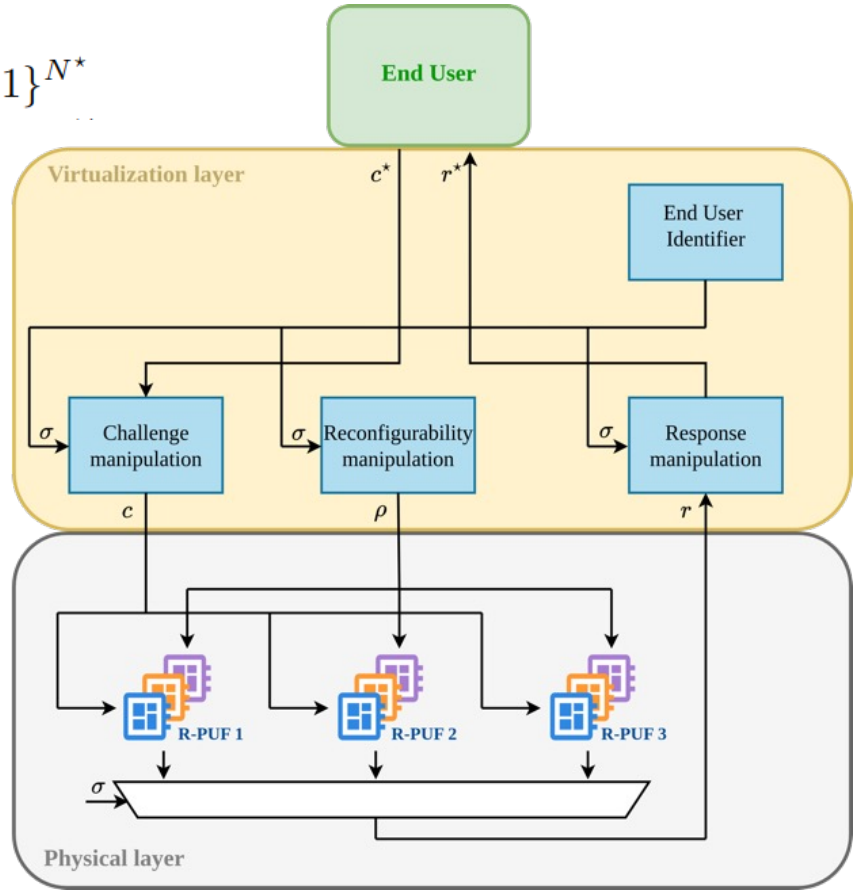
PUF in multi-user contexts

Contribution

- The **V-PUF**[7] model:

$$\upsilon(\theta, \chi, \rho, \sigma, \cdot) : \mathcal{C}^\star \rightarrow \mathcal{R}^\star, \mathcal{C}^\star \in \{0,1\}^{L^\star}, \mathcal{R}^\star \in \{0,1\}^{N^\star}$$

- The V-PUF *properties*:
  - Equivalence;
  - Isolation;
  - Anti-forging;
  - Interface-inheritance;
  - Fairness.
- The V-PUF *quality metrics*:
  - Uniqueness and Bit-Aliasing evaluated intra- and inter-chip
- The *Virtual enrollment* procedure
- *Strategies of virtualization*



[7] *Pioneering Virtual Physical Unclonable Functions – M. Barbareschi, A. Emmanuele, D. Lombardi*

PUF in multi-user contexts

Results

- Target Hw:
  - RISC-V Rocket Chip on Artix A7 100T (FPGA)
- Target Sw:
  - Xvisor Hypervisor
- Target PUF:
  - SRAM PUF + AES
- Average response time: 6.450 ms

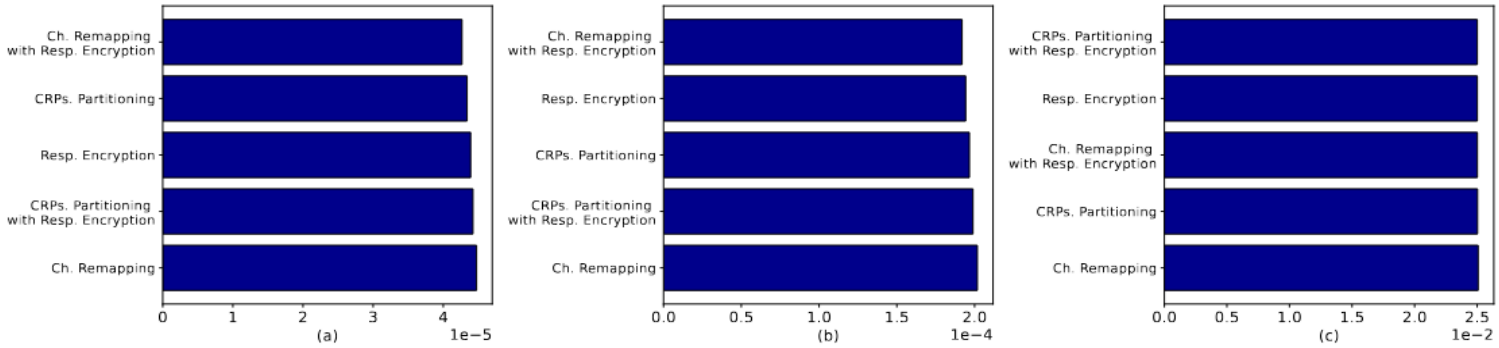


Fig. 5. MSE calculated on various error metrics for different virtualization strategies. (a) Intra Uniqueness (b) Uniformity (c) Intra Bit-Aliasing.

Products for Activity A1*

Security of resource-constrained devices

[W1]	Title: *Lightweight Secure Keys Management Based on Physical Unclonable Functions* Authors: M. Barbareschi, V. Casola, **D. Lombardi** Workshop: The 9th IEEE International Workshop on Advances in Sensors and Interfaces. [published]
[C2]	Title: *Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions* Authors: M. Barbareschi, V. Casola, **D. Lombardi**. Conference: CLOUDCOM 2023, The 14th IEEE International Conference on Cloud computing technology and science, Secure Cloud Continuum. Status: published
[J3]	Title: *A Lightweight PUF-based Protocol for Dynamic and Secure Group Key Management in the IoT* Authors: M. Barbareschi, V. Casola, A. Emmanuele, **D. Lombardi**. Journal: IEEE Internet of Things Journal. Status: published.
[C4]	Title: *On the adoption of PUF for key agreement scheme in Internet of Things* Authors: M. Barbareschi, V. Casola, A. Emmanuele, **D. Lombardi.** Conference: Computing Frontiers Conference Status: published.
[J4]	Title: *Pioneering Virtual Physical Unclonable Functions* Authors: M. Barbareschi, E. Emmanuele, **D. Lombardi**. Journal: IEEE Transactions on Emerging Topics in Computing. Status: submitted.
[J5]	Title: *On the large-scale characterization of FPGA-based Physical Unclonable Functions* Authors: **D. Lombardi**, M. Barbareschi, V. Casola, Journal: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Status: Submitted.
[C6]	Title: A One-LUT Physical Unclonable Function on AMD FPGAs Authors: F. Ferrandino, **D. Lombardi**, A. Cilardo. Conference: Late Breaking Results, DATE'25. Status: Submitted
[T7]	Title: SPECTRE Authors: D. Lombardi. Type: Platform for the automatic evaluation of generic PUFs. Status: Released.

Products for Activity A2

Design of critical systems

[D1]	Title: Non-intrusive Testing of RfiOS Authors: S. Barone, S. Della Torca, **D. Lombardi.** Type: Deliverable on Testing of rt-critical system. Project: Joint Project between DIETI and RFI on rt-critical systems design. Status: Released.
[D2]	Title*: MngSCC* Authors: F. Bianco, A. Emmanuele, S. Della Torca, **D. Lombardi.** Type: Deliverable on Design and development of software in rt-critical systems (entire lifecycle). Project: Joint Project between DIETI and RFI on rt-critical systems design. Status: Released.
[D3]	Title: *Mechanisms of redundancy in 2x2oo2 systems* Authors: A. Emmanuele, M. Gaudino, **D. Lombardi**, D. Marcello. Type: Deliverable on Design and development of software in rt-critical systems (entire lifecycle). Project: Joint Project between DIETI and RFI on rt-critical systems design. Status: Released.
[C1]	Title: *Automatic Test Generation to Improve Scrum for Safety Agile Methodology* Authors: M. Barbareschi, S. Barone, V. Casola, S. Della Torca, **D. Lombardi** Conference: ARES 2023, The 18th International Conference on Availability, Reliability and Security. Status: Published
[C2]	Title: *Timing Behavior Characterization of Critical Real-Time Systems through Hybrid Timing Analysis* Authors: S. Barone, V. Casola, S. Della Torca, **D. Lombardi** Conference: 7th International Conference on System Reliability and Safety. Status: Published.
[C3]	Title: *A comprehensive evaluation of interrupt measurement techniques for predictability in safety-critical systems* Authors: D. Lombardi, M. Barbareschi, S. Barone, V. Casola Conference: International Conference on Availability, Reliability and Security. Status: Published

D = Deliverable of research, C=Conference paper