Università degli Studi di Napoli Federico II

itee PhD information technology electrical engineering

DIETI UNINA

Daniele Lombardi

Design of secure IoT devices:

ensuring security by PUF

Tutor: Prof.ssa Valentina Casola

Cycle: XXXVII

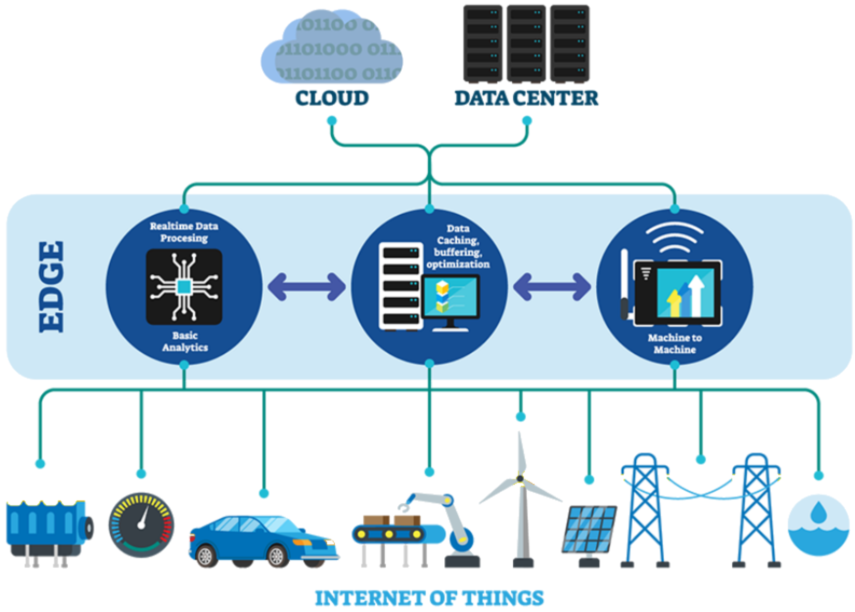
Year: Second

My background

- MSc degree: Computer Engineering
- Research group/laboratory: RFI / SecLab
- PhD start date: 01.01.2022
- Scholarship type: None
- Research fellowship, founded by Rete Ferroviaria Italiana S.p.A.

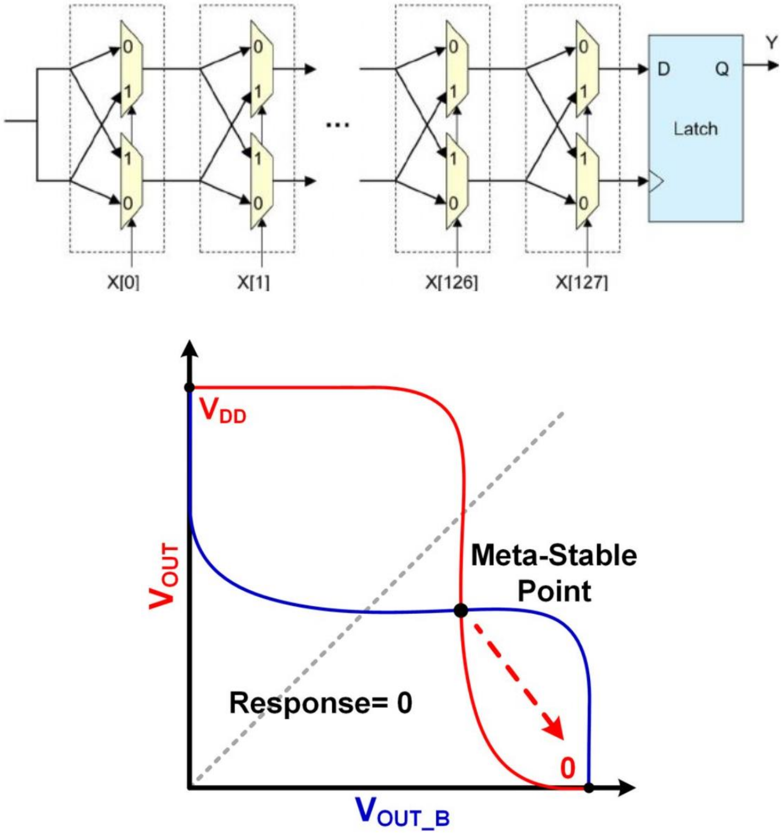
Research field of interest

- My research activity involves the analysis and design of innovative solutions for **secure critical infrastructure** (e.g. diagnostic unit).
- Particularly, during the second year, I was concerned with figuring out how to ensure security at the **lowest levels** of a typical IoT infrastructure.



Research field of interest

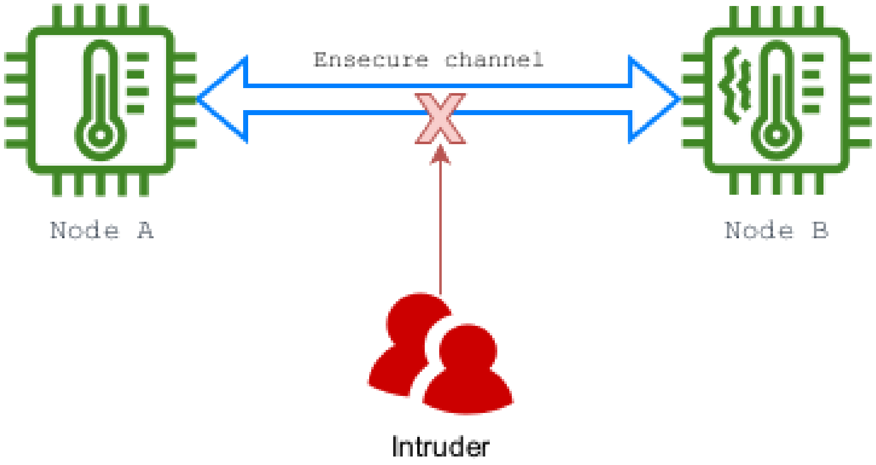
- The **problems identified** are many and relate to:
  - lack of cryptography;
  - use of weak passwords;
  - lack of robust authentication;
  - inappropriate keys management;
  - counterfeiting of devices;
  - …
- **Physical Unclonable Functions** are one of the most promising enabling technologies to solve many of these problems.



Examples of PUFs

Research activity A1: Overview (1)

- **Problem**
  - Ensuring the **security of IoT-based applications** that are generally characterized by:
    - Large numbers of nodes;
    - Devices poorly equipped in terms of resources (no asymmetric cypher);
    - Lack of security in exchanged data.



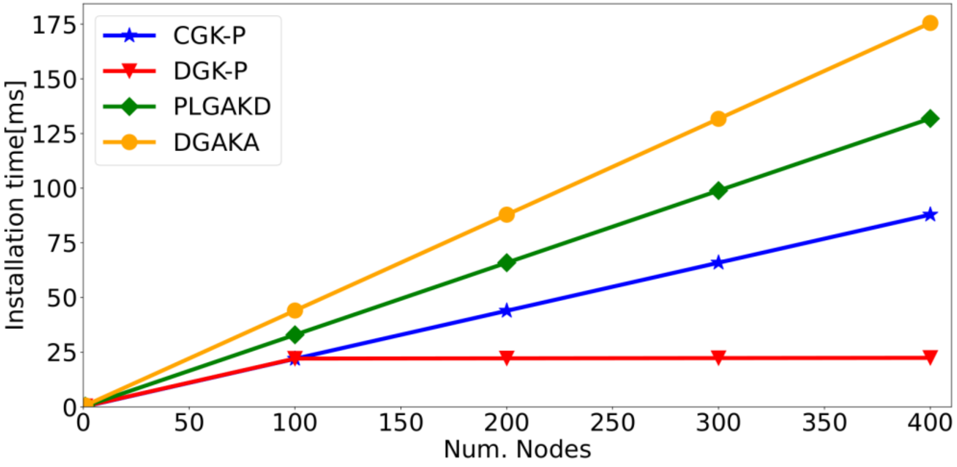
- **Objective**
  - **Define** schemes for the **management of symmetric cryptographic keys**, suitable for resource-poor devices in IoT, in order to guarantee *confidentiality*, *integrity* and *authentication* of data exchanged in both end-to-end and group communications.

Research activity A1: Overview (2)

- **Methodology**
  1. **Design a family of solutions** characterized by:
     - Low overheads;
     - Use of innovative and safe primitives (PUF);
     - Use of simple operations (XOR);
  2. **Compare** the proposals with existing solutions w.r.t.
     - Computiational costs;
     - Comunication costs;
     - Scalability;
     - Execution times.

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

Group key composition



Experimental results

Summary of study activities

- **Seminars:**
  - 6, mainly related to security issues and PUF
- **Conferences / events attended:**
  - 9th IEEE International Workshop on Advances in Sensors and Interfaces (IWASI 2023)
  - 14th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2023)
  - International Security Challenge PUF-enabled Security Challenge **(**CSAW'23), **selected as finalist**
- – **Research Areas:**
  - A1: Data security of IoT-based applications
  - A2: Design of critical systems

Products for Activity A1

Data security of IoT-based applications

[W1]	Title: *Lightweight Secure Keys Management Based on Physical Unclonable Functions* Authors: M. Barbareschi, V. Casola, **D. Lombardi**. Workshop: IWASI 2023, The 9th IEEE International Workshop on Advances in Sensors and Interfaces. Status: 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: submitted.

Products for Activity A2

Design of critical systems

[P1]	<u>Title</u>: *Non-intrusive Testing of RfiOS* <u>Authors</u>: S. Barone, S. Della Torca, **D. Lombardi.** <u>Type</u>: Deliverable on Testing of rt-critical system. <u>Project</u>: Joint Project between DIETI and RFI on rt-critical systems design. <u>Status</u>: Released.
[P2]	<u>Title</u>*: MngSCC* <u>Authors</u>: F. Bianco, A. Emmanuele, S. Della Torca, **D. Lombardi.** <u>Type</u>: Deliverable on Design and development of software in rt-critical systems (entire lifecycle). <u>Project</u>: Joint Project between DIETI and RFI on rt-critical systems design. <u>Status</u>: Released.
[P3]	<u>Title</u>: *Mechanisms of redundancy in 2x2oo2 systems* <u>Authors</u>: A. Emmanuele, M. Gaudino, **D. Lombardi**, D. Marcello. <u>Type</u>: Deliverable on Design and development of software in rt-critical systems (entire lifecycle). <u>Project</u>: Joint Project between DIETI and RFI on rt-critical systems design. <u>Status</u>: Under development.
[C4]	<u>Title</u>: *Automatic Test Generation to Improve Scrum for Safety Agile Methodology* <u>Authors</u>: M. Barbareschi, S. Barone, V. Casola, S. Della Torca, **D. Lombardi** <u>Conference</u>: ARES 2023, The 18th International Conference on Availability, Reliability and Security. <u>Status</u>: Published
[C5]	<u>Title</u>: *Timing Behavior Characterization of Critical Real-Time Systems through Hybrid Timing Analysis* <u>Authors</u>: S. Barone, V. Casola, S. Della Torca, **D. Lombardi** <u>Conference</u>: 7th International Conference on System Reliability and Safety. <u>Status</u>: Published.