

TEEOD

Trusted Execution Environments On-Demand via Reconfigurable FPGA

Sérgio Pereira

Advisors:

Prof. Dr. Sandro Pinto

Prof. Dr. Jorge Cabral

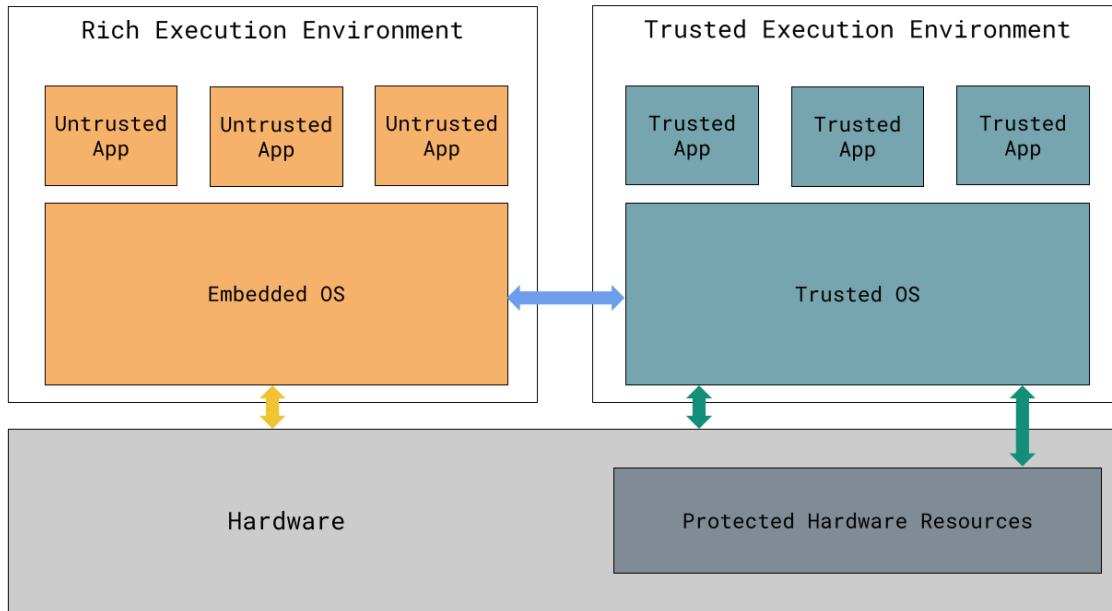
Prof. Dr. Mongkol Ekpanyapong





The Internet Of Things (IoT) is **here**.

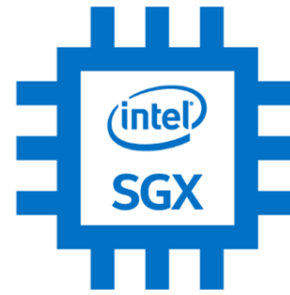
Trusted Execution Environment (TEE)



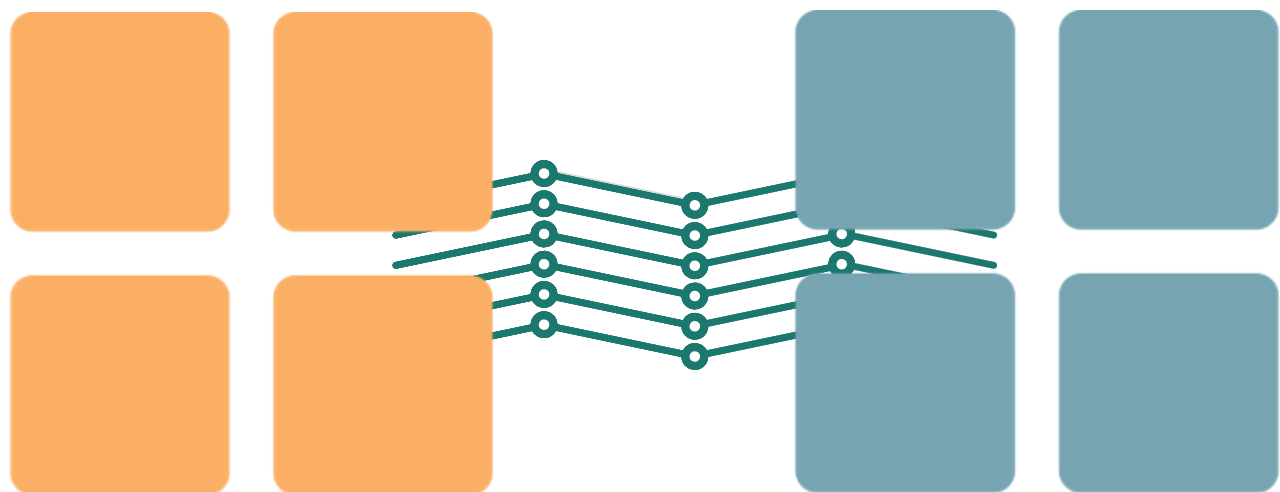
Environment that provides a level of assurance of the following three properties:

- **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

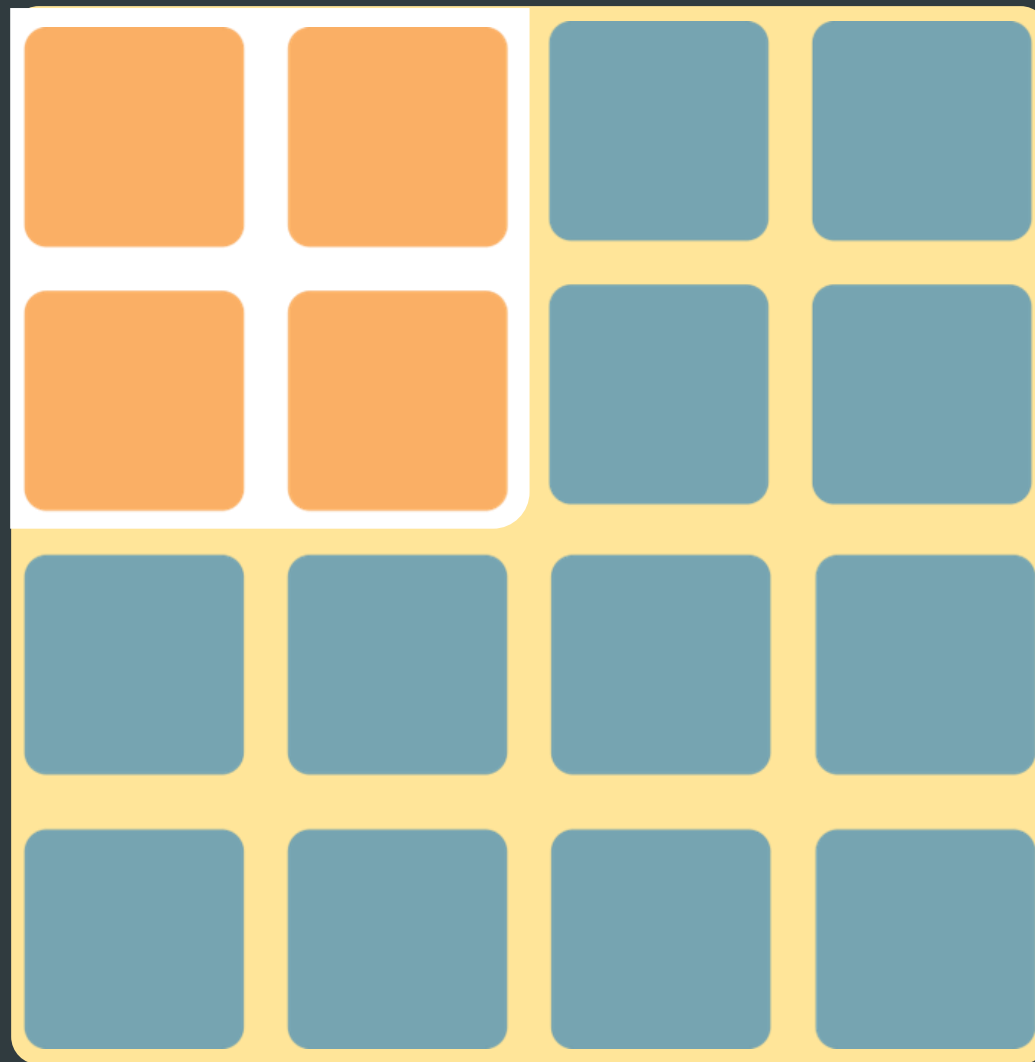


Apple T2



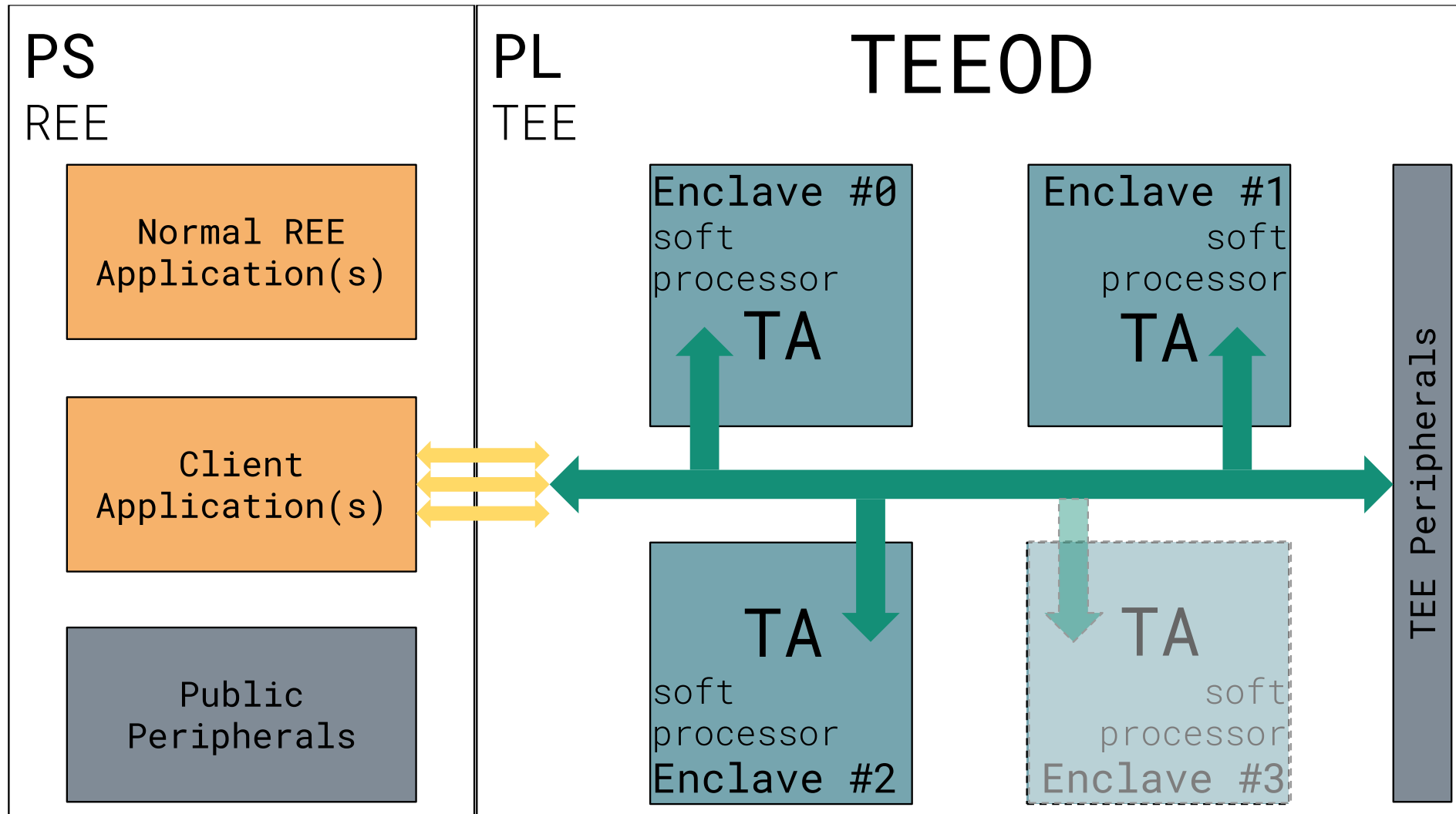
 opentitan

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



ESRGv3

2018 4th International Conference for Convergence in Technology (I2CT)
SDMIT Ujire, Mangalore, India, Oct 27-28, 2018

Scientific Research Publishing
Circuits and Systems, 2017, 8, 237-246
<http://www.iiste.org/journals>
ISSN Online: 2153-1293
ISSN Print: 2153-1285

Designing of AES Algorithm using Verilog

Abstract—On AES, which has of 128bits, 192 method implem 14.7, which red encode and implementation with DES, be modules, in whi method. In a security measur

Key words—

Data transi the main rol communication

Protecting the FPGA IPs against Higher-order Side Channel Attacks using Dynamic Partial Reconfiguration

i Del Rosal, Sanjeev Kumar
Network Security Research Lab, Department of Electrical/Computer Engineering, The University of Texas Rio Grande y, El Paso, USA
i.kumar@utrgv.edu

Fast FPGA Implementation for Triple DES Encryption Scheme

Abstract— cryptography, the Triple DES (3DES, TDES or officially TDEA) is a symmetric-key block cipher which applies the Data Encryption Standard (DES) iter algorithm three times to each data block. Electronic payment systems known to use the TDES scheme for the encryption/decryption of data, and nce faster implementations are of great significance. Field Programmable te Arrays (FPGAs) offer a new solution for optimizing the performance of plications meanwhile the Triple Data Encryption Standard (TDES) offers a nan to secure information. In this paper we present a pipelined implemen-

Abstract—To secure FPGA's erable counter resistance of 1) (DPA) and Co recent years. It which utilizes t erty of the EP DPR capability design on the di interruption. V technology in s runtime to violi analysis attack first-order DPA

A high-speed and s (DPR) system is realia

BITSTREAM ENCRYPTION AND AUTHENTICATION WITH AES-GCM IN DYNAMICALLY RECONFIGURABLE SYSTEMS

Abstract—To secure FPGA's erable counter resistance of 1) (DPA) and Co recent years. It which utilizes t erty of the EP DPR capability design on the di interruption. V technology in s runtime to violi analysis attack first-order DPA

A high-speed and s (DPR) system is realia

Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop

Sheetal U. Jonwal

Hardware Acceleration of the AES Algorithm using Nios-II Processor

Argyrios Sideris
Department of Electrical & Computer Engineering
University of Western Macedonia
Kozani, 50131, Greece
asideris@uowm.gr

FPGA-based design and implementation of reduced AES algorithm

Yang Jun Ding Jun Li Na Guo Yixiong
School of Information Science and Engineering, Yunnan University
Kunming, China

AES hardware implementation in FPGA for algorithm acceleration purpose

Artur Gielata
AGH-UST, Dept. of Ele
Mickiewicza 30, 30-059 Cra
e-mail: gielata@agh.edu.pl

Development of Dynamic Reconfiguration Implementation of AES on FPGA Platform

Shuchishman Burman * P. Rangababu* Kamalika Datta[†]
* Department of Electronics and Communication Engineering, National Institute of Technology Meghalaya, Shillong 793003, Meghalaya India
[†] Department of Computer Science and Engineering, National Institute of Technology Meghalaya, Shillong 793003, Meghalaya India
Email: shuchishmanburman@gmail.com, [p.rangababu, kdatta]@nitm.ac.in

Hardware Acceleration of the AES Algorithm using Nios-II Processor

Abstract—Nowadays, cryptography plays both transmitting and receiving sensitive i any unauthorized person does not have ac Encryption Standard (AES) is the most encryption algorithm widely used in many document, we present the implementation of in Very High Speed Integrated Circuit Ha language (VHDL) programming language w bit key sizes using the Nios II processor in the (10AX115N2F45E1SC). We implemented tw custom instruction and with floating point the two implementations the three AES ke integration time, number of cycle clocks, an used hardware resources (LUTs used in the have shown that, the larger key size, requir and longer integration time as well. Implemen Point 2 shows over 11.07% acceleration in d time on all key sizes. The results of two ti compared with existing similar designs and i better performance.

Index Terms—Cryptography, Advanced E (AES), NIOS II Processor, SOPC Builder, wware Implementation.

I. INTRODUCTION

Today, in order to increase performan graphic algorithms are implemented in h years, the use of FPGAs has increased signi architectures have been used for this purpos ally intensive algorithms, like AES. The replaced the Double Encryption Standard been adopted as a standard for symmetric e National Institute of Standards and Techno constitutes the most commonly used symm algorithm in many applications such as Smar Teller Machines (ATM), Magnetic Cards, SSD Device [3].

As a symmetric cryptographic algorithm and decrypt information. The process of

Development of Dynamic Reconfiguration Implementation of AES on FPGA Platform

Abstract—Dynamic partial reconfiguration is the ability of modern FPGA's to dynamically change some selected area(s) of the FPGA while rest of the device is running. This feature allows to reuse the same hardware for different applications. In this paper we have chosen various Advanced Encryption Standard (AES) key sizes, viz. 128-bit, 192-bit and 256-bit as parameter for reconfiguration. A dynamic reconfigurable implementation for high speed and low area AES has been developed on Digilent's Zed board (XC7Z020-1-G484-1). The proposed work implements two pipelined versions of AES for reconfiguration, (i) High speed version using modular pipelining, (ii) Area efficient version using simpler pipeline. Maximum operational frequencies of 389.25, 389.25 & 386.2 MHz have been achieved using modular pipelined

Abstract—This paper in algorithm and the detail on FPGA. This system ai Compared with the pipel resources and high cost high security and reliabi used in the terminal equi

Keywords—AES; FPGA; V

I. IN

With the developm cryptanalysis, the DES algorithm is already no Encryption Standard) becomes the new stan supported by a few inter AES algorithm is wide domestic, such as reali POS, ATM, magnetism

On the current situ abroad^[1,2], AES algo using pipeline pattern improve the system t disadvantage that is at in accordance that AE requirements of the ter high safety and cost-e designed and valida

Development of Dynamic Reconfiguration Implementation of AES on FPGA Platform

Abstract—Dynamic partial reconfiguration is the ability of modern FPGA's to dynamically change some selected area(s) of the FPGA while rest of the device is running. This feature allows to reuse the same hardware for different applications. In this paper we have chosen various Advanced Encryption Standard (AES) key sizes, viz. 128-bit, 192-bit and 256-bit as parameter for reconfiguration. A dynamic reconfigurable implementation for high speed and low area AES has been developed on Digilent's Zed board (XC7Z020-1-G484-1). The proposed work implements two pipelined versions of AES for reconfiguration, (i) High speed version using modular pipelining, (ii) Area efficient version using simpler pipeline. Maximum operational frequencies of 389.25, 389.25 & 386.2 MHz have been achieved using modular pipelined

Abstract—This paper in algorithm and the detail on FPGA. This system ai Compared with the pipel resources and high cost high security and reliabi used in the terminal equi

Keywords—AES; FPGA; V

I. IN

With the developm cryptanalysis, the DES algorithm is already no Encryption Standard) becomes the new stan supported by a few inter AES algorithm is wide domestic, such as reali POS, ATM, magnetism

On the current situ abroad^[1,2], AES algo using pipeline pattern improve the system t disadvantage that is at in accordance that AE requirements of the ter high safety and cost-e designed and valida

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