IEEE EI^2 2022 ▸ Chengdu, China ‖ November 11-13, 2022

IEEE EI^2 2022

Paper ID: EI0377

A RISC-V System-on-Chip Based on Dual-core Isolation for Smart Grid Security

Chen Chen, Qimin Yuan, Xiaowen Jiang, Kai Huang, Peng Li, Wei Xi

浙江大学 1897 ZHEJIANG UNIVERSITY

The 6th IEEE Conference on Energy Internet and Energy System Integration

Background

- With the construction of digital power grids, **a large number of smart power terminals with low security level makes power grid easier to face secure risks.**

Distributed Generation

Smart Transmission

Power IoT

Smart Distribution

terminal security

Malware

Computer virus

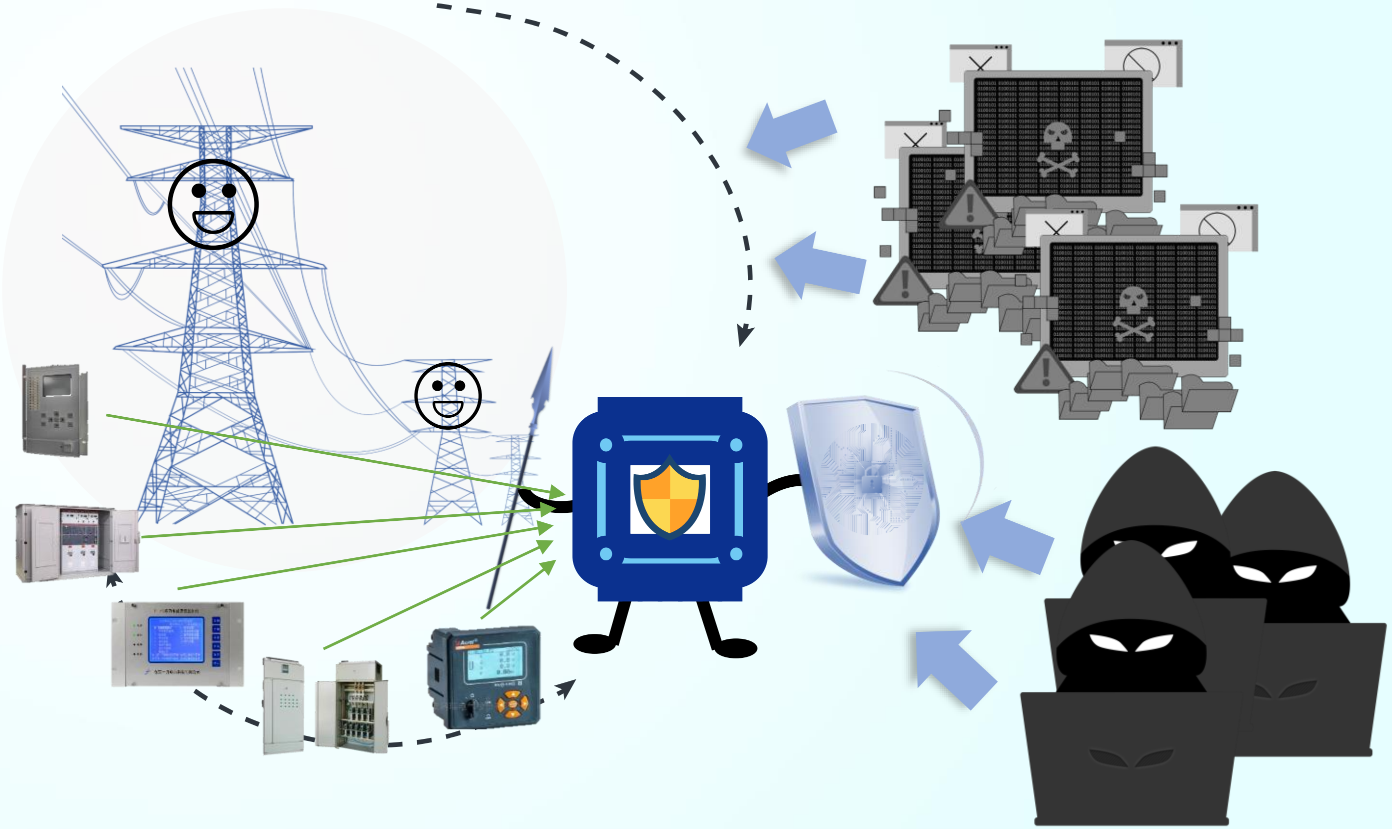
Hacking

Background

- In order to protect the terminal devices and build a secure and reliable power grid, it is very important to **ensure the security of the chip**.

Chip in terminals

- data storage
- information transmission
- peripheral control



Traditional Implementations

Software Security Protection

use the operating system for security access control

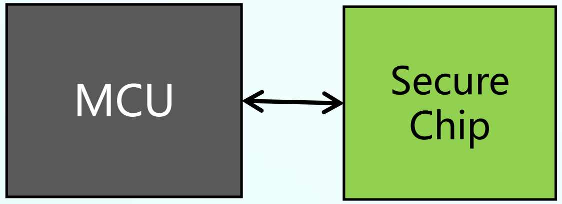
⚠ memory leakages or tampering problem

Hardware Security Protection

Intel SGX
ARM TrustZone

⚠ The Virtual Processer form is difficult to meet the needs of real-time services

External Secure Processor



⚠ The communication channel between the secure elements is vulnerable

→ **Security**

→ **Efficiency**

Traditional implementations

Security **Efficiency**

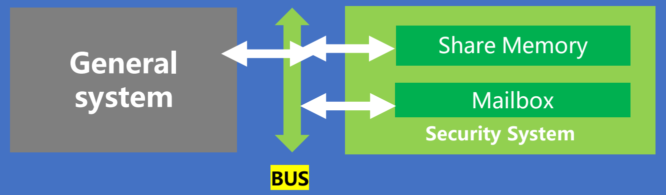
Internal secure processor
both high security and high performance
Apple with its Secure Enclave Processor(SEP)

Power Domain

In the power security system, it is common to focus on protecting the external communications that are more vulnerable to attacks, while **neglecting the security of the internal communications**
e.g. I2C bus attackment[1], UART bus attackment[2]

Our method

A System-on-Chip Based on Dual-core Isolation



- Dual Core for high level secure
- Encryption and decryption
- Secure boot
- Secure serial ports and authentication mechanisms

[1]M. A. Khelif, J. Lorandel and O. Romain, "Non-invasive I2C Hardware Trojan Attack Vector," 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2021, pp. 1-6, doi: 10.1109/DFT52944.2021.9568347.
[2]A. Gupta, The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things. Apress*, 2019.

Secure SoC Architecture

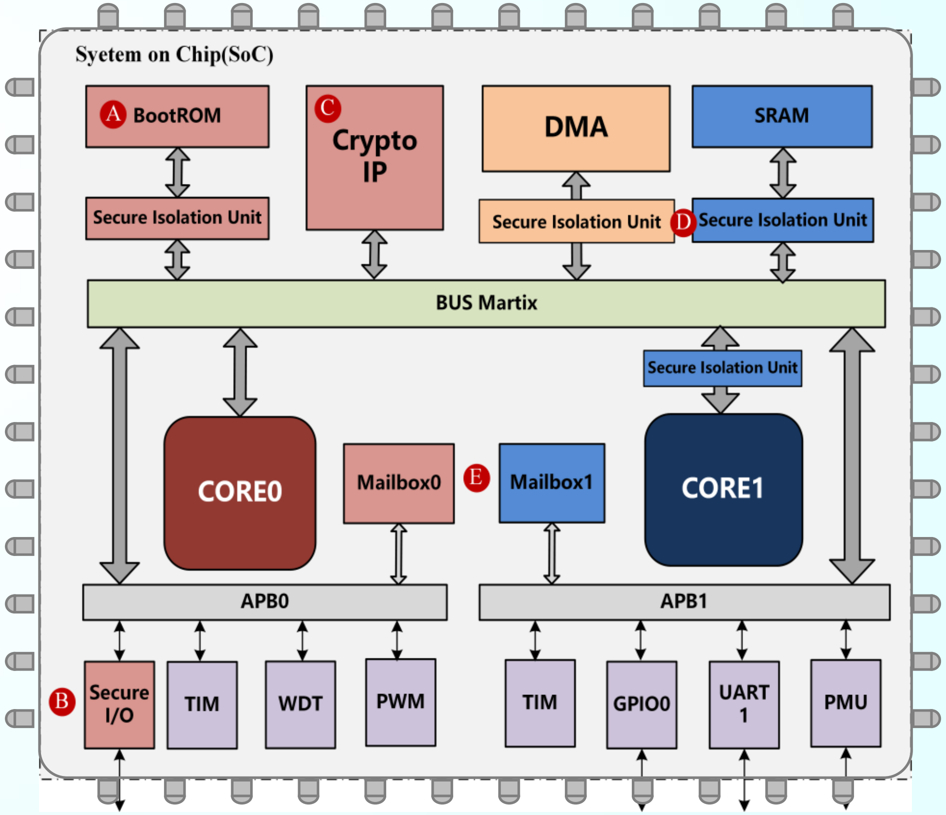
- The power domain-specific secure SoC adopts a **dual-core design** that divides the system into a **security subsystem** and a **general computing system.**

security subsystem

- secure core (Core 0)
- BootROM
- Secure I/O
- Crypto IP

general computing system

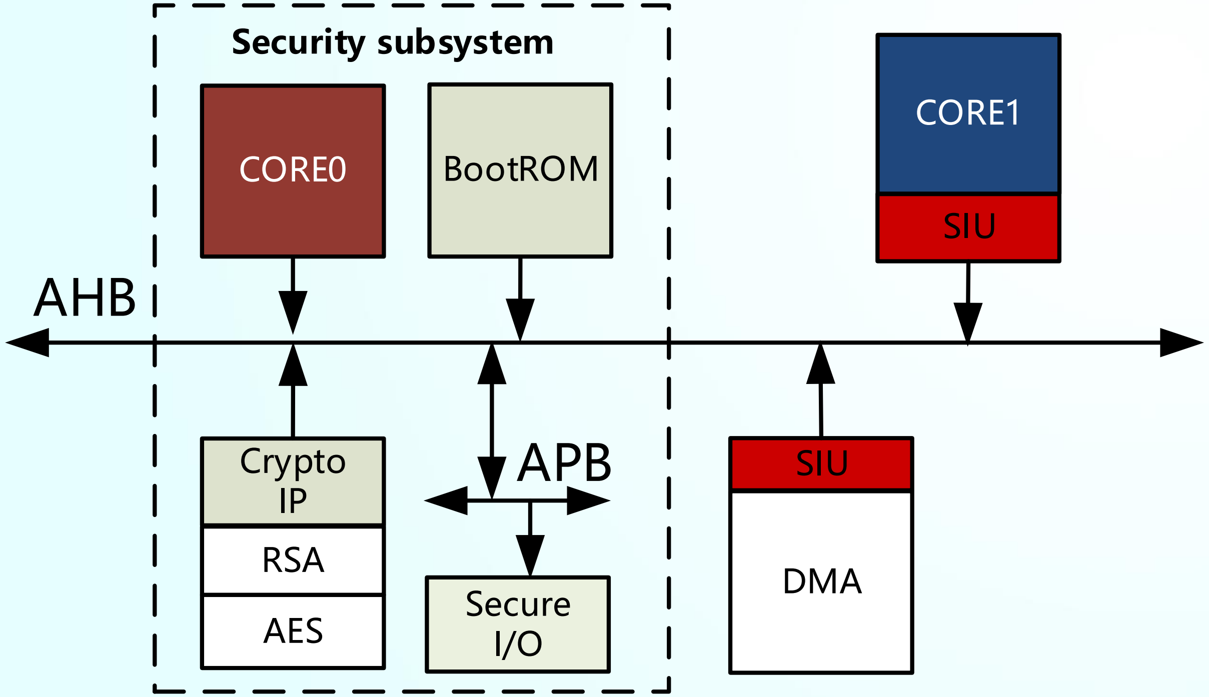
- non-secure core (Core 1)
- SRAM
- general peripherals



Secure SoC Architecture

• Dual-core Isolation mechanism

➢ General core and secure core are connected by the shared bus, and **the secure isolation unit** is used to achieve the isolation of resources and access control



Secure Isolation Unit (SIU)

- Control the isolation of the storage units and peripherals
- Use address tags to determine the validity of current access behavior

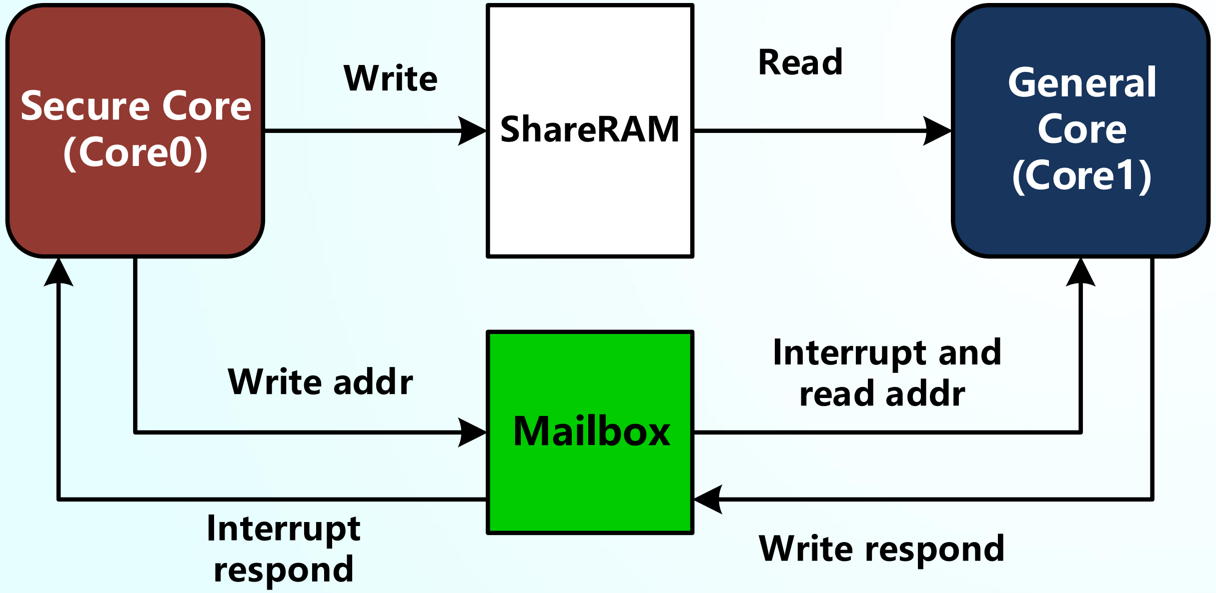
✓ **Shared bus** guarantees the flexibility of the system and maximizes the use of peripherals and other hardware resources

✓ **SIU ensures the secure isolation**

Secure SoC Architecture

• Dual-core Communication

➢ Communication between secure core and general core takes place via **Mailbox** and **ShareRAM**



Mailbox ONLY

✓ Ensure the data security in secure core

Shared memory-based method

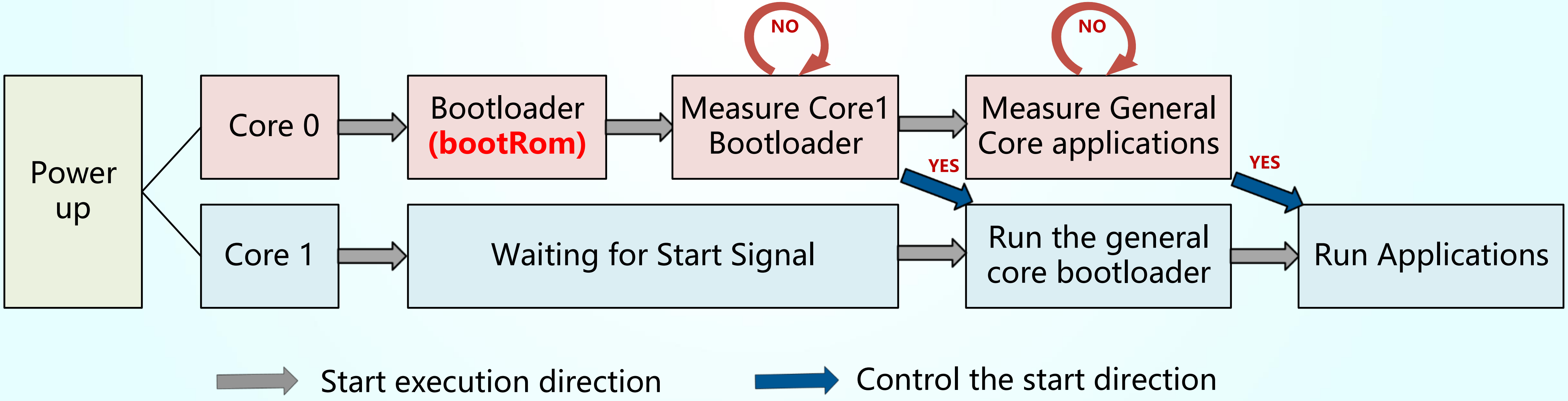
✓ high transmission efficiency and large data volume

Secure Protocols

- **Dual-core secure boot**

➢ When the SoC is powered on, the security of other nodes is unknown except for the trusted root. Each node must be verified by the previous trusted node before it can be trusted.

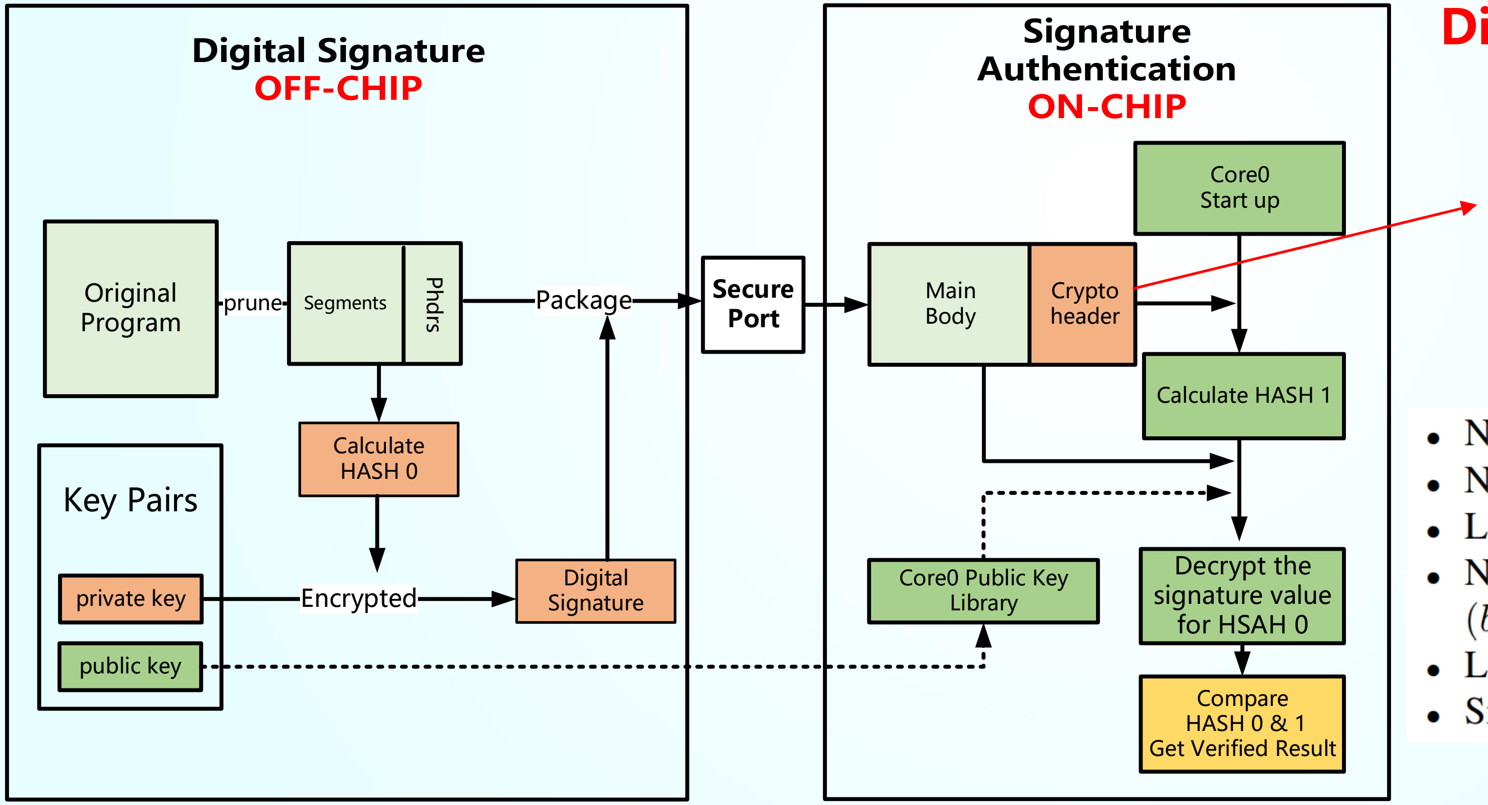
➢ The immutable BootROM in security subsystem is used as the trusted root.


Power up
Core 0
Bootloader (bootRom)
Measure Core1 Bootloader
NO
YES
Measure General Core applications
NO
YES
Core 1
Waiting for Start Signal
Run the general core bootloader
Run Applications
Start execution direction
Control the start direction

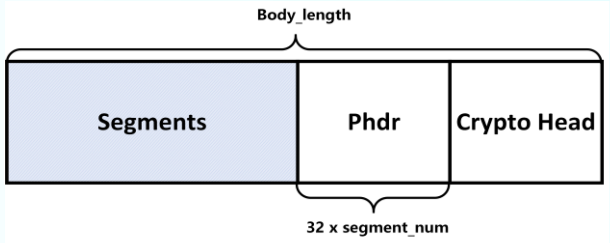
Secure Protocols

- **Secure serial loading**

➢ The secure core authenticates the transmitted program which is digitally signed.



Digital Signature



output data

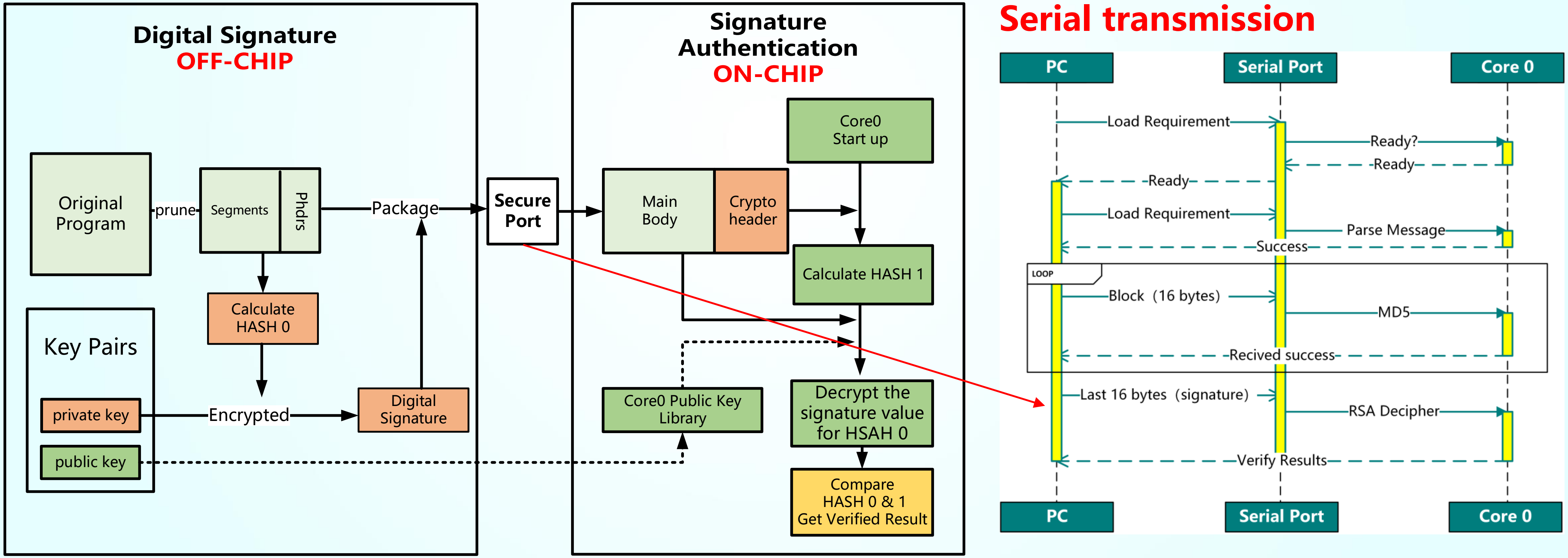
Crypto Head

- Number of Key-pair
- Number of segments (related to the program)
- Length of the program body
- Number of blocks after 16-bits padding: $block\_num = (body\_length + 15)/16$
- Length of the signature
- Signature value

Secure Protocols

- **Secure serial loading**

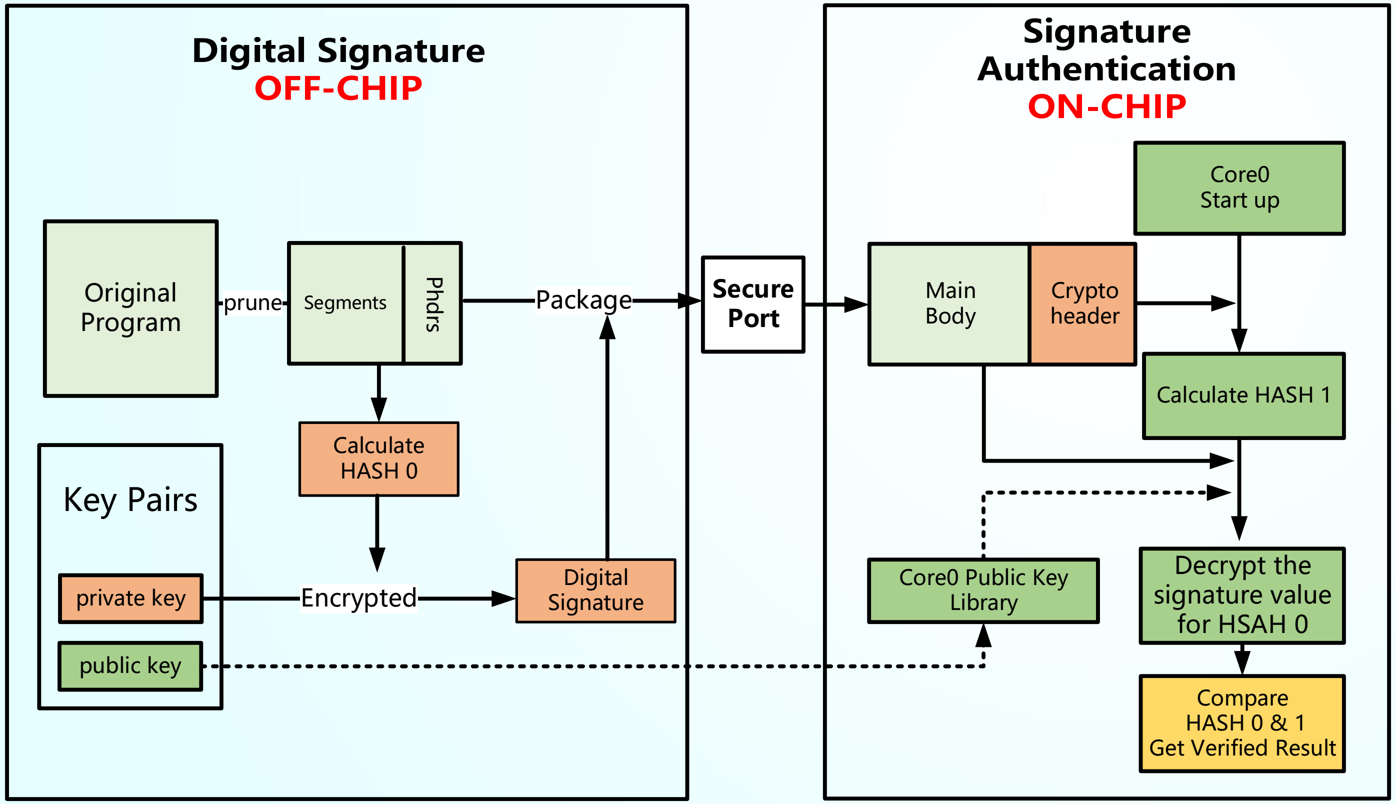
➢ The secure core authenticates the transmitted program which is digitally signed.



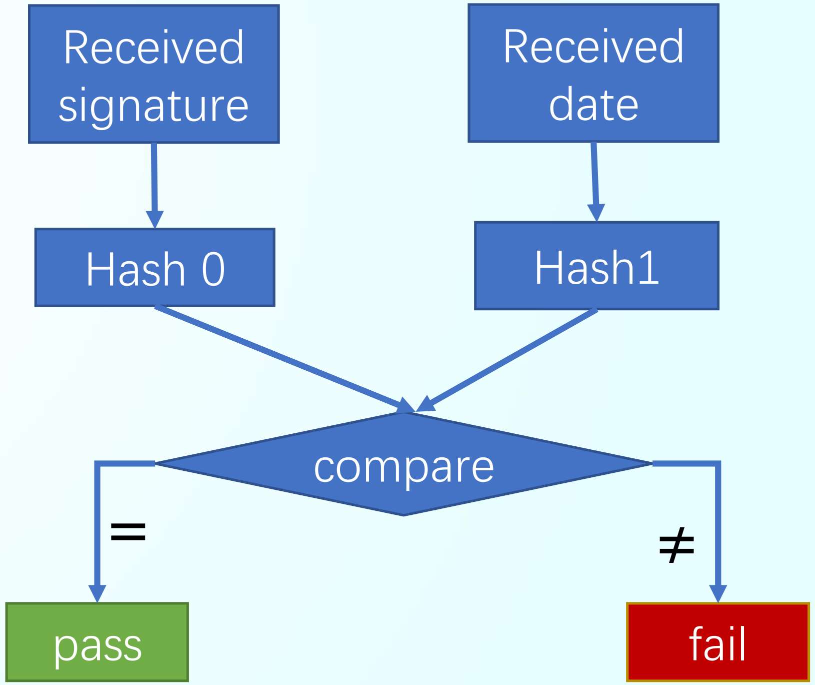
Secure Protocols

• Secure serial loading

➢ The secure core authenticates the transmitted program which is digitally signed.



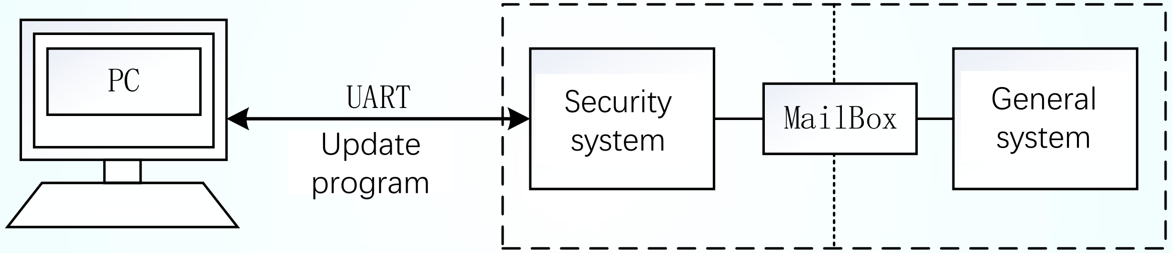
Digital Signature Authentication



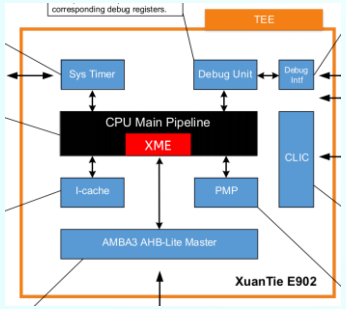
Experiments and Results

- An application example

➢ Scene：Terminal application upgrade



➢ Platform



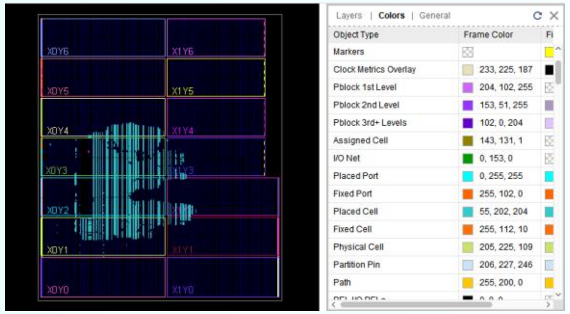
Xuantie E902

Xilinx Kintex-7 FPGA开发板

wujian100

Experiments and Results

- **Area**
  - ➢ we pay **40%** additional hardware cost for the dual-core and security needs



Object Type	Frame Color	Fi
Markers	▨	■
Clock Metrics Overlay	■ 233, 225, 187	■
Pblock 1st Level	■ 204, 102, 255	▨
Pblock 2nd Level	■ 153, 51, 255	■
Pblock 3rd+ Levels	■ 102, 0, 204	■
Assigned Cell	■ 143, 131, 1	▨
I/O Net	■ 0, 153, 0	▨
Placed Port	■ 0, 255, 255	■
Fixed Port	■ 255, 102, 0	■
Placed Cell	■ 55, 202, 204	■
Fixed Cell	■ 255, 112, 10	■
Physical Cell	■ 205, 225, 109	■
Partition Pin	■ 206, 227, 246	■
Path	■ 255, 200, 0	■

Table1. Lookup Table (LUT) Overhead of The Duel-Core Secure SoC Architecture Compared to The Single E902 Base Platform

Configuration	Area[LUTs]	Area OverHead
single E902 base platform	27113	-
duel-core secure SoC	38103	40.53%

- **Performance**
  - ➢ The secure serial port has a negligible impact on the data transmission rate(**less than 1%**)

$$RateImpact(\%) = \frac{nonSecureRate - SecureRate}{nonSecureRate} \times 100\%$$

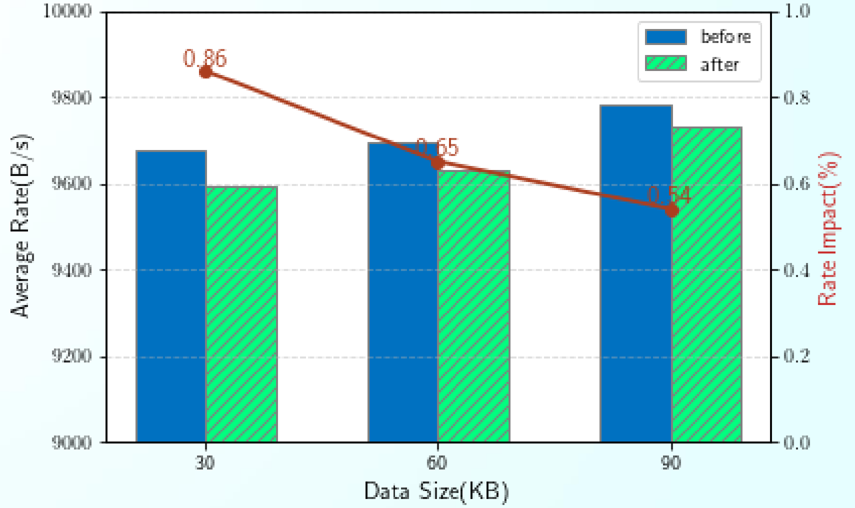
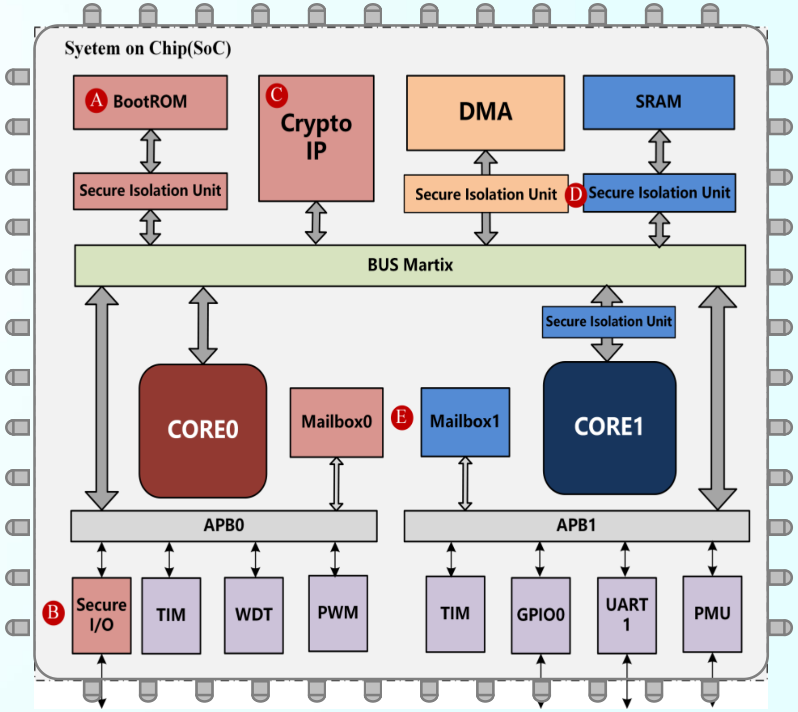


Fig1. The Results of Serial Port Transmission Time

Conclusion

We proposes a dual-core secure System-on-Chip (SoC) architecture for power terminal application scenarios

- The secure elements can implement **data encryption** and **decryption**, **identity authentication** that provide strong security guarantees for electrical equipment.
- **Dual-core secure boot** is realized through trusted root and transmission
- Considering the secure transmission requirements of the power terminal, the **secure serial port** with authentication is realized.



In future, We will use the good scalability of RISC-V to implement more secure functions for power domain

Thanks for your listening!

Q&A Time

《A RISC-V System-on-Chip Based on Dual-core Isolation for Smart Grid Security》

Chen Chen, Qimin Yuan, Xiaowen Jiang, Kai Huang, Peng Li, Wei Xi

Paper ID: EI0377

A RISC-V System-on-Chip Based on Dual-core Isolation for Smart Grid Security

Chen Chen, Qimin Yuan, Xiaowen Jiang, Kai Huang, Peng Li, Wei Xi

浙江大学 1897 ZHEJIANG UNIVERSITY