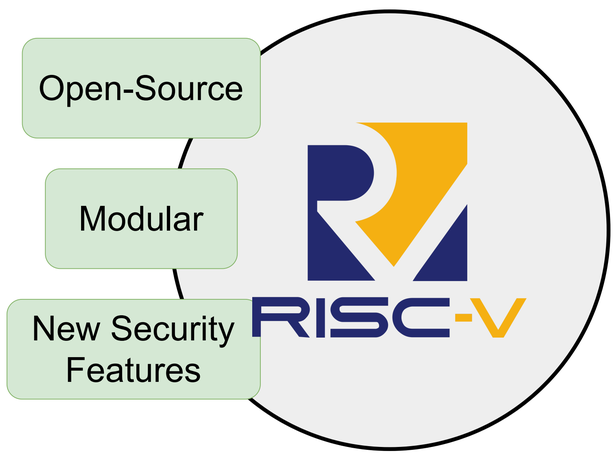
Security assessment methodology for RISC-V cores

Apurba Karmarkar, Pablo Navarro-Torrero, Eros Camacho-Ruiz*, Macarena C. Martínez-Rodríguez, Piedad Brox
Instituto de Microelectrónica de Sevilla, IMSE-CNM, CSIC, US, Spain
camacho@imse-cnm.csic.es

Context and Motivation

- The **Internet of Things (IoT)** has become an integral part of daily life, from homes and workplaces to industrial systems, all of which rely on extensive data sharing.
- Many of these systems use **embedded processors** to perform the majority of tasks.
- In this context, **assessing the security** of these processors is critical to protecting against potential **cyberattacks**.

Why RISC-V in Security ?



Growing use makes **Side Channel resistance** a *must have* for embedded security.

What is a Side-Channel Attack ?

A **side-channel attack (SCA)** is a method used to extract secret information from a system by observing its **physical behavior**.

Timing | **Power consumption** | **Electromagnetic emissions**

Goals

- Define a **Methodology** that will facilitate the evaluation of the **Side Channel resistance** of RISC-V cores.
- Design an **experimental setup** to evaluate the Methodology.
- Test the methodology and the experimental setup using a specific use case.

Methodology

Requirements

- **Independent** on any kind of RISC-V core or compiled program.
- **Flag signal** to indicate the operation

Selection of the **platform test** (SAKURA-X)

Implementation of a generic **communication interface** (UART)

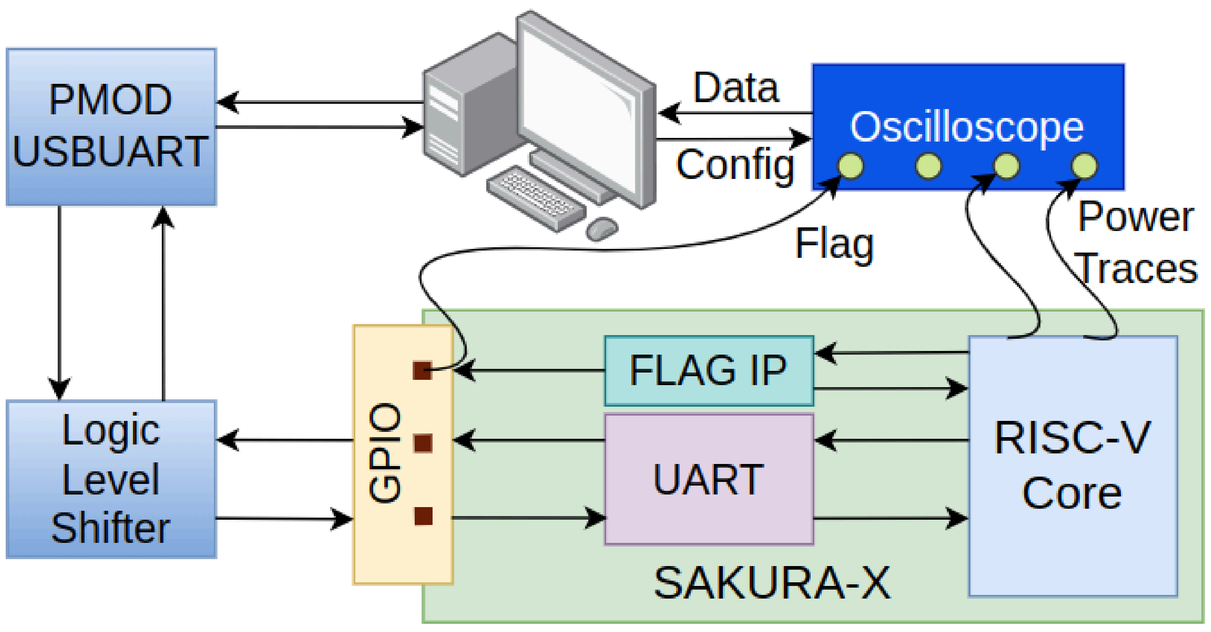
Design of a **Flag hardware module**

Compilation of the **Program Under Test** on the RISC-V Core (baremetal)

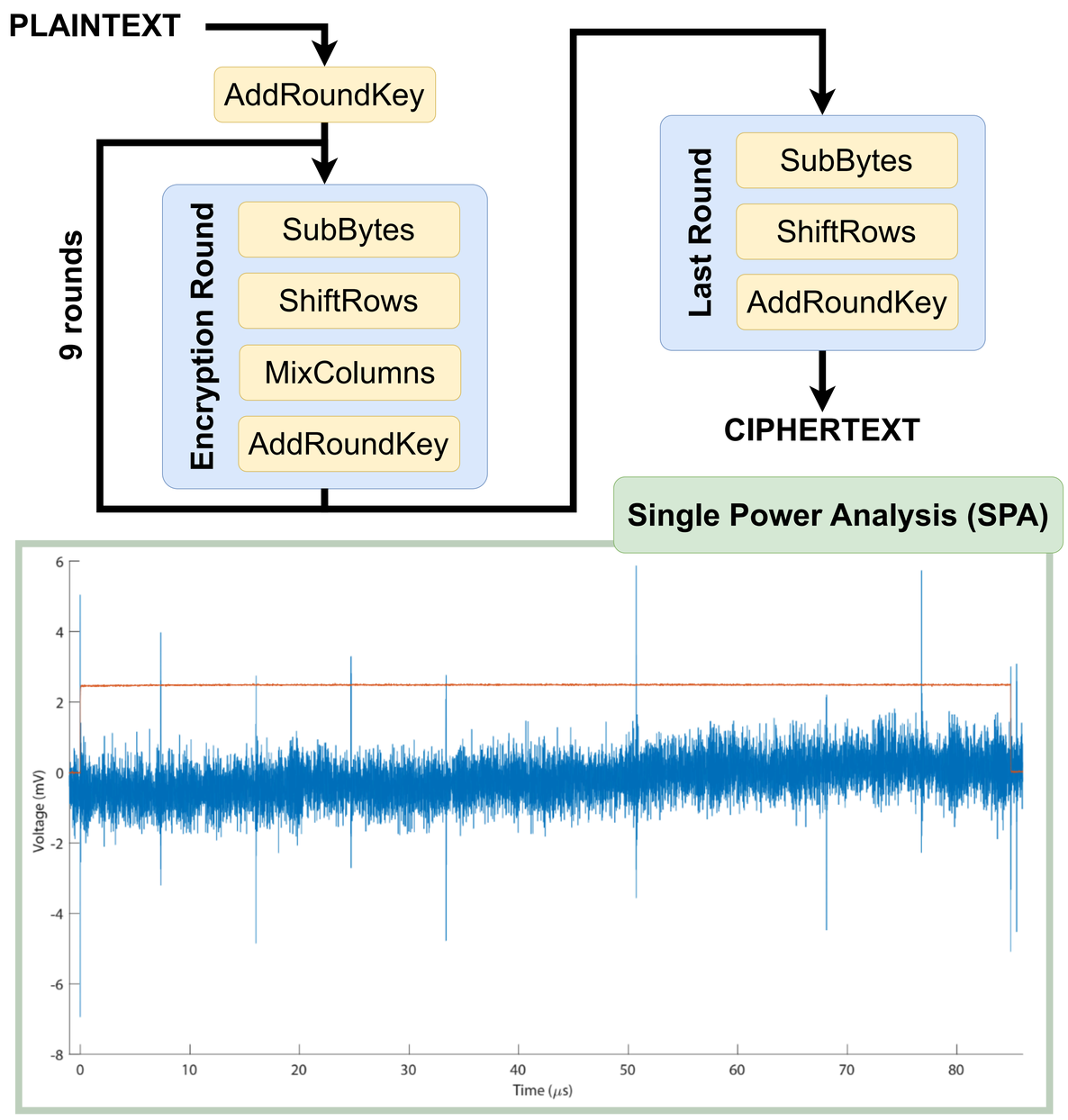
Run the **Analysis** (SPA, DPA or CPA)

Evaluate the results

Experimental Set-up



Use Case: Encryption of AES-128



Conclusions

- A **novel methodology** for evaluating the **security of RISC-V cores** has been presented.
- This methodology is **independent** of any kind of RISC-V core or the compiled program. The present methodology might be also applied to other systems that are not reliant on baremetal, such as operating systems.
- The present study can be used for **deeper evaluations**, such as those pertaining to **DPA or CPA**.
- It is possible to utilise this methodology in order to **facilitate** the development of RISC-V cores that incorporate **countermeasures against Side-Channel Attacks**.

This research was supported in part by the QUBIP Project with Grant Agreement No. 101119746 under the EU Horizon Europe research and innovation programme