COMPASS Lab
COMPuter And System Security Lab

SoK: A Comparison Study of Arm TrustZone and CCA

Haoyang Huang[1], Fengwei Zhang[1],
Shoumeng Yan[2], Tao Wei[2], Zhengyu He[2].

1 南方科技大学 SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

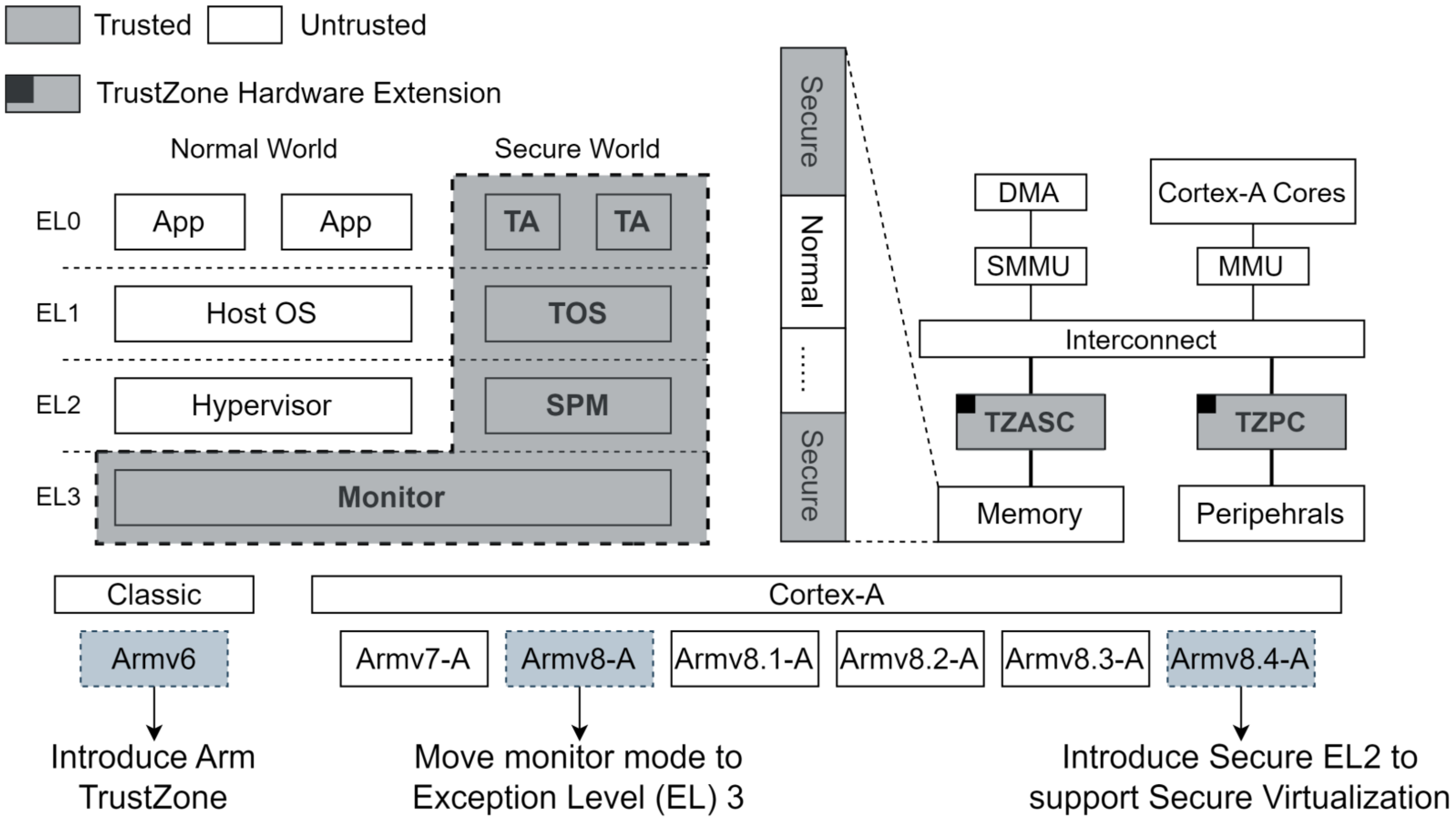
2 蚂蚁集团 ANT GROUP

Outline

- **Introduction to Arm TrustZone and CCA**
- Comparison in Flexibility
- Comparison in Security
- Conclusion

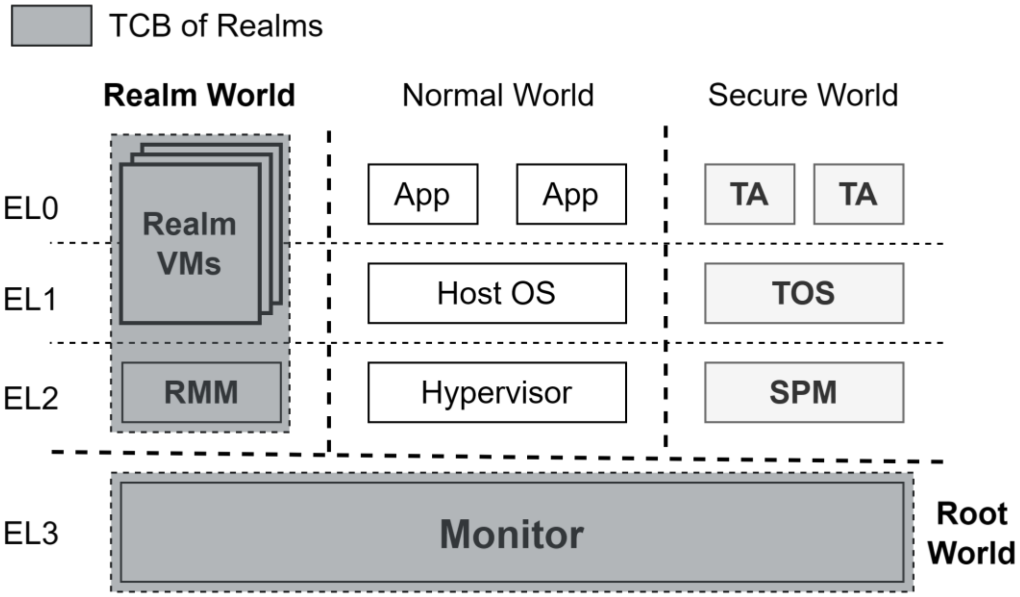
1 TrustZone Overview

- TrustZone was first introduced in ARMv6 and provides a hardware-based isolated execution environment.
- TrustZone divides the whole system into two parts: **Normal World** and **Secure World**.
- TrustZone ensures isolation between two words through hardware extensions (e.g. **TZASC** and **TZPC**).



1 Confidential Compute Architecture (CCA) Overview

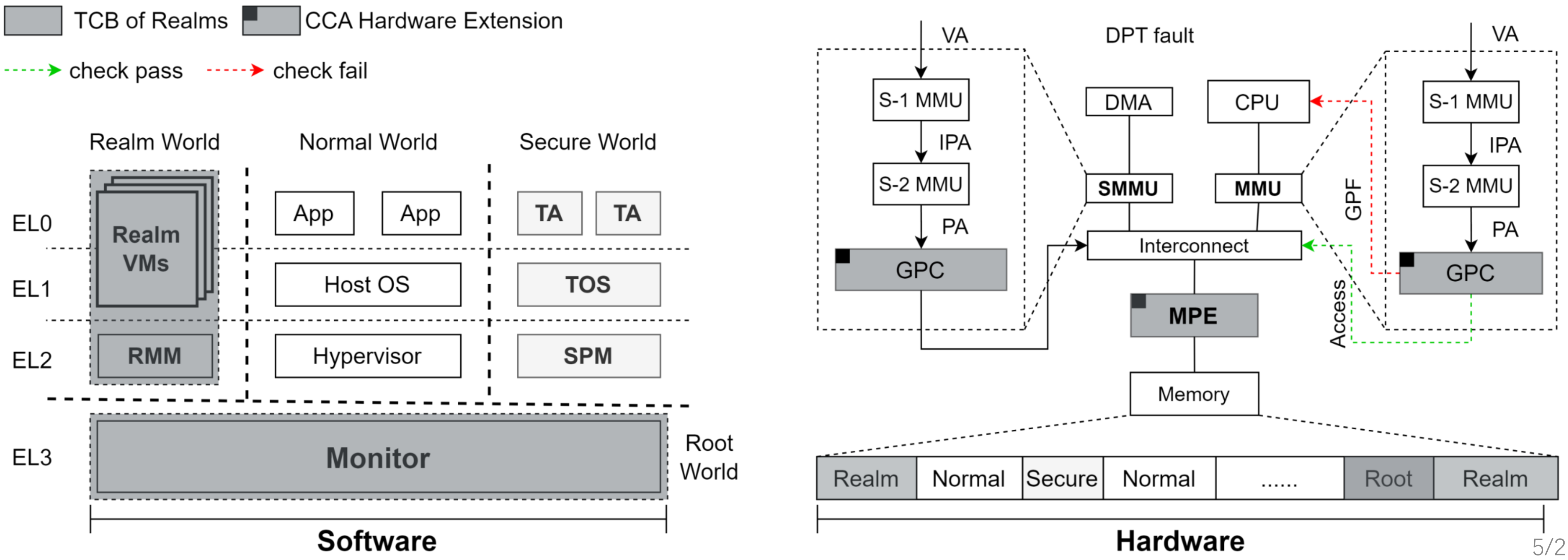
- CCA was announced in 2021 and introduced as supplement to Armv9.2-A
- CCA introduces a series of New isolation boundaries:
  - **Root World:** Used for code and data in EL3
  - **Realm World :** Used for third party confidential computing



	Normal World	Secure World	Realm World	Root World
Non-Secure	Allow	Block	Block	Block
Secure	Allow	Allow	Block	Block
Realm	Allow	Block	Allow	Block
Root	Allow	Allow	Allow	Allow

1 Confidential Compute Architecture (CCA) Overview

- Besides two additional worlds, CCA also introduces a set of new hardware features:
  - Dynamic assignment of memory to different worlds **(Granule Protection Check, GPC)**
  - Memory Encryption **(Memory Protection Engine, MPE)**
  - ……

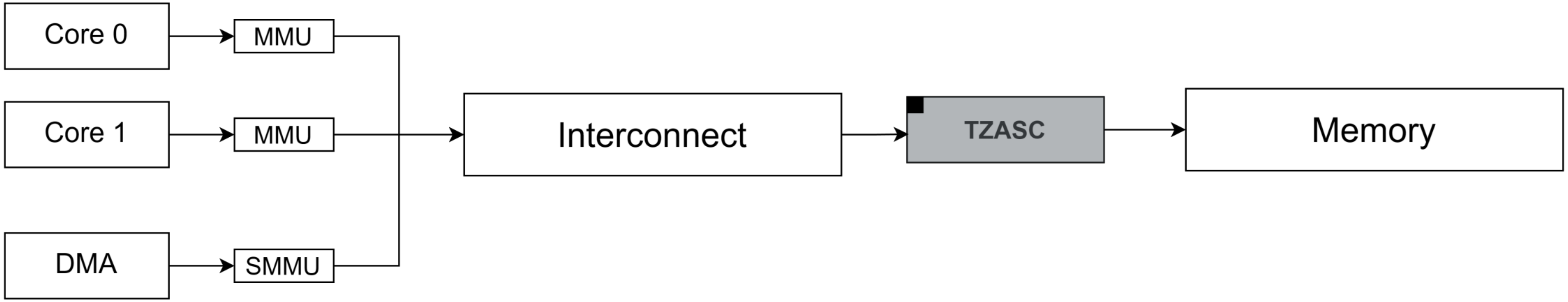


Outline

- Introduction to Arm TrustZone and CCA
- **Comparison in Flexibility**
- Comparison in Security
- Conclusion

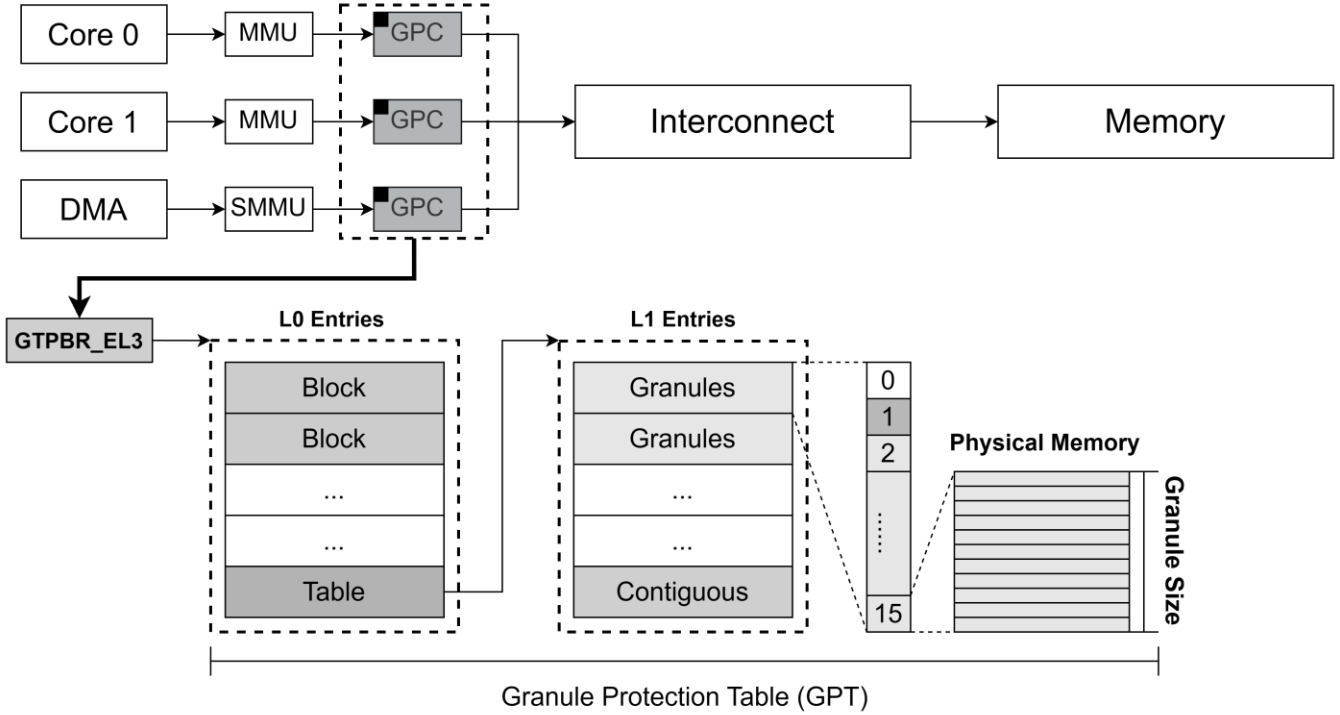
2 Flexibility Comparison: Memory Management

- Memory management represents the system's ability to **adjust permission settings of memory regions** to meet specific requirements.
- TrustZone achieves memory partition using **TZASC**:
  - TZASC determine the **range** of each memory region and their corresponding worlds through specific registers.
  - TZASC allows to configure the **read and write permissions** for each memory region.



2 Flexibility Comparison: Memory Management

- Memory management represents the system's ability to **adjust permission settings of memory regions** to meet specific requirements.
- CCA achieves memory partition using **GPC**:
  - GPC is a hardware extension in **MMU** and relies on **Granule Protection Table (GPT)** to identify the associated world of each memory granule.

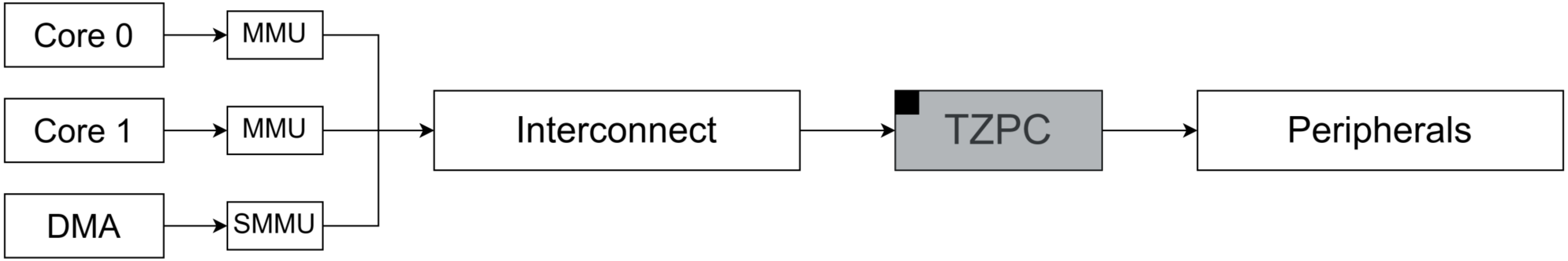


2 Flexibility Comparison: Memory Management

- Regarding Memory Management, TZASC and GPC are different in following fields:
  - **Minimal Granularity of Memory Regions**:
    - TrustZone: 32KB
    - CCA: 4KB
  - **Memory Region Number**:
    - TrustZone: Limited
    - CCA: Unlimited
  - **Core-specific Configuration**:
    - TrustZone: All cores share the same memory partition policy.
    - CCA: Each core can be configured with different partition policy.
  - **R/W-separate Configuration**:
    - TrustZone: Supported
    - CCA: Unsupported

2 Flexibility Comparison: Peripheral Management

- Peripheral management represents the system's ability to **adjust permission settings of peripherals** to meet specific requirements.
- TrustZone achieves peripheral management using **TZPC**:
    - TZPC allows to configure the security state dynamically for each peripheral.
- CCA achieves peripheral management using **GPC**:
    - In Arm architecture, access to peripherals is achieved through Memory Mapped I/O (MMIO).
    - Therefore, GPC can be used to adjust access permissions of peripherals.



2

Flexibility Comparison: Peripheral Management

- Regarding Peripheral Management, TZPC and GPC are different in following fields:

  - **Minimal Granularity**:
    - TrustZone: The Whole Peripheral
    - CCA: 4KB
  - **Peripheral Number**:
    - TrustZone: Limited
    - CCA: Unlimited
  - **Core-specific Configuration**:
    - TrustZone: All cores share the same memory partition policy.
    - CCA: Each core can be configured with different partition policy.

Outline

- Introduction to Arm TrustZone and CCA
- Comparison in Flexibility
- **Comparison in Security**
- Conclusion

3 Security Comparison: Memory and Peripheral Isolation

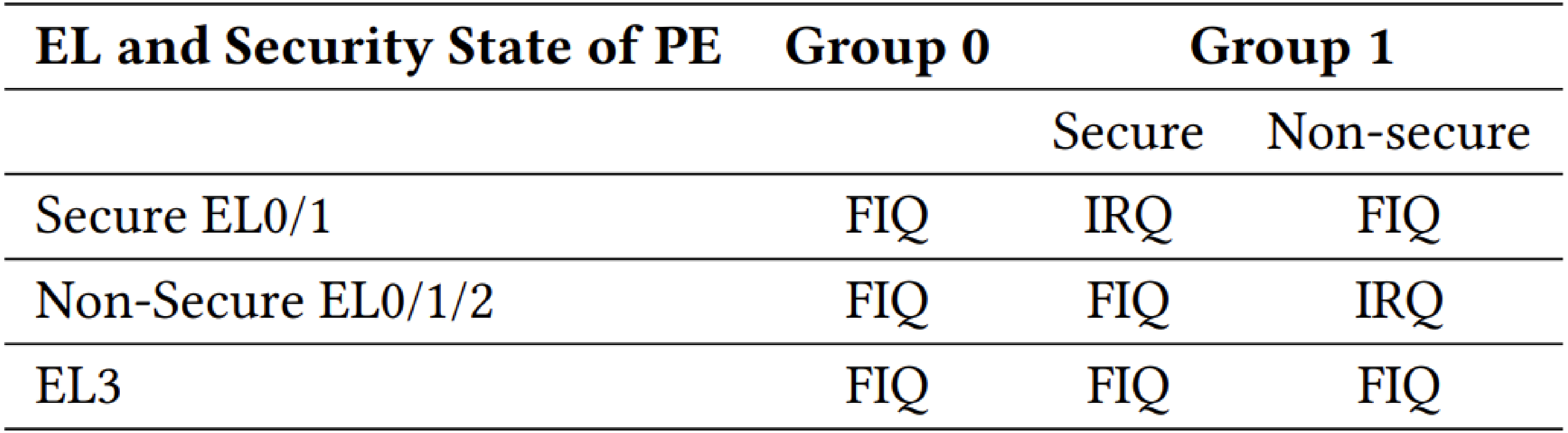
- Both TrustZone and CCA can prevent the processor and DMA devices from illegally accessing memory and peripherals. However, they are different in following fields:

- **Level to Configure:**
  - **TrustZone: TZASC** and **TZPC** can be configured by the software in **S-EL1/2**.
  - **CCA: GPC** can only be configured by the code running in **EL3**.
- **Isolation for Monitor in EL3:**
  - TrustZone: The code and data belonging to EL3 belong to **Secure World**.
  - CCA: The code and data belonging to EL3 belong to **Root World**.
- **Hardware-assisted Encryption:**
  - TrustZone: Not Support.
  - CCA: Support through **Memory Protection Engine (MPE)**.

3 Security Comparison: Interrupt Isolation

- An interrupt is a signal from hardware or software sent to the processor to indicate that an event has occurred.
- Malicious interrupts can interfere with the expected workflow of the processor.

- **Interrupt Isolation:**
  - **TrustZone:** It supports the isolation of secure interrupts and non-secure interrupts.
  - **CCA:** Interrupts for VMs are virtualized by the hypervisor in Normal World.

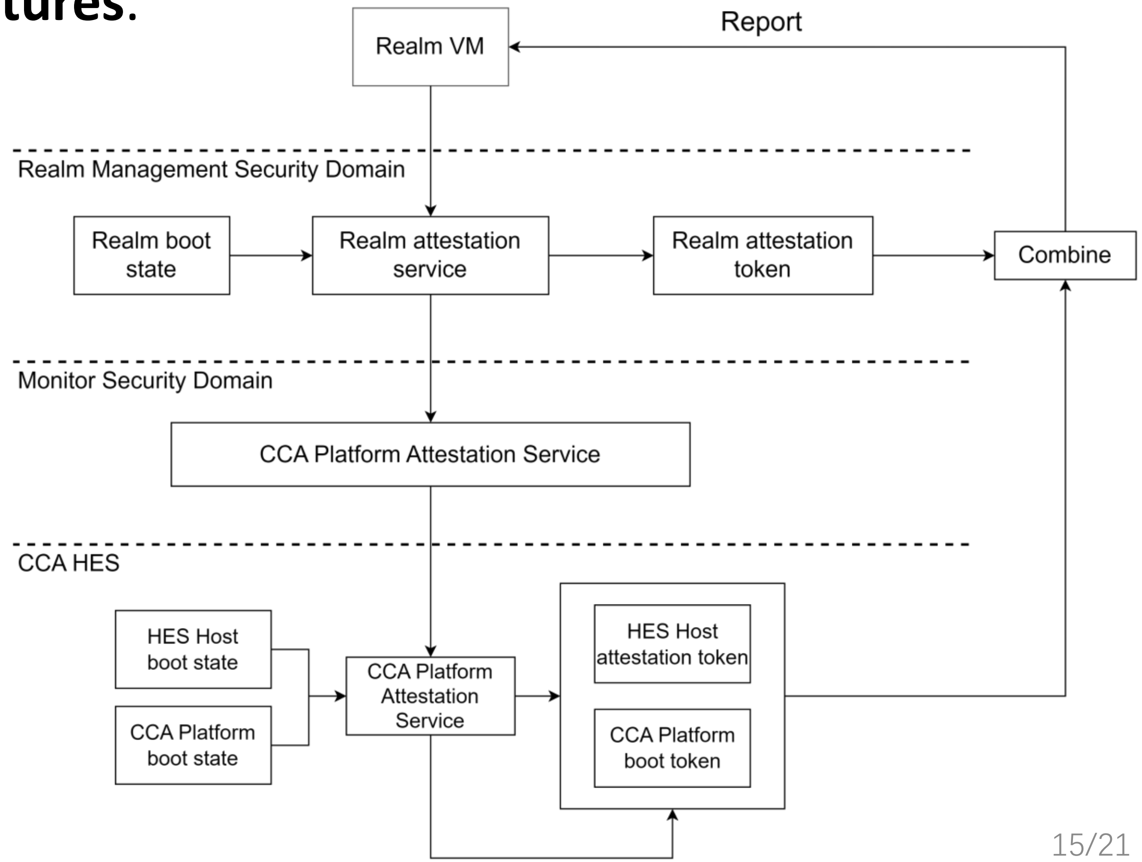


EL and Security State of PE	Group 0	Group 1	
		Secure	Non-secure
Secure EL0/1	FIQ	IRQ	FIQ
Non-Secure EL0/1/2	FIQ	FIQ	IRQ
EL3	FIQ	FIQ	FIQ

3 Security Comparison: Attestation

- The hardware-assisted attestation brings significant benefits to system security and integrity.
- It measures the system's state and provides assurance that the software running on the system has **not been tampered with or modified** since its initial trusted state.
- Moreover, hardware-assisted attestation can verify whether applications **run on a platform that genuinely supports the required security features**.

- **Hardware-assisted Attestation:**
  - **TrustZone:** Not Support
  - **CCA:** Support



3 Security Comparison: TLB and Cache

- When the processor tries to access the memory, it first checks whether the translation result and data are in TLB and cache.
- However, since the hardware extensions for memory isolation are behind the TLB and cache, they cannot intercept access to the TLB and cache.
- Therefore, there is a need for TEEs to provide additional hardware mechanisms to ensure the security of TLB and cache.

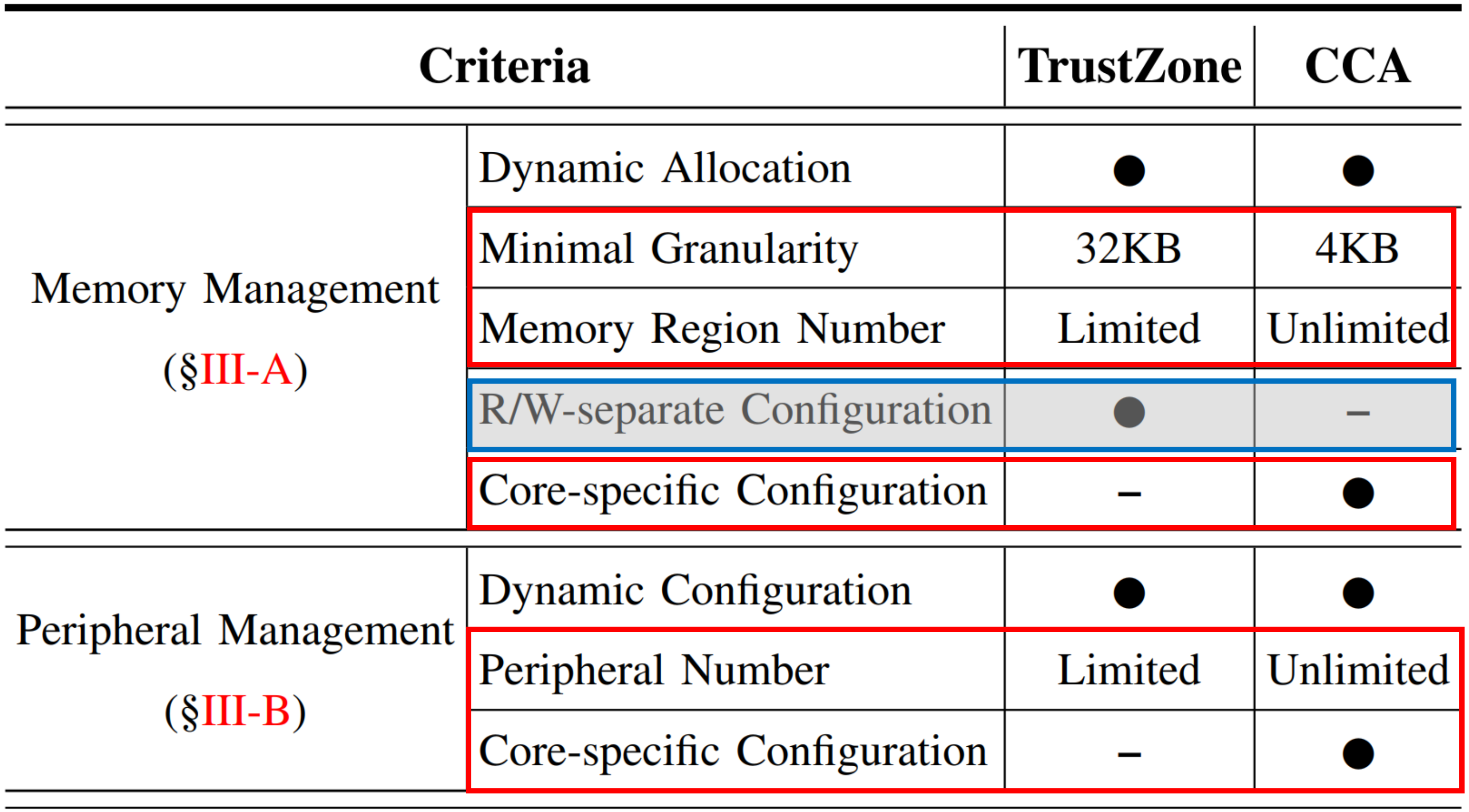
- **Isolation for TLB:**
  - **Both TrustZone and CCA** extends the TLB with additional bits in **entries** to support identifying their associated worlds.

- **Isolation for Cache:**
  - **Both TrustZone and CCA** extends the Cache with additional bits in **cache line** to support identifying their associated worlds.

Outline

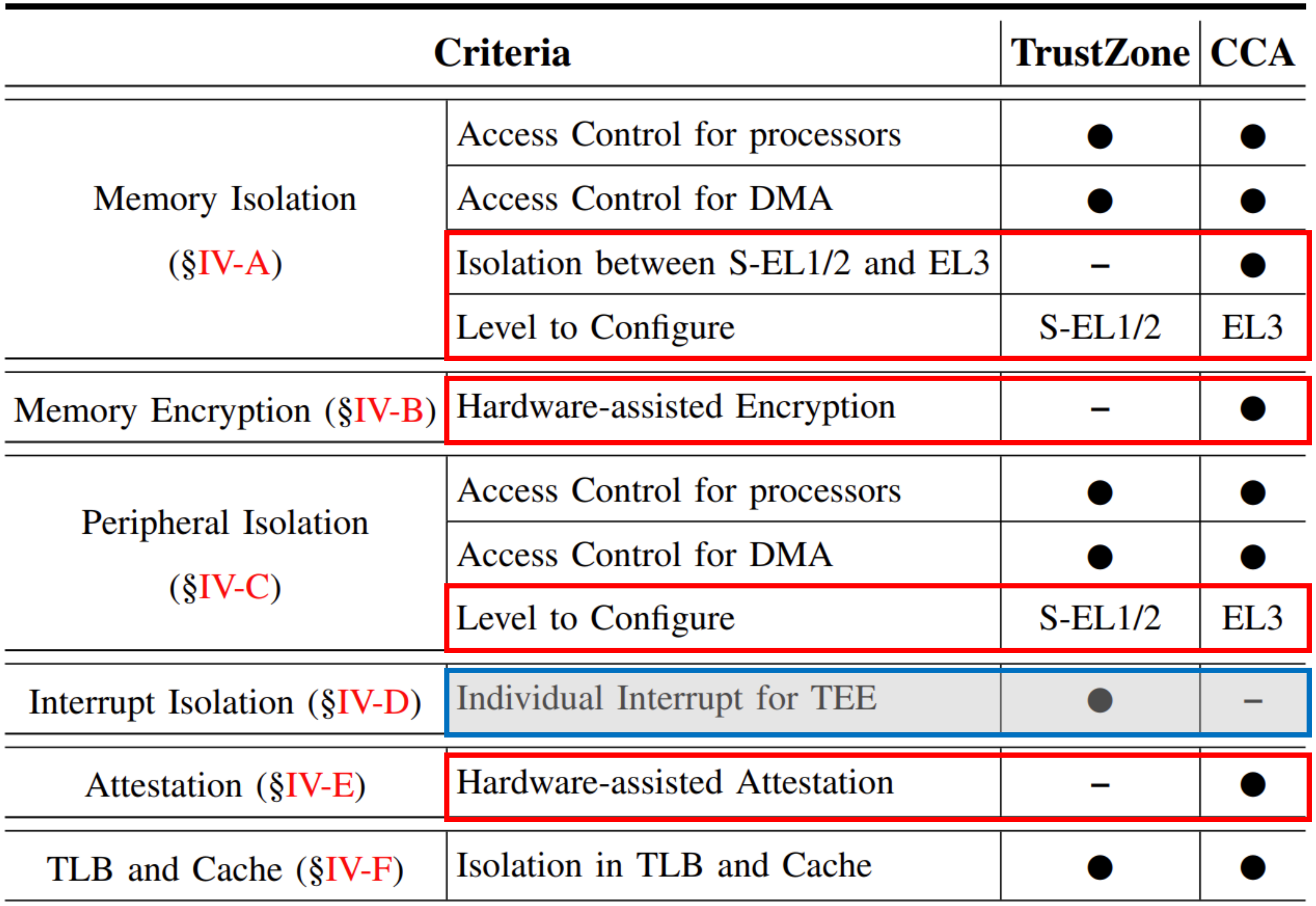
- Introduction to Arm TrustZone and CCA
- Comparison in Flexibility
- Comparison in Security
- **Conclusion**

4 Summary for Comparison in Flexibility



Criteria		TrustZone	CCA
Memory Management (§III-A)	Dynamic Allocation	●	●
	Minimal Granularity	32KB	4KB
	Memory Region Number	Limited	Unlimited
	R/W-separate Configuration	●	–
	Core-specific Configuration	–	●
Peripheral Management (§III-B)	Dynamic Configuration	●	●
	Peripheral Number	Limited	Unlimited
	Core-specific Configuration	–	●

4 Summary for Comparison in Security



Criteria		TrustZone	CCA
Memory Isolation (§IV-A)	Access Control for processors	●	●
	Access Control for DMA	●	●
	Isolation between S-EL1/2 and EL3	–	●
	Level to Configure	S-EL1/2	EL3
Memory Encryption (§IV-B)	Hardware-assisted Encryption	–	●
Peripheral Isolation (§IV-C)	Access Control for processors	●	●
	Access Control for DMA	●	●
	Level to Configure	S-EL1/2	EL3
Interrupt Isolation (§IV-D)	Individual Interrupt for TEE	●	–
Attestation (§IV-E)	Hardware-assisted Attestation	–	●
TLB and Cache (§IV-F)	Isolation in TLB and Cache	●	●

Thank You

https://compass.sustech.edu.cn/

南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COMPASS Lab
COMPuter And System Security Lab

蚂蚁集团
ANT GROUP