UEC 国立大学法人 電気通信大学 The University of Electro-Communications

Pham Laboratory
Integrated circuit design laboratory

RISC-V Day Tokyo 2024 Winter

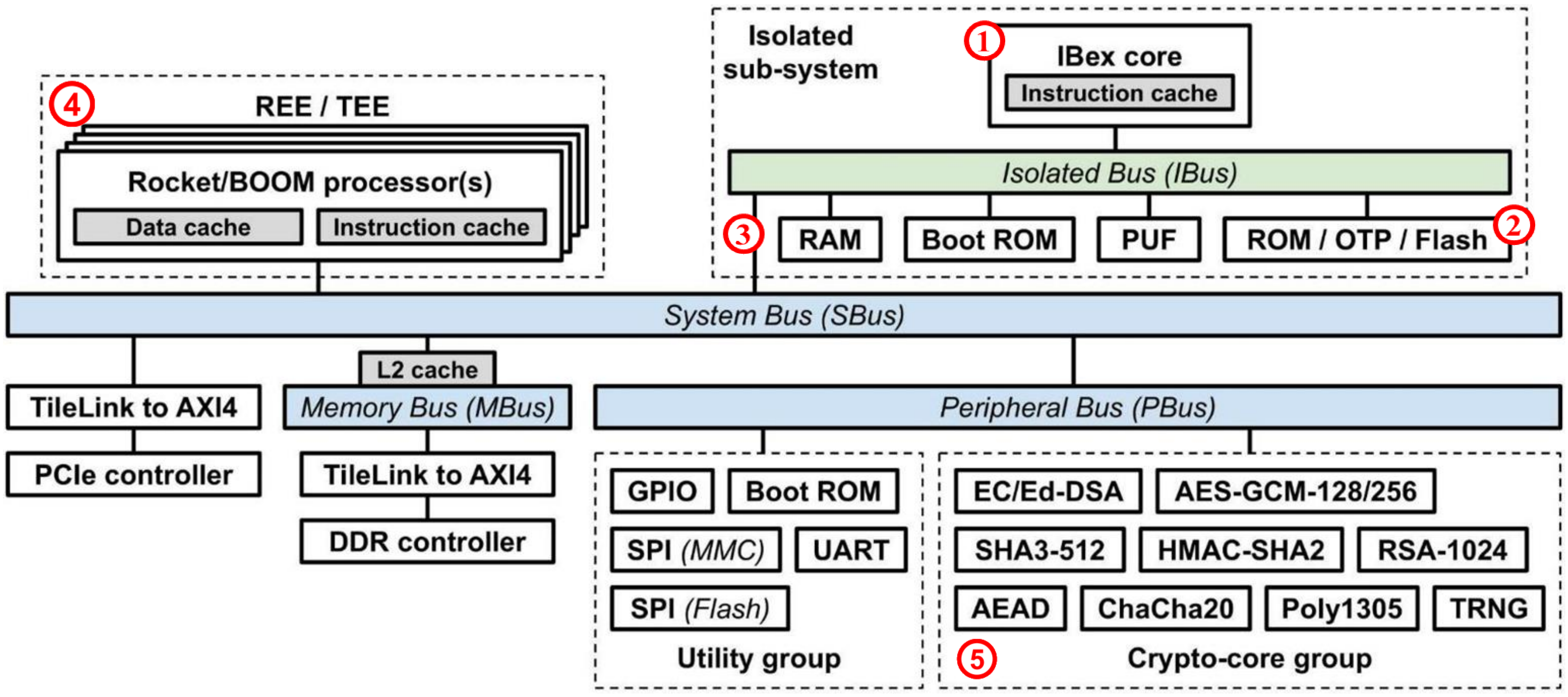
Live Demonstration: Linux-bootable Trusted Execution Environment (TEE) System-on-chip (SoC) with Cryptographic Accelerators

Tuan-Kiet Dang, Trong-Thuc Hoang, Cong-Kha Pham
The University of Electro-Communications (UEC), Tokyo, Japan

ABSTRACT

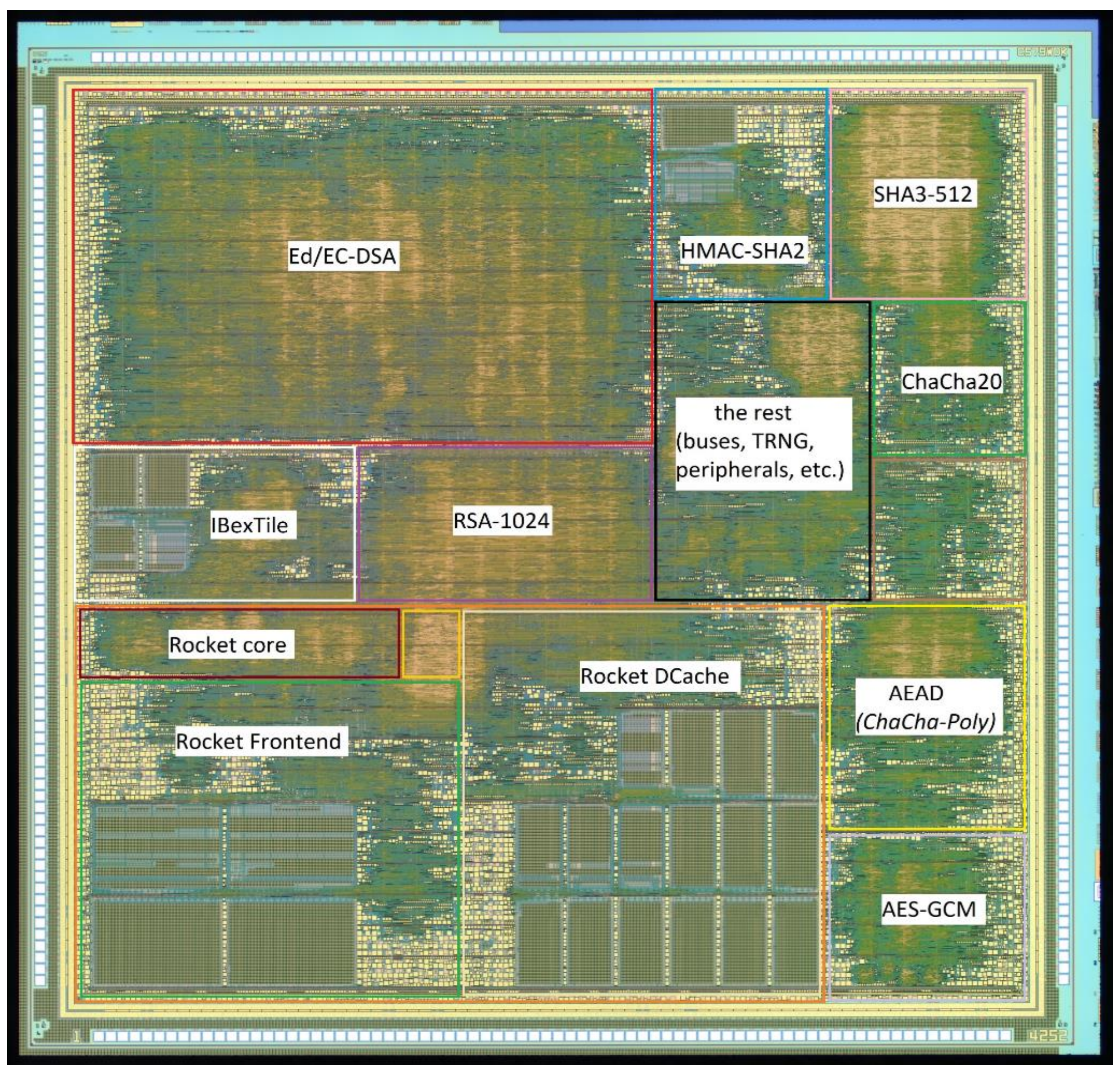
In this demonstration, a silicon-proof System-on-Chip (SoC) is presented. The demo can boot into Linux with multiple cryptographic accelerators. The proposed architecture consists of one IBex core and one Rocket core for the secure boot process and the Trusted Execution Environment (TEE). The crypto-cores are Transport Layer Security (TLS)-1.3-ready. The demo was set up with one ROHM-180nm chip and one Field-Programmable Gate Array (FPGA). The FPGA provides power, clock, and primary Double Data Rate (DDR) memory for the ROHM-180nm SoC. The boot terminal is shown via UART serial printing.

I. ARCHITECTURE

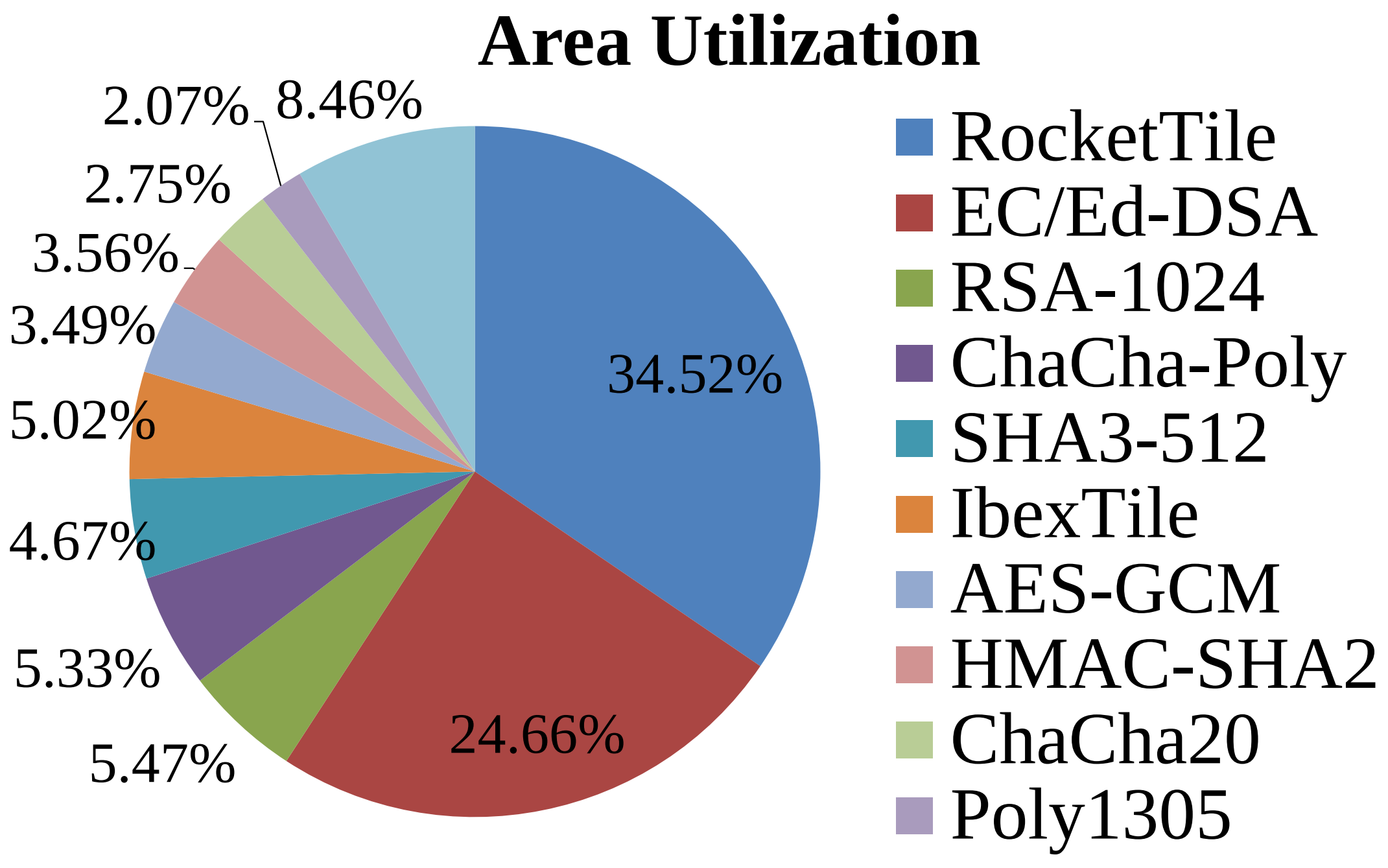


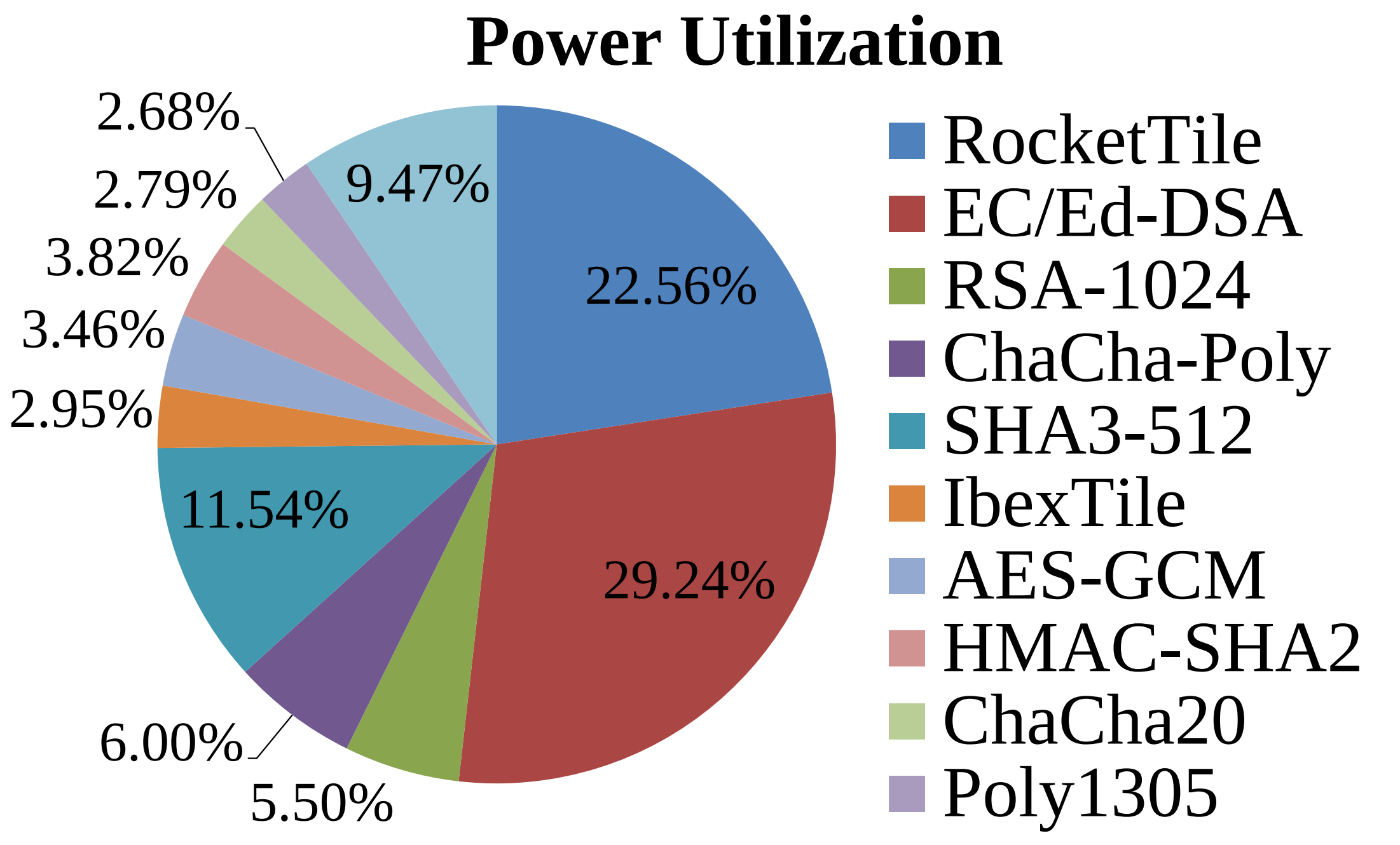
1. Hidden MCU for secure boot program
2. Exclusive storage for root key
3. Hierarchy-bus for preventing sensitive data access after boot
4. High-performance processor(s) for TEE or REE after boot
5. Many cryptography accelerators for multi-purpose crypto-system

II. IMPLEMENTATION

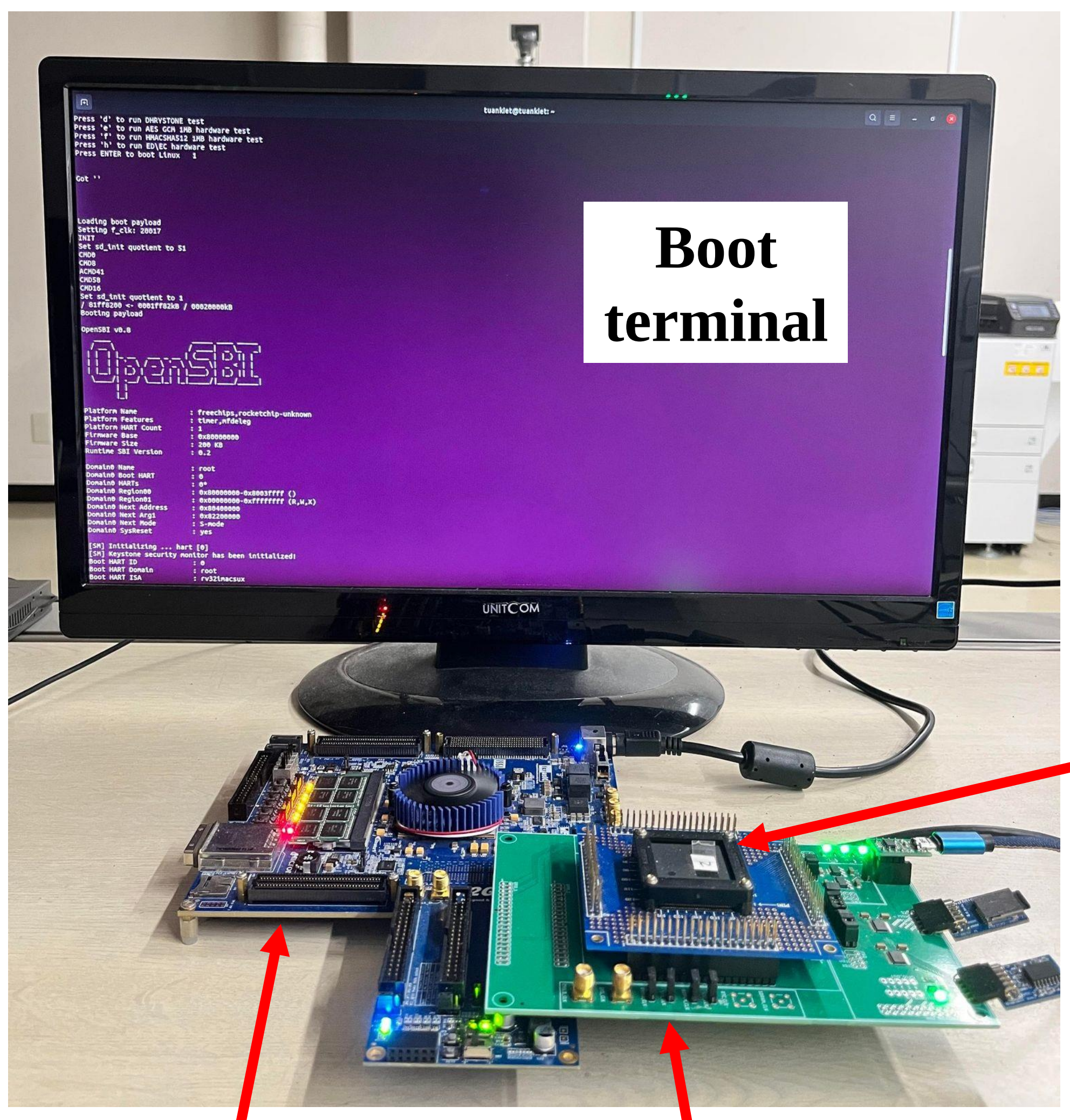


5.0×5.0-mm2 ROHM-180nm on *2022/02*	
Core	Rocket (×1)
ISA	RV32IMAC
Cache	\$I =16KB and \$D = 16KB
Crypto-cores: TRNG, RSA, AES-GCM, SHA3, HMAC-SHA2, ChaCha20, Poly1305, AEAD, and EC/Ed-DSA	
#Gate	1,535,403
#Cell	466,882
Area (μm^2)	20,799,437
Density	71.43%
Power (mW)	1,992
Fmax (MHz)	71
#MOSFET	7,982,582





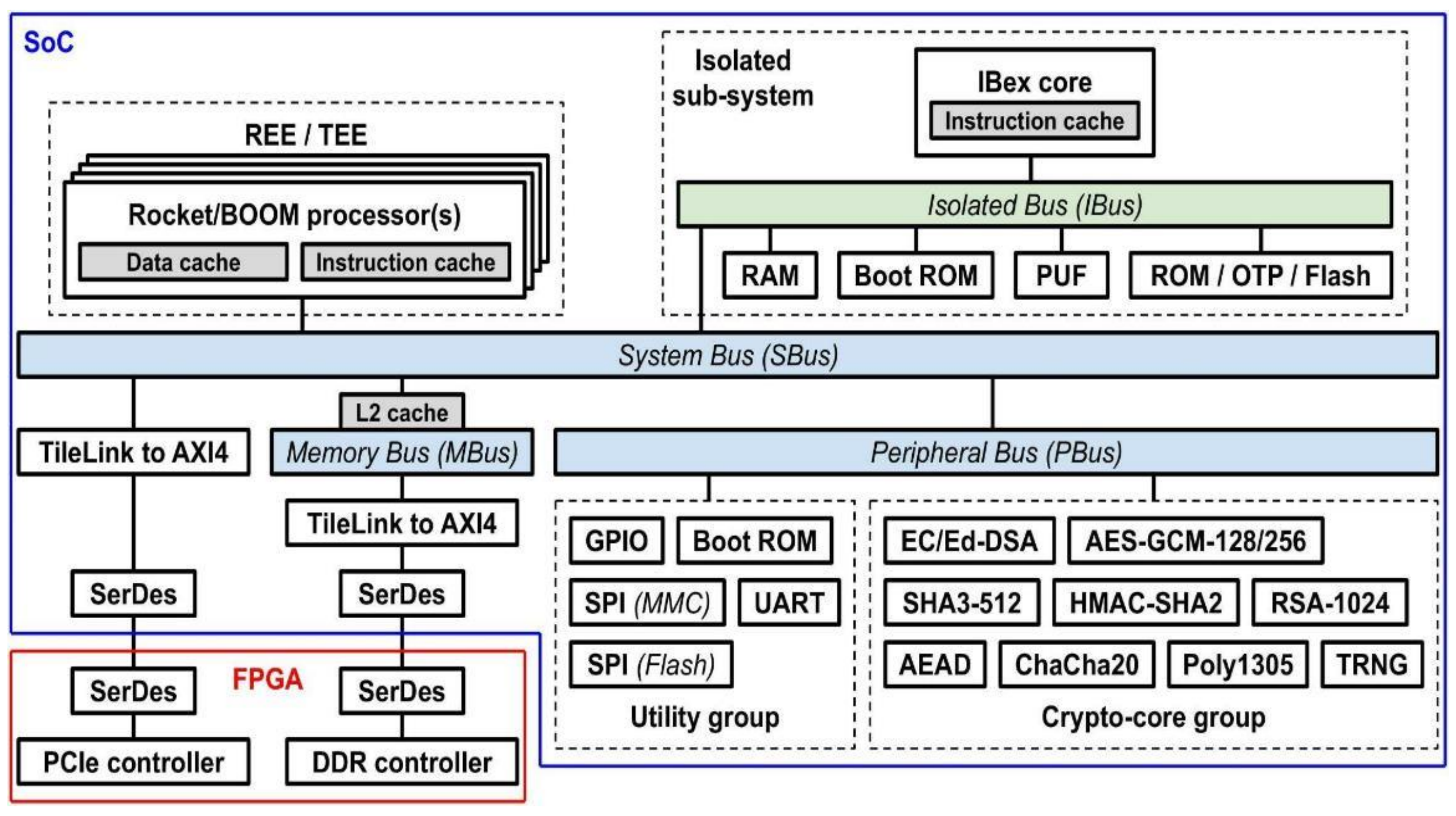
III. DEMO SETUP



Chip

FPGA for *power*, *clock*, and *DDR memory*

PCB for other utilities



REFERENCES

[1] T.-T. Hoang, *et al.*: Trusted Execution Environment Hardware by Isolated Heterogeneous Architecture for Key Scheduling, *IEEE Access*, 2022.

[2] D. Lee, *et al*: Keystone: An Open Framework for Architecting Trusted Execution Environments, *EuroSys*, 2020.

[3] B. K.-D.-Nguyen, *et al*: Multi-Functional Resource-Constrained Elliptic Curve Cryptographic Processor, *IEEE Access*, 2023.

[4] R. Serrano, *et al*: ChaCha20-Poly1305 Crypto Core Compatible with Transport Layer Security 1.3, *ISOCC*, 2021.

[5] R. Serrano, *et al.*: A Robust and Healthy Against PVT Variations TRNG Based on Frequency Collapse, *IEEE Access*, 2022.

[6] R. Serrano, *et al.*: In-NVRAM Unified PUF and TRNG Based on Standard CMOS Technology, *ISCAS*, 2023.

ACKNOWLEDGEMENT

The chip in this study has been fabricated through the activities of VDEC, the University of Tokyo in collaboration with Cadence Design Systems, Mentor Graphics, ROHM Corporation, and Toppan Printing Corporation.

hoangtt@uec.ac.jp