TEEOD

Trusted Execution Environments On-Demand via Reconfigurable FPGA

Sérgio Pereira

Advisors:
Prof. Dr. Sandro Pinto
Prof. Dr. Jorge Cabral
Prof. Dr. Mongkol Ekpanyapong

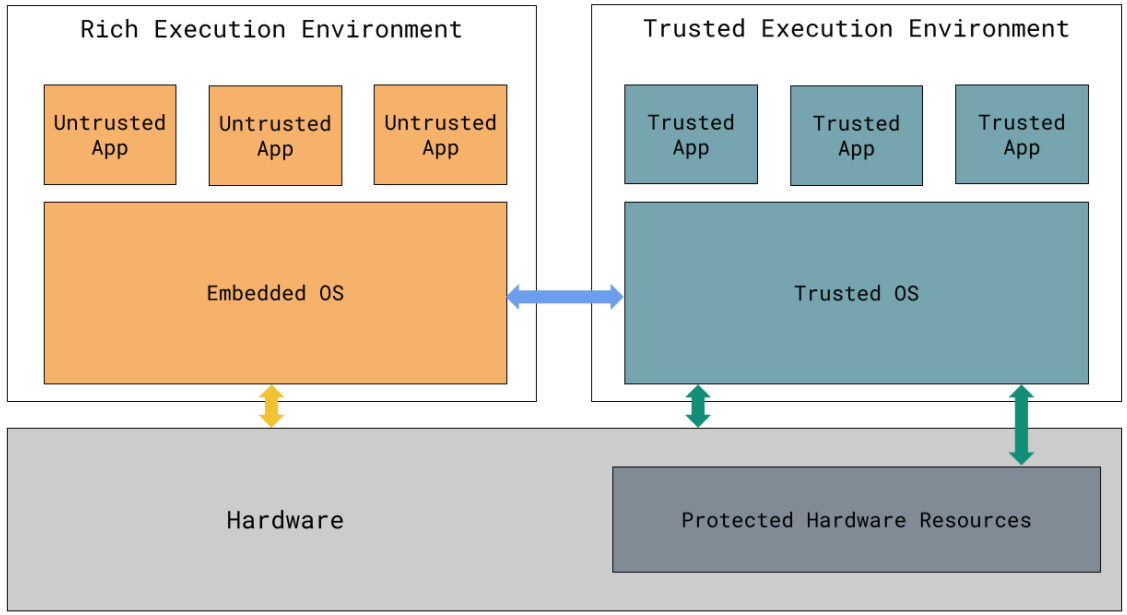
FCT Fundação para a Ciência e a Tecnologia

CENTROALGORITMI

UNIVERSIDADE DO MINHO

The Internet Of Things (IoT) is here.

Trusted Execution Environment (TEE)

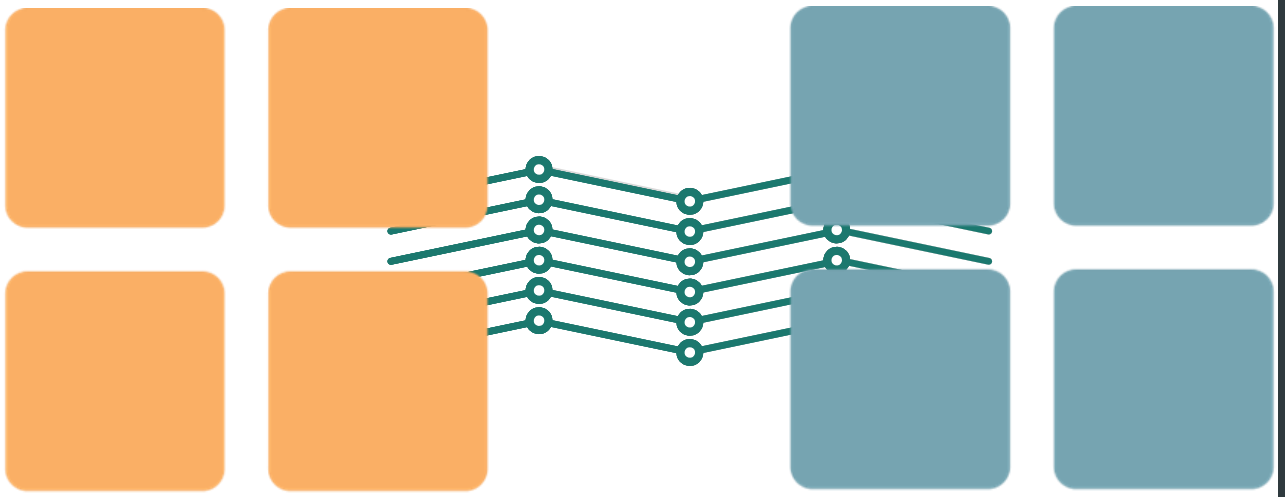


Environment that provides a level of assurance of the following three properties:

- **Data confidentiality:** Unauthorized entities cannot view data while in use within the TEE
- **Data Integrity**: Unauthorized entities cannot add, remove, or alter data while it is in use within the TEE
- **Code integrity:** Unauthorized entities cannot add, remove, or alter code executing in the TEE

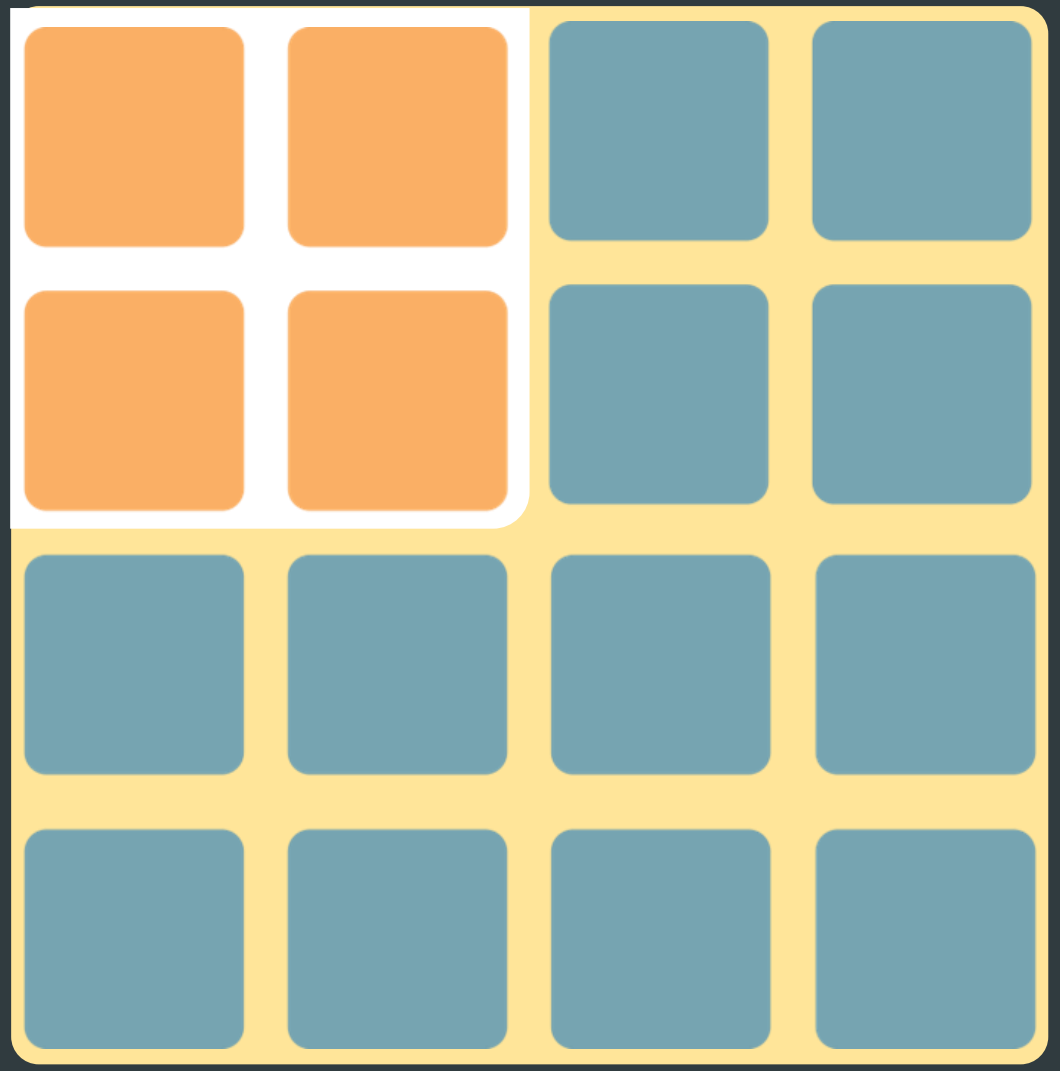
Virtual Secure Processor
Approach

T2



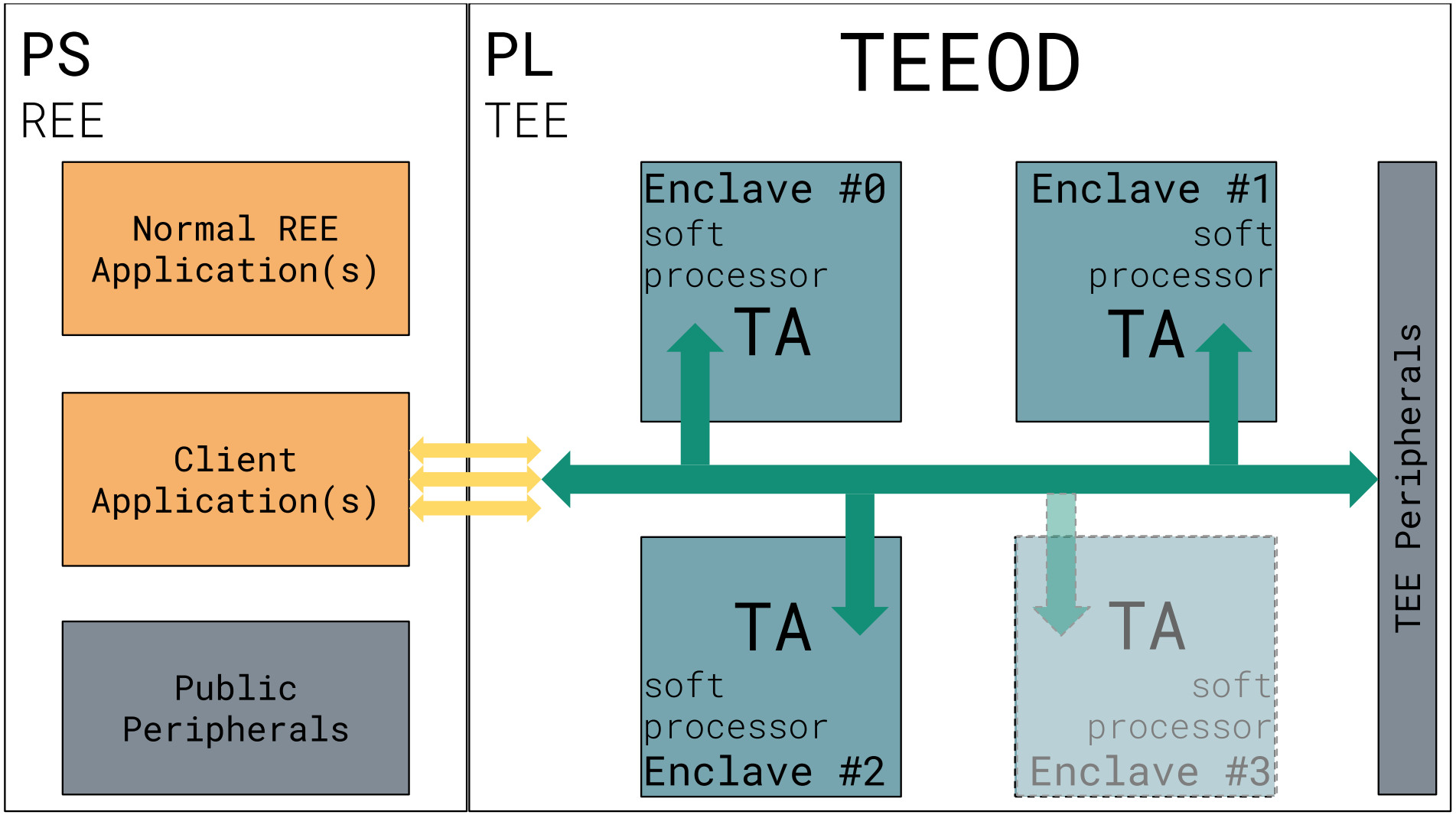
opentitan

Dedicated Secure Processor Approach



Trusted Execution Environments On-Demand

TEEOD approach



MSc Thesis Proposal

DPR-based Secure Cryptographic Solutions

Hardware acceleration solutions of encryption algorithms has been a hot topic

Full hardware implementation is very expensive in terms of area, power and can also deteriorate speed of information transitions

DPR-based Secure Cryptographic Solutions

- Research and develop Advanced Encryption Standard (AES) in hardware;
- Develop a DPR-based system that only loads the algorithm to the PL when it is needed;
- Adapt the implemented algorithm to increase the granularity of the system and thus take even more advantage of DPR's advantages.

THANK YOU!

ANY QUESTIONS?

sergio.pereira@dei.uminho.pt