Antonio Emmanuele

Computing at the edge: from acceleration to security

Tutor: prof. Mario Barbareschi

Cycle: XXXIX Year:Second

Candidate's information

- MSc degree: Computer Engineering
- Research group/laboratory: SecLab
- PhD Start Date: 01/11/2023
- Scholarship type: UNINA
- Periods abroad: 07/10/2025 – 31/10/2025

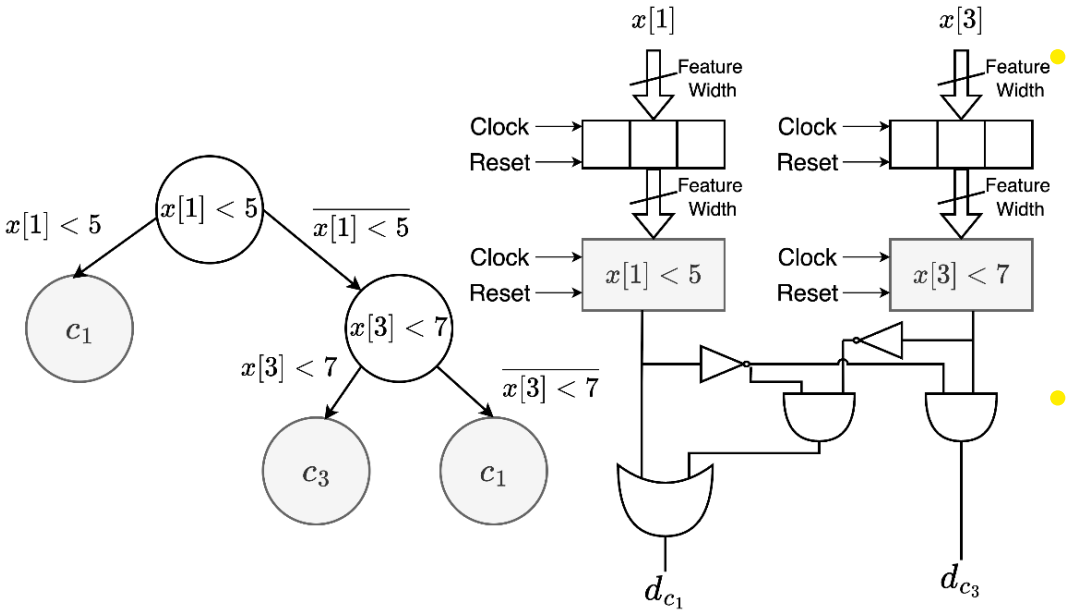
Summary of study activities

- **Seminars (Ph.D. Schools):**
  - 20th TAROT Summer School on Software Testing, Verification & Validation
  - IWES PhD School on Embedded Systems
- **Courses:**
  - Safety Critical Systems for Railway Traffic Management
- **Research Areas:**
  - **A1: Edge deployment** of Decision Tree ML models.
  - **A2:** Security solutions based on **Physical Unclonable Functions** .

Research Activity: Overview

- With the growing adoption of **IoT**, the **edge computing** paradigm is being increasingly embraced for enhancing:
  - **User privacy**;
  - **Latency**;
  - **Network bandwidth;**
- Edge devices are usually characterized by:
  - **Limited computational and memory resources**
  - **Energy constraints** when battery powered.
  - **Lack of secure memory**
- **Challenges**:
  - Running **ML models on edge nodes (Edge-AI).**
  - Ensuring **security properties**, such as **communication confidentiality (Edge-Security).**

Research Activity: Edge-AI



- Deep Learning model are no longer considered a *silver-bullet* for all tasks.
  - Many of them can be carried out with simpler models, such as **Decision Trees**.
- Decision Trees are well-suited for the edge, as their **inference is a simple tree-traversal**.

Nonetheless, their adoption is not-trivial:

1. Hardware resource demand in FPGA/ASIC **grows with the size of the models**.
2. As they are **irregular data-structures**, they **cannot exploit the** SIMD capabilities of new microcontrollers
3. Their **resiliency to faults** is still not studied (difficult to adopt in safety critical systems).

Research Results: Edge-AI

1. To minimize hardware demands we proposed a **Modular Redundancy based Approximation technique** for Tree Ensembles.
   - For each class label, subset of trees are selected for a single class. **Each label is therefore assigned in a Modular Redundancy fashion.**
   - Trees not present in the subset are approximated via **fan-in and fan-out removal**.
2. We proposed a **SIMD-based visiting Kernel**.
   - The kernel enables full-exploitation of vectorial capabilities by relying on Tighly Coupled Memories (no cache-uncertainty!).
3. Analyzed the reliability of Decision Tree accelerators through **Fault Injection**.
   - **Statistical Fault Injection** has been applied to **minimize the number of fault injection sites**.

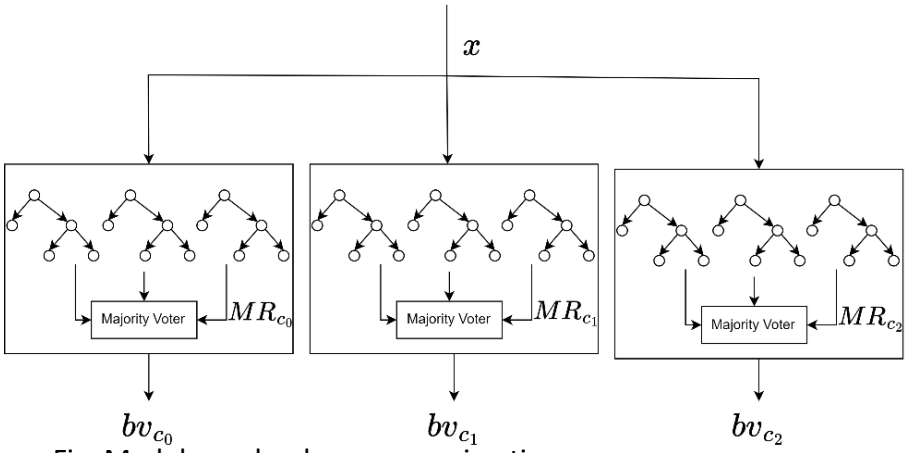


Fig: Modular redundancy approximation

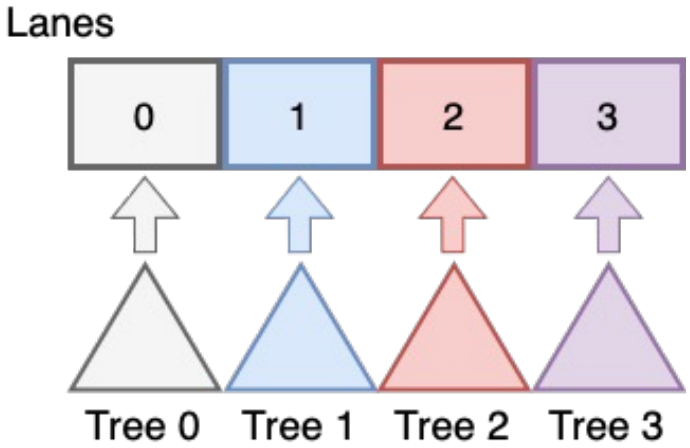


Fig: SIMD visiting

Research Activity: Edge-Security

- I tackled edge security challenges using **Physical Unclonable Functions** (PUFs).
  - **PUFs** are security primitives which leverage the **manufacturing imperfections** of digital circuits to generate **device-specific** cryptographic material.

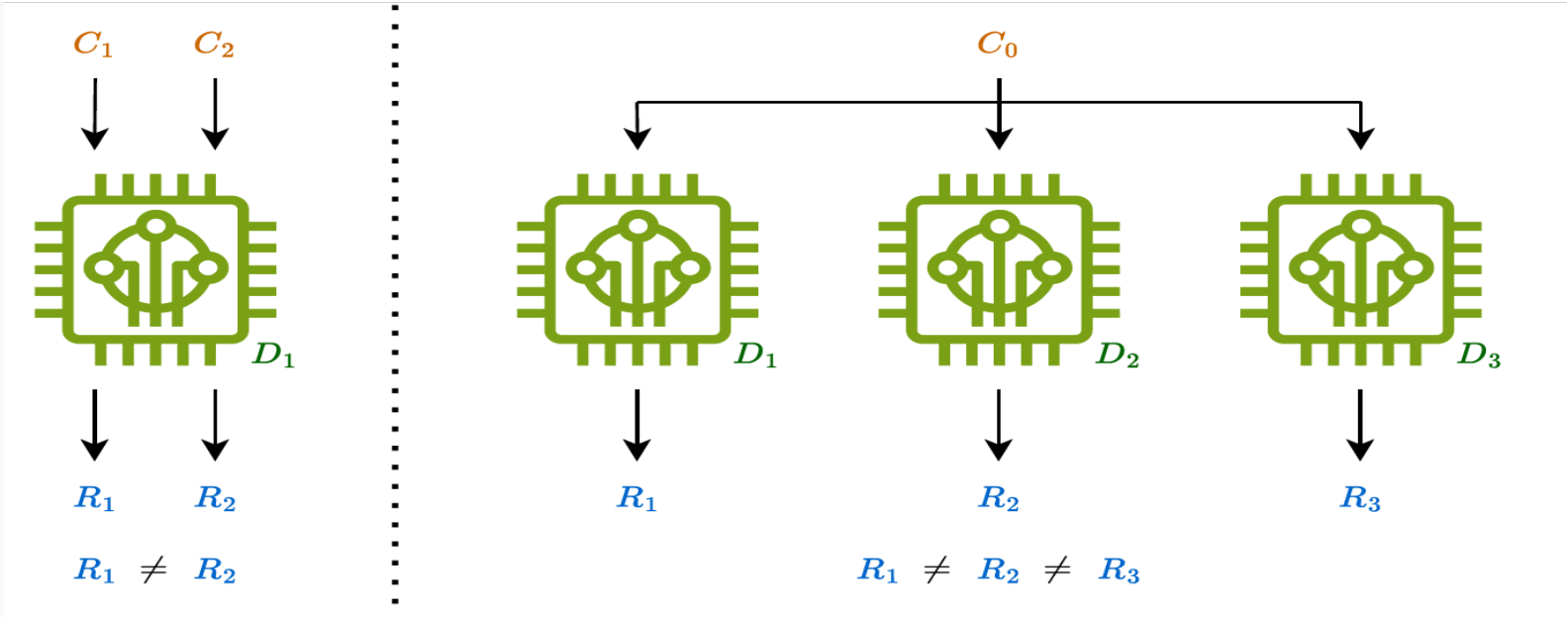


Fig: PUF behaviour over single and different devices.

Research Results: Edge-Security

- IoT nodes operate in large groups. Security applications require to verify the internal state of nodes with: i) Minimum Network Bandwidth ii) Lightweight Computation
  - I investigated the use of PUFs in Decentralized Remote Attestation, a procedure which allows a verifier to attest a large number of IoT nodes with minimum network overhead.
  - The solution is entirely based on XOR operation !
- The IoT is increasingly adopting the **multi-user paradigm**. The latter entails that heterogeneous applications are deployed within the same IoT node.
  - PUFs are tailored for **single-user applications**.
  - I investigated their **virtualization** by proposing a new primitive called **virtual PUF (vPUF).**

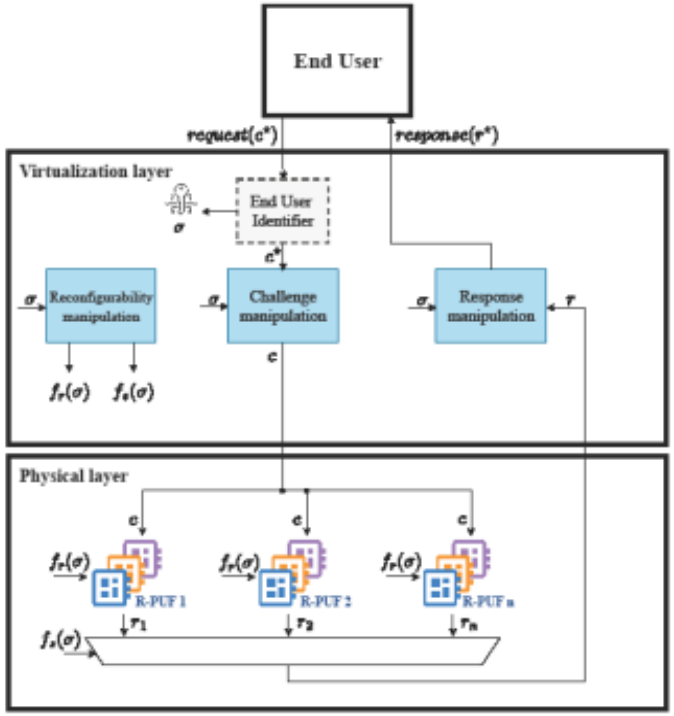


Fig: Virtual PUF architecture

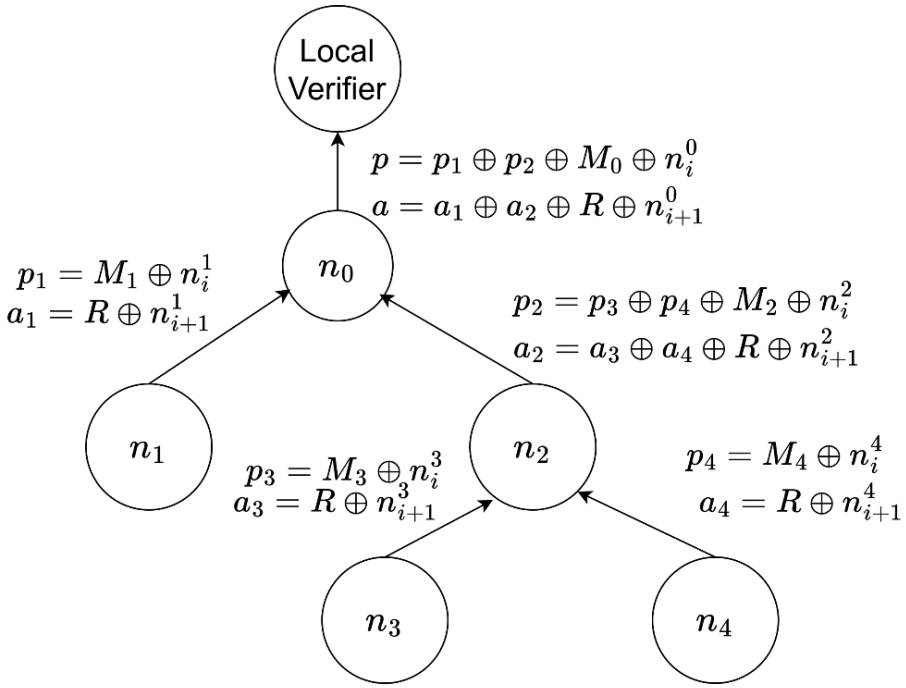


Fig: Proposed Spanning Tree Attestation

Research products

[C1]	*Mario Barbareschi, Antonio Emmanuele, Daniele Lombardi* A Decentralized PUF-Based Scheme for Remote Attestation **International Conference on Availability, Reliability and Security, pp. 167-180**
[C2]	*Mario Barbareschi, Antonio Emmanuele* A Margin Based Early-Stopping Approach for Random Forest Classifiers **2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 123 – 126**
[C3]	*Mario Barbareschi, Antonio Emmanuele, Nicola Mazzocca, Franca Rocco Di Torrepadula* Bridging Efficient and Explainable Traffic Flow Prediction on the Edge **International Conference on Advanced Information Networking and Applications, pp. 347-356**
[C4]	*Mario Barbareschi, Antonio Emmanuele, Nicola Mazzocca, Franca Rocco Di Torrepadula* Harnessing Explainable AI in Railway: A Decision Tree-Based Approach **2025 20th European Dependable Computing Conference Companion Proceedings (EDCC-C), pp. 119-124**
[C5]	*Mario Barbareschi, Valentina Casola, Antonio Emmanuele, Daniele Lombardi* PUF-Based Secure Key Management for Continuum Computing **International Conference on Advanced Information Networking and Applications, pp. 390-399**

Research products

[J1]	*Antonio Emmanuele, Mario Barbareschi, Alberto Bosio* Exploiting Modular Redundancy for approximating Random Forest classifiers **Future Generation Computer Systems (Under Review)**
[J2]	*Mario Barbareschi, Salvatore Barone, Antonio Emmanuele, Alberto Bosio* Reliability analysis of Random Forest Classifiers **Future Generation Computer Systems (Under Review)**
[J3]	*Mario Barbareschi, Antonio Emmanuele, Nicola Mazzocca, Franca Rocco Di Torrepadula* A dual stage approach for interpretal time series forecasting in Cyber Physical Systems **Internet Of Things, Elsevier (Under Review)**
[J4]	*Mario Barbareschi, Valentina Casola, Antonio Emmanuele, Daniele Lombardi* vPUF: Virtualizing the Physical Unclonable Function **Under Revision after Reject**

PhD thesis overview

- My thesis will focus on the Edge-AI components including the following topics and structure:
  - *Computing Architectures for Edge AI models*
  - *Approximate Computing Techniques for AI models*
  - *Fault resiliency of models*
  - *Pratical applications in industrial domain*