System-on-Chip Implementation of Trusted Execution Environment with Heterogeneous Architecture

Trong-Thuc Hoang[1,2], Ckristian Duran[2], Ronaldo Serrano[2], Marco Sarmiento[2],
Khai-Duy Nguyen[2], Akira Tsukamoto[1], Kuniyasu Suzaki[1,3], and Cong-Kha Pham[2]

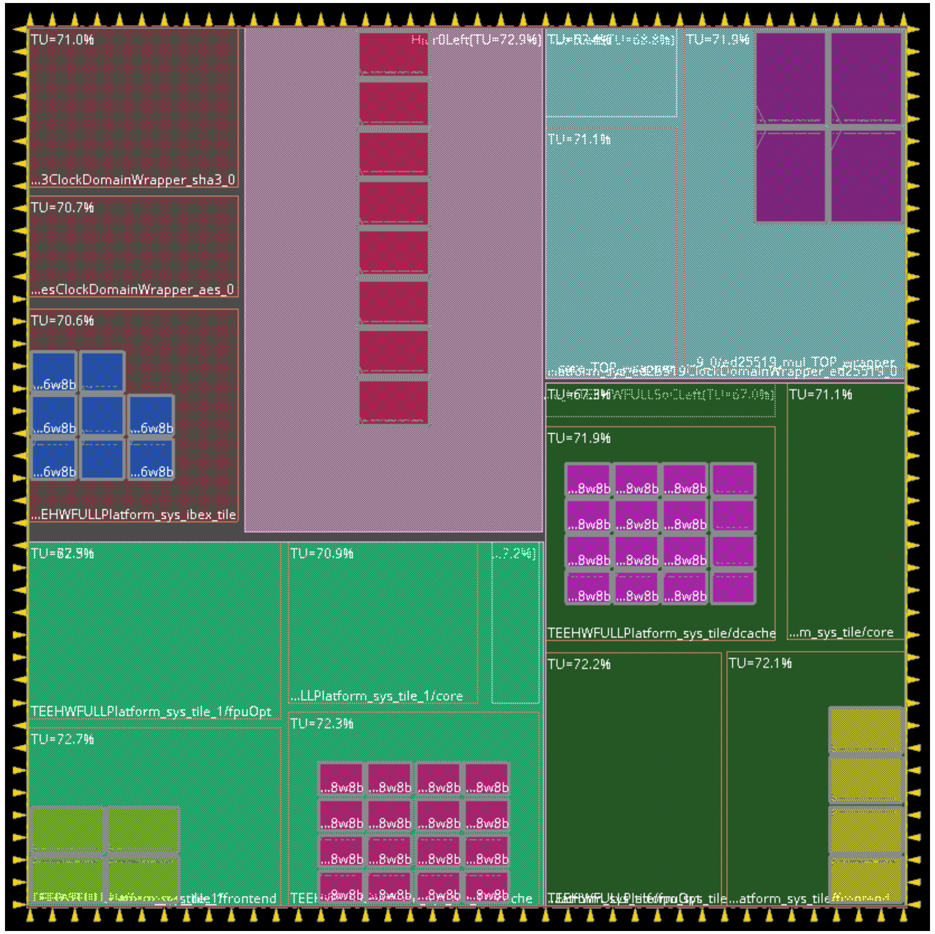
[1]National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
[2]University of Electro-Communications (UEC), Tokyo, Japan
[3]Tech. Research Asso. of Secure IoT Edge App. based on RISC-V Open Arch. (TRASIO), Tokyo, Japan

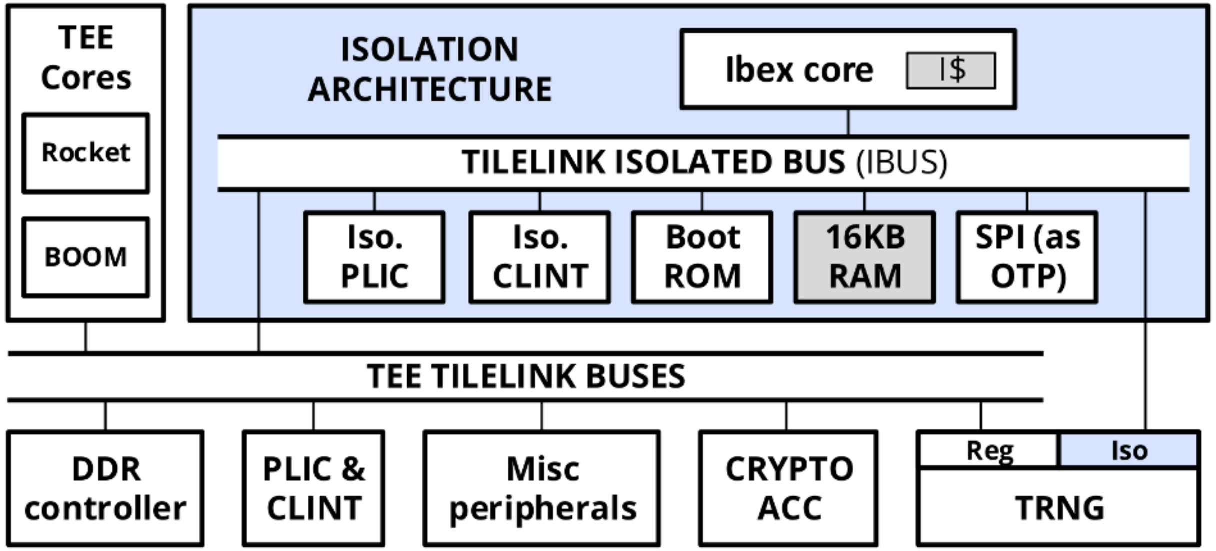
Presenter: Trong-Thuc Hoang

2021/7/21

Introduction (1/1)

This poster presents a Trusted Execution Environment (TEE) hardware implementation based on a heterogeneous architecture. The TEE verifies the integrity of software applications based on a chain of trust with the initial authentication. The chain-of-trust is implemented in software, using TEE hardware crypto-processors. The initial authentication is called the Root-of-Trust (RoT), and the isolated 32-bit system handles it. On the peripheral bus, there are several cryptography accelerators implemented such as SHA-3, ED25519, AES, and a True Random Number Generator (TRNG). The TRNG module has not only the public channel over the peripheral bus but also a special private channel just for the isolated core. The proposed system was implemented in a 5mm x 5mm die by the 180-nm ROHM process library.




TEE Cores

Rocket

BOOM

ISOLATION ARCHITECTURE

Ibex core

I$

TILELINK ISOLATED BUS (IBUS)

Iso. PLIC

Iso. CLINT

Boot ROM

16KB RAM

SPI (as OTP)

TEE TILELINK BUSES

DDR controller

PLIC & CLINT

Misc peripherals

CRYPTO ACC

Reg

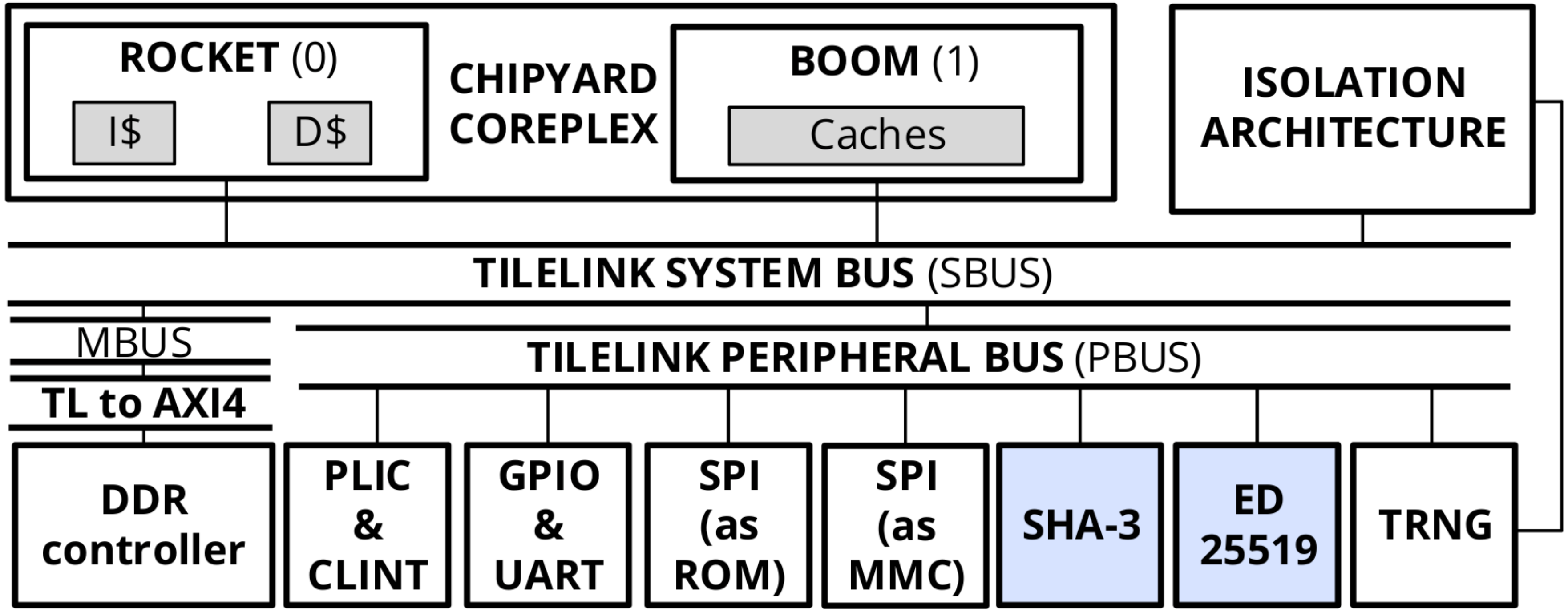
Iso

TRNG

OUTLINE

- TEE Hardware System
- VLSI Implementation
- Conclusion

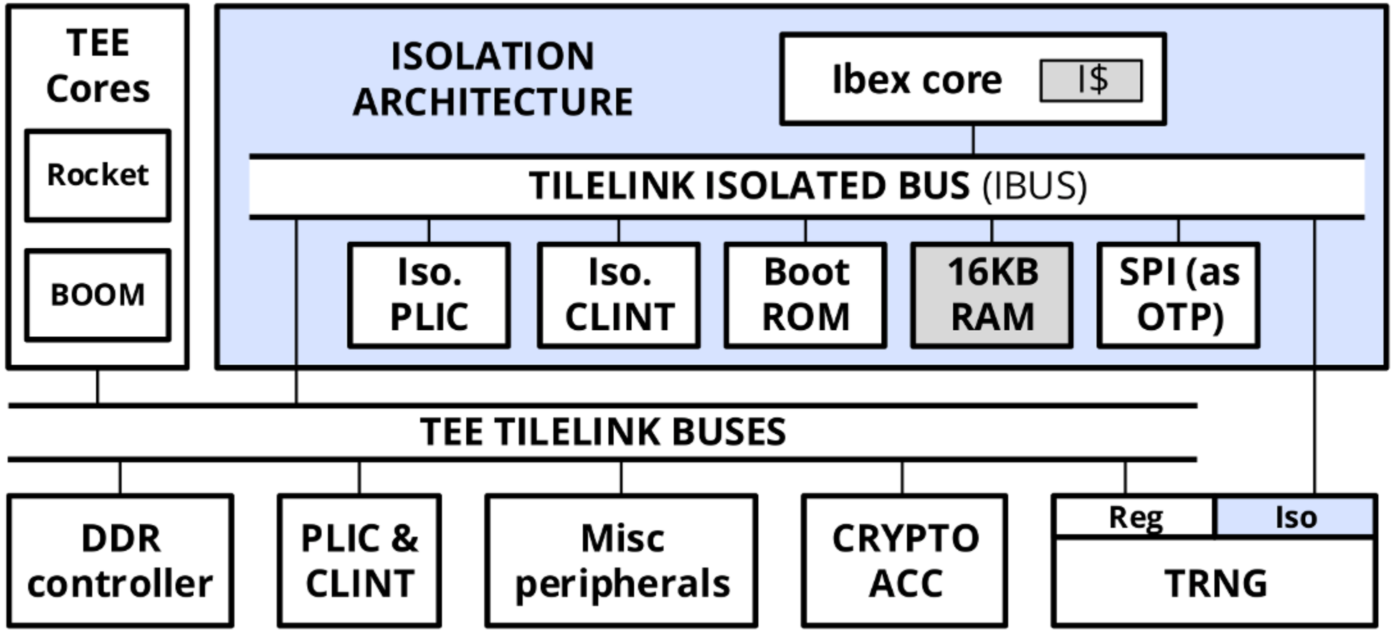
TEE Hardware System (1/4)



The TEE hardware system

- Support Linux-capable cores: Rocket-chip and BOOM *(core configurations are flexible)*.
- Convert memory-bus (MBUS) to AXI4: able to utilize the out-side DDR IP.
- The crypto-cores are on the peripheral bus (PBUS): can be shared for both Chipyard coreplex and isolated architecture.

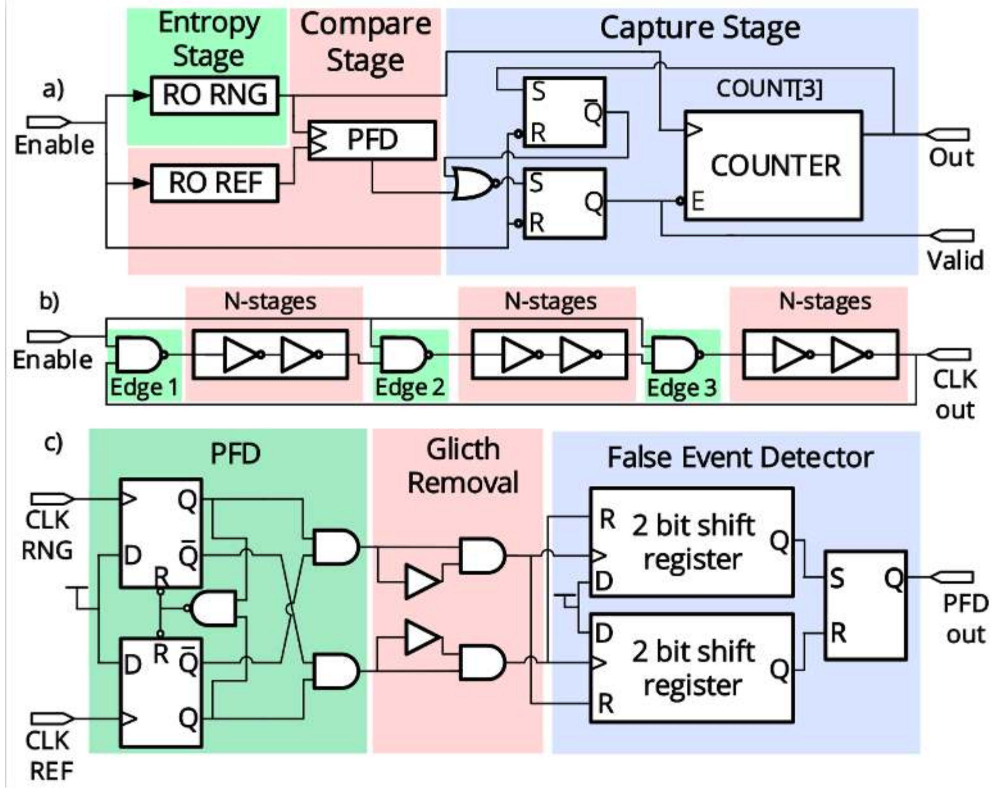
TEE Hardware System (2/4)



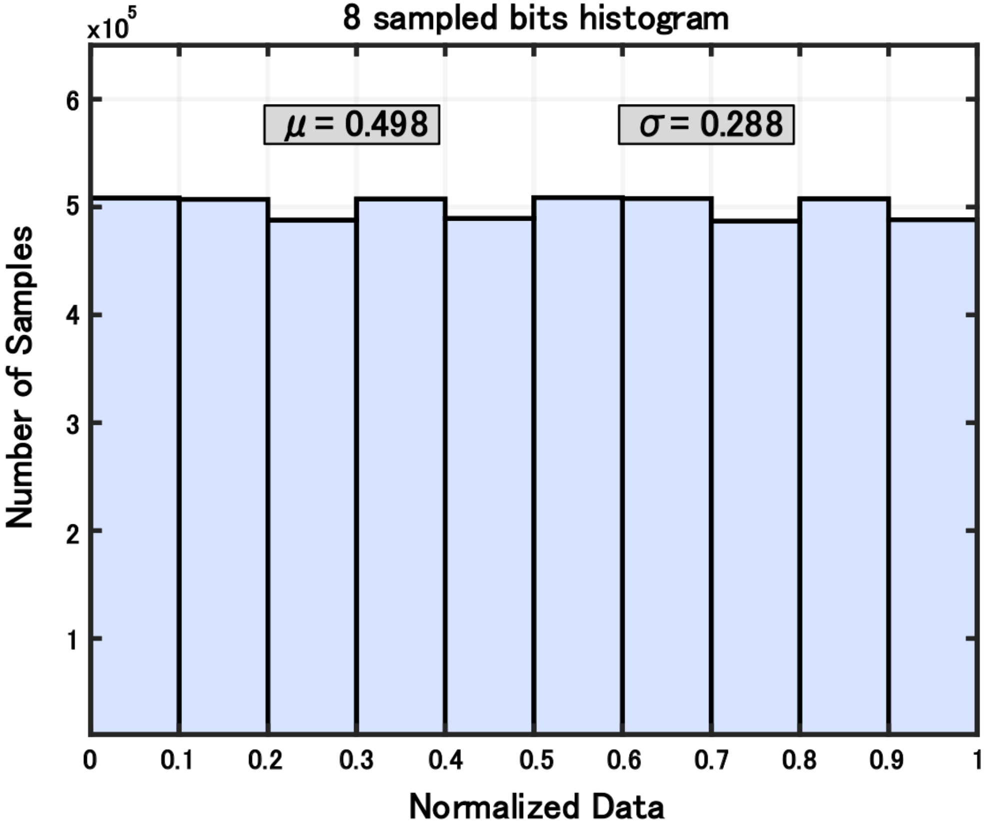
The isolation architecture

- Utilize the 32-bit Ibex-core from the opentitan.
- Isolated from the out-side TEE architecture.
- Has a secure One-Time-Programable (OTP) memory to hold the root-key.
- Has a special private channel to the True Random Number Generator (TRNG) module.
- Use the root-key *(in the OTP memory)* together with the TRNG to create a pair-key *(will enact as the Root-of-Trust for the later verification step in TEE).*

TEE Hardware System (3/4)



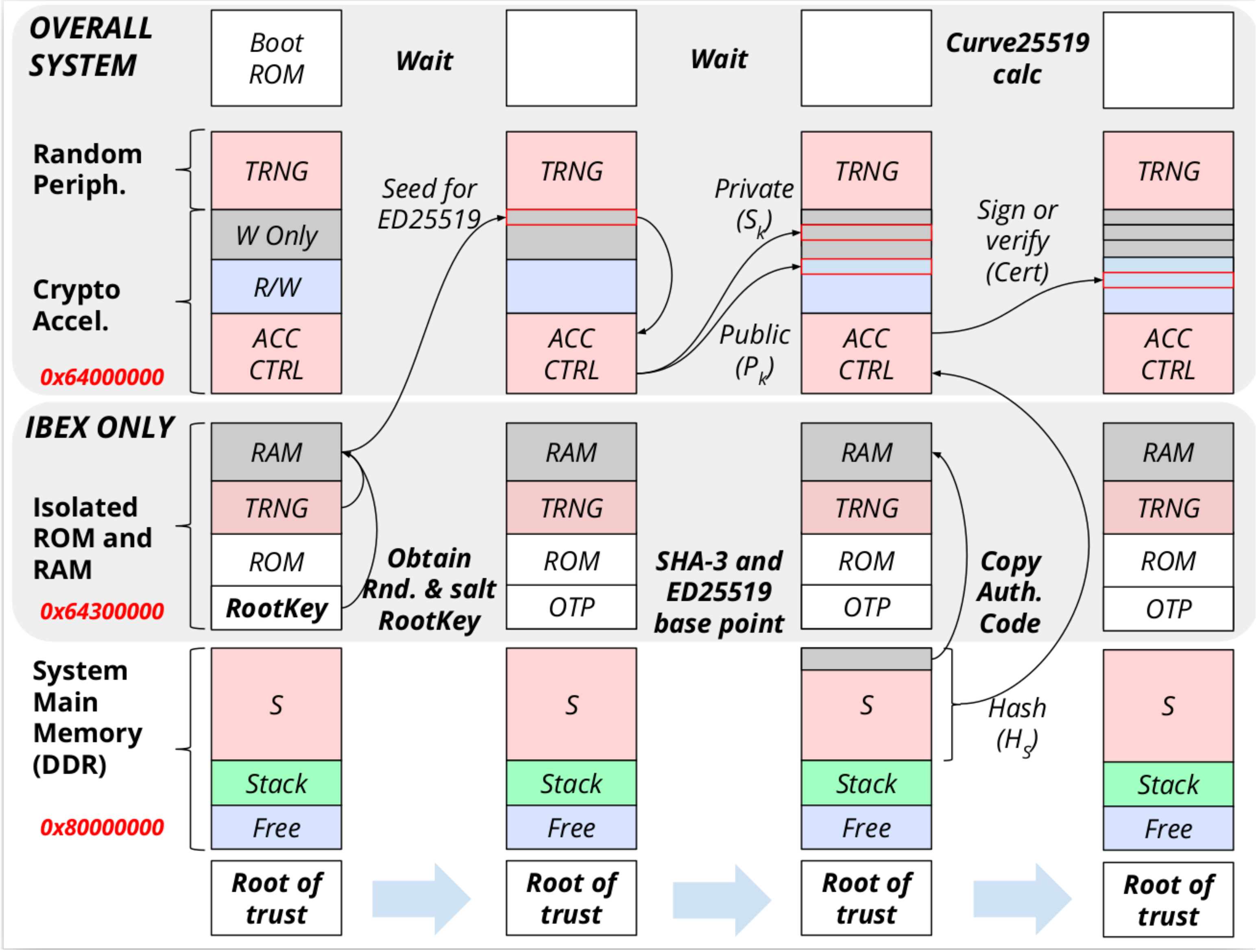
The TRNG architecture



The data distribution

- Use jitter accumulation (frequency collapse) in ring oscillators as the entropy source.
- The architecture is independent of the system clock.
- Pass all the NIST tests using a 5-MB dataset.

TEE Hardware System (4/4)



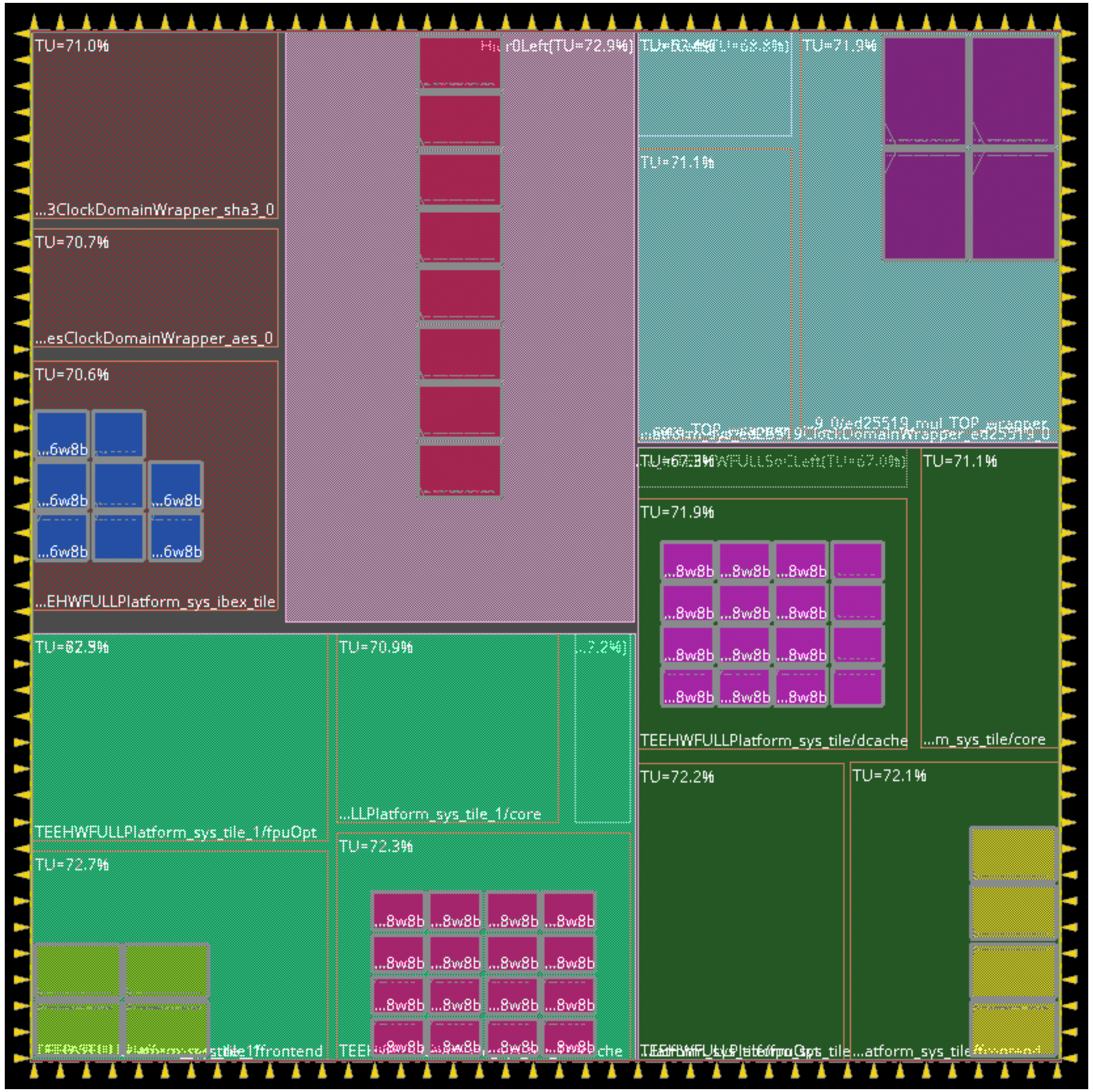
Boot sequence of the system

1. Ibex fetches root-key from OTP, salts it with TRNG → pass to the ED25519.
2. ED25519 receives the seed → create crypto pair-key.
3. The secret key is stored in the write-only memory.
4. The applications *(in DDR)* are hashed by the SHA-3 → then signed internally by the ED25519.
5. The certificates are created → will be verified later after-boot.

OUTLINE

- TEE Hardware System
- VLSI Implementation
- Conclusion

VLSI Implementation (1/5)

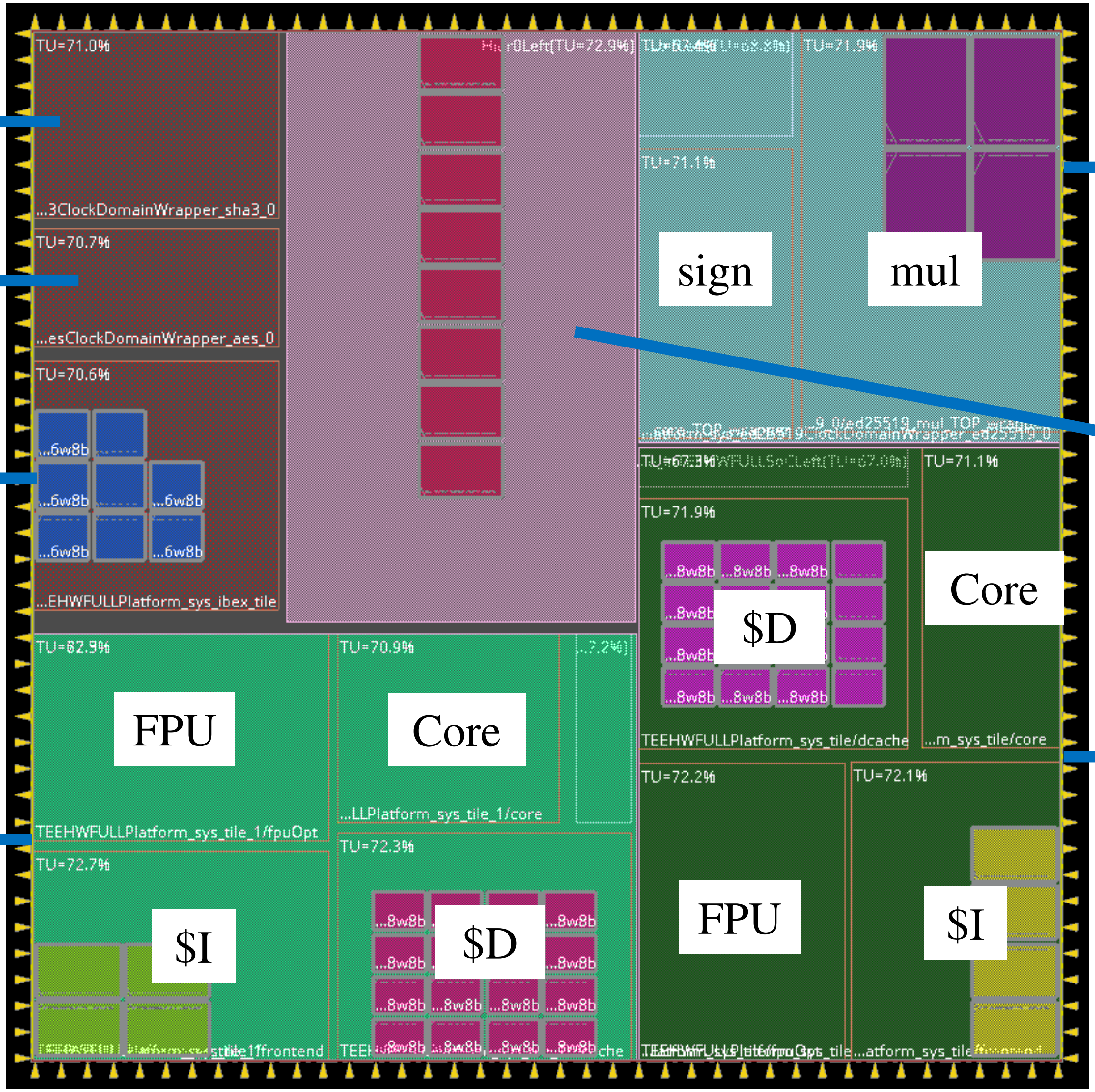


The floorplanning view

VLSI implementation configuration

- Process: ROHM-180nm; die size: 5-mm × 5-mm
- Dual Rocket-chip cores with:
  - ❑ ISA: RV64GC
  - ❑ I-cache: 2-KB; D-cache: 2-KB
- Single Ibex core with:
  - ❑ ISA: RV32IMC
  - ❑ I-cache: none; D-cache: 2-KB
- L2-cache: 4-KB
- Crypto-cores: SHA-3, AES, ED25519-multiplication, ED25519-sign, and TRNG
- Core area: 1.5-million NAND2-gate, 14.5-mm^2 (about 4-mm × 4-mm)
- Power *(at 100MHz)*: 63-μW of static + 348.9-mW of dynamic = 348.96-mW in total
- F_{Max}: 50-MHz

VLSI Implementation (2/5)



SHA-3

AES

Ibex-core

2nd Rocket-chip core

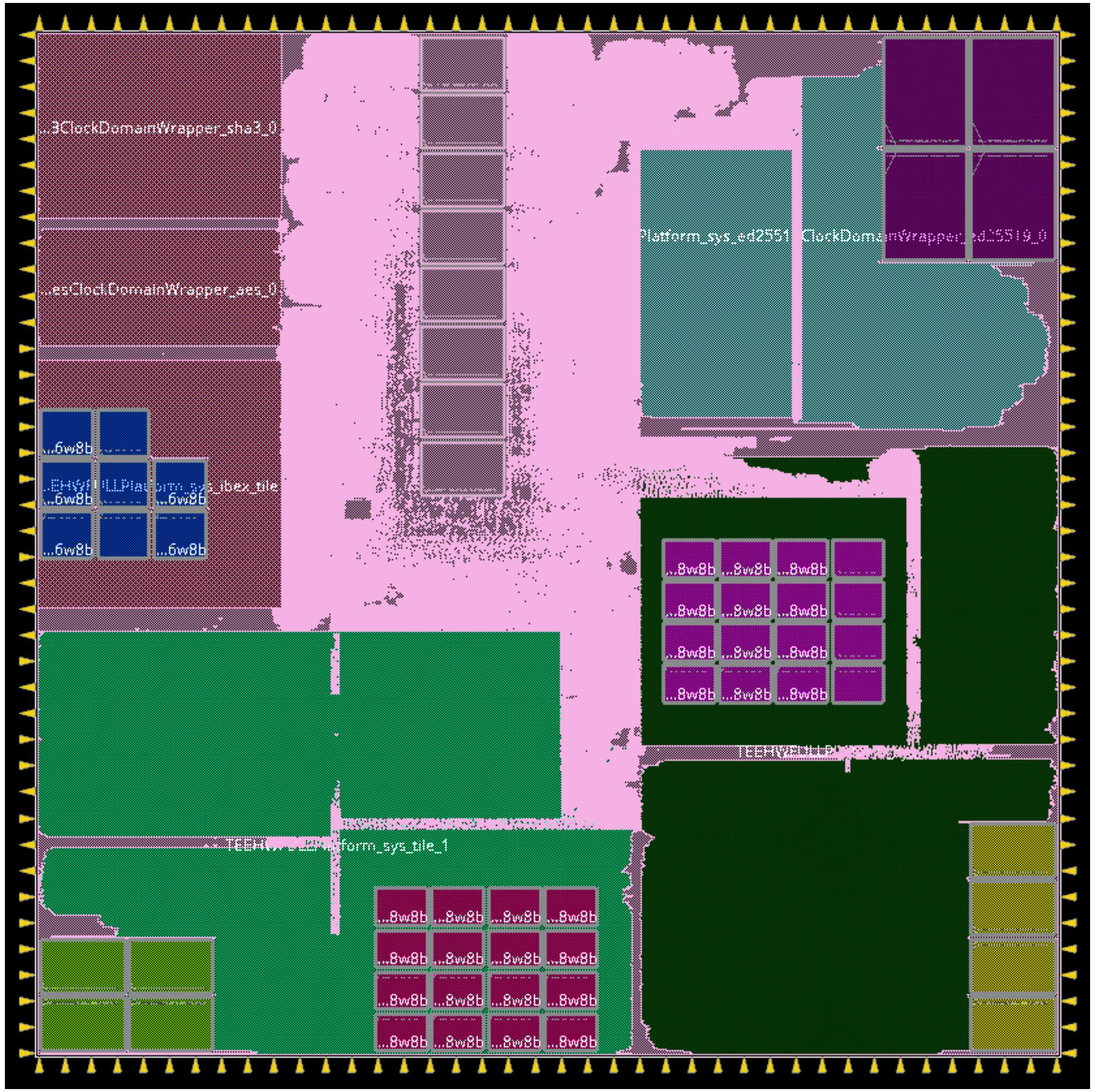
ED25519

The rest: buses, L2-cache, TRNG, boot ROM, GPIOs, etc.

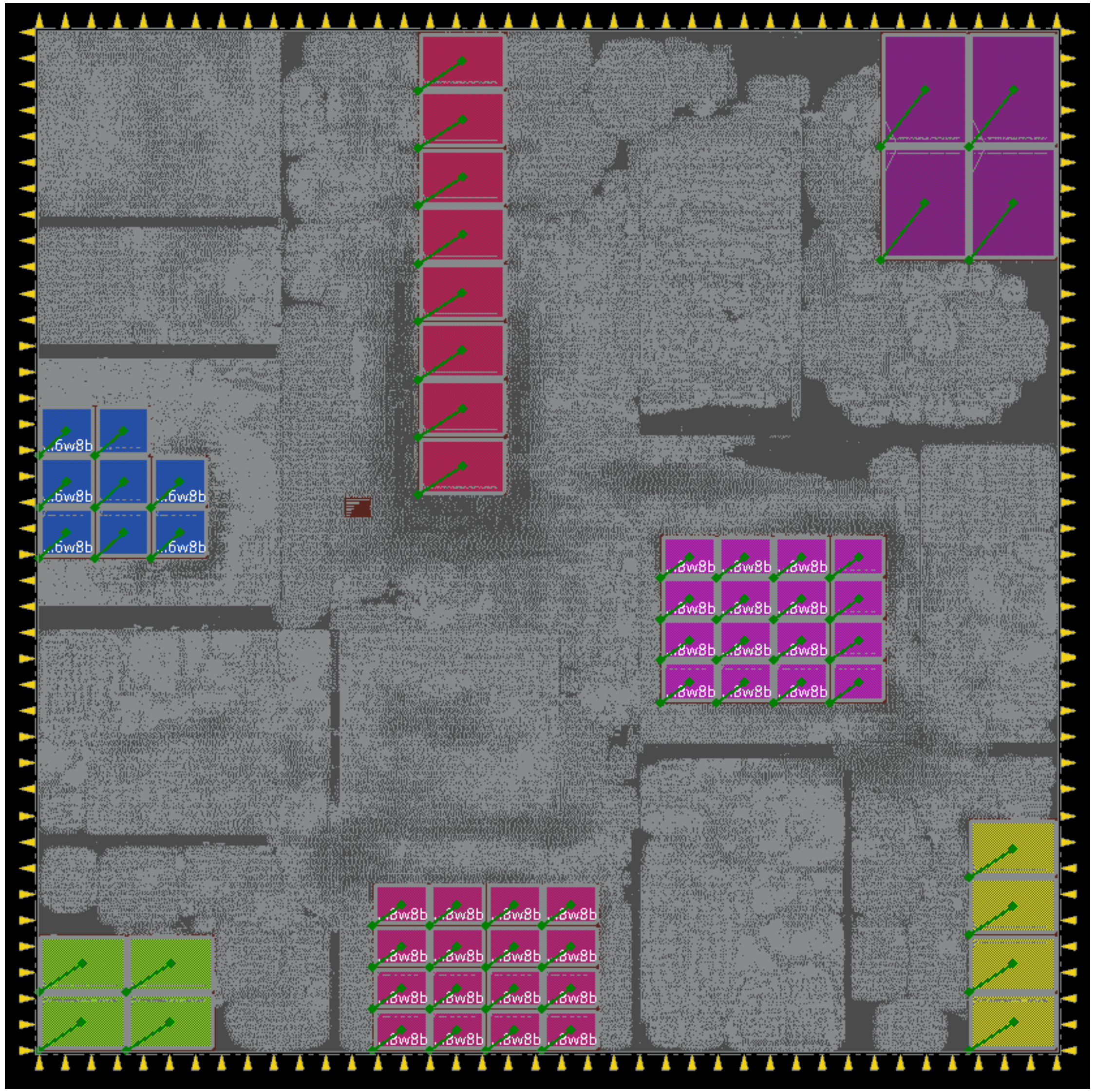
1st Rocket-chip core

The floorplanning view

VLSI Implementation (3/5)

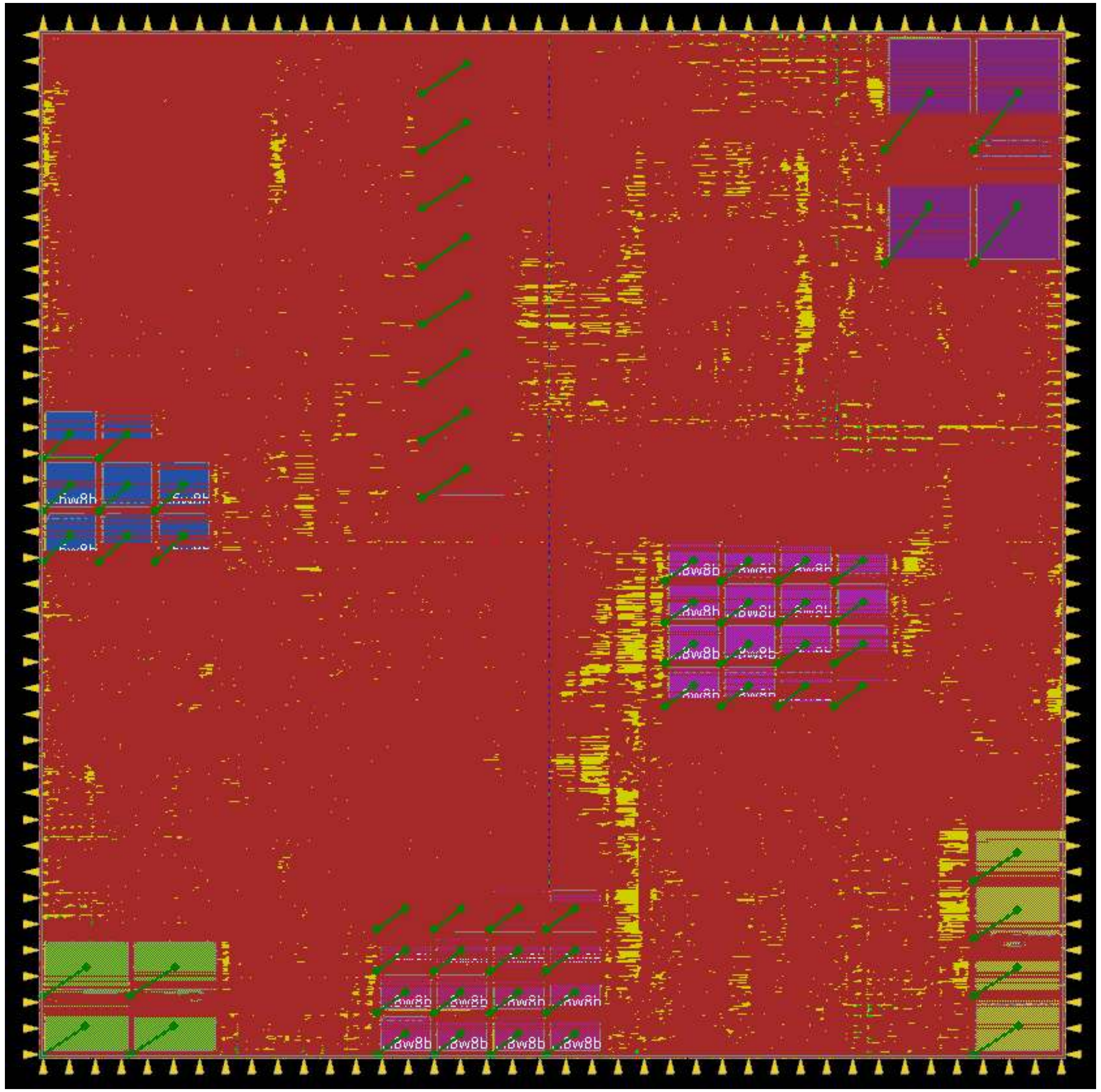

...3ClockDomainWrapper_sha3_0
...esClockDomainWrapper_aes_0
Platform_sys_ed2551
ClockDomainWrapper_ed25519_0
...6w8b
...Platform_sys_ibex_tile
...8w8b
TEEHW
TEEHW...form_sys_tile_1

The amoeba view

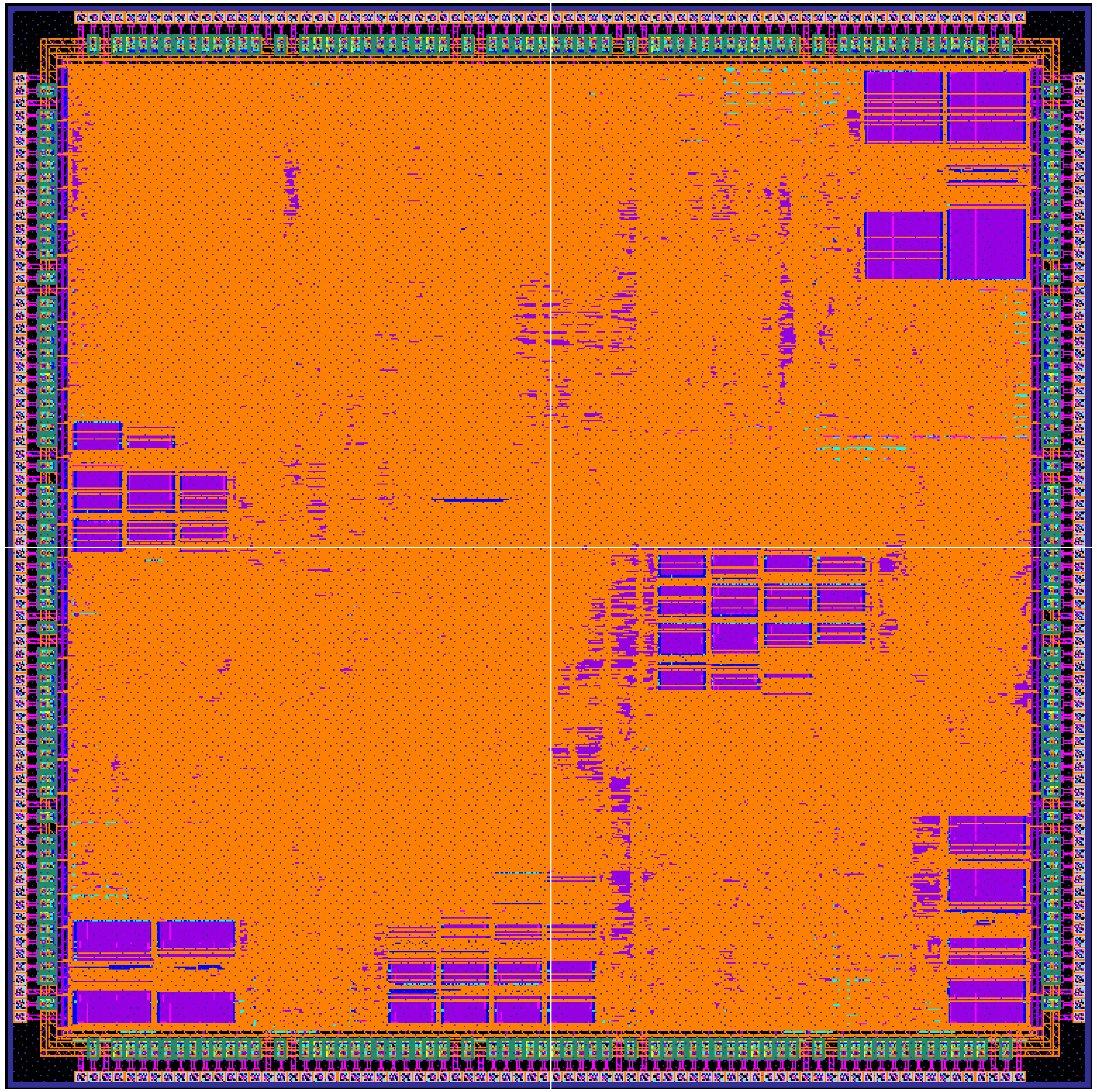


The place-only view

VLSI Implementation (4/5)



The place-and-route view



Layout view with I/O frame

VLSI Implementation (5/5)

VLSI results on the 180-nm ROHM process library.

	Cell-count	Cell-area		Power *(at 100MHz)*			
	(NAND2)	μm^2	%	Leakage (nW)	Dynamic (mW)	Total (mW)	%
Total system	1,498,530	14,500,979	100.00	63,010	348.90	348.96	100.00
Rocket	364,421	3,526,432	24.32	15,290	73.85	73.87	23.48
core	63,261	611,303	4.22	313	18.20	18.20	2.08
dcache	101,039	978,761	6.75	8,540	10.54	10.55	8.38
icache	93,374	904,606	6.24	5,954	11.26	11.27	9.20
fpu	92,038	886,711	6.11	404	29.47	29.47	3.26
Ibex	102,272	989,671	6.82	5,793	14.70	14.71	3.16
core	50,826	491,833	3.39	215	11.78	11.78	1.34
ED25519	242,302	2,344,712	16.17	13,500	43.50	43.51	18.16
sign	64,754	626,618	4.32	332	12.06	12.06	1.88
mul	154,855	1,498,508	10.33	13,040	27.01	27.02	15.49
SHA3	69,574	673,254	4.64	322	73.02	73.02	5.49
AES	42,235	408,700	2.82	216	10.77	10.77	1.35
BootROM	1,912	18,502	0.13	12	20.47	20.47	1.17
TRNG	2,333	22,576	0.16	13	4.09	4.09	0.22

OUTLINE

- TEE Hardware System
- VLSI Implementation
- Conclusion

Conclusion (1/1)

- A TEE hardware system with heterogeneous design is presented.
- Isolated scheme with 64-bit Linux-capable cores on the public domain and a 32-bit core on the private domain.
- Isolated Ibex-core holds the Root-of-Trust (RoT) and manage the root-key; Rocket/BOOM-cores control the later boot sequence and the TEE.
- Crypto-cores available: SHA-3, AES, ED25519-multiplication, ED25519-sign, and TRNG.
- The developed TRNG module passed all the NIST tests. In the system, it has a special private channel just for the isolated core.
- The VLSI implementation is done by the ROHM-180nm process on the 5-mm×5-mm die.

THANK YOU

2021/7/21

Acknowledgement
This work is based on results obtained from project JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO). This work was also supported through the activities of VDEC, The University of Tokyo, in collaboration with Cadence Design Systems and Mentor Graphics.