PORTAL

Fast and Secure Device Access with Arm CCA for Modern Arm Mobile System-on-Chips (SoCs)

Fan Sang[1], Jaehyuk Lee[1], Xiaokuan Zhang[2], Taesoo Kim[1]

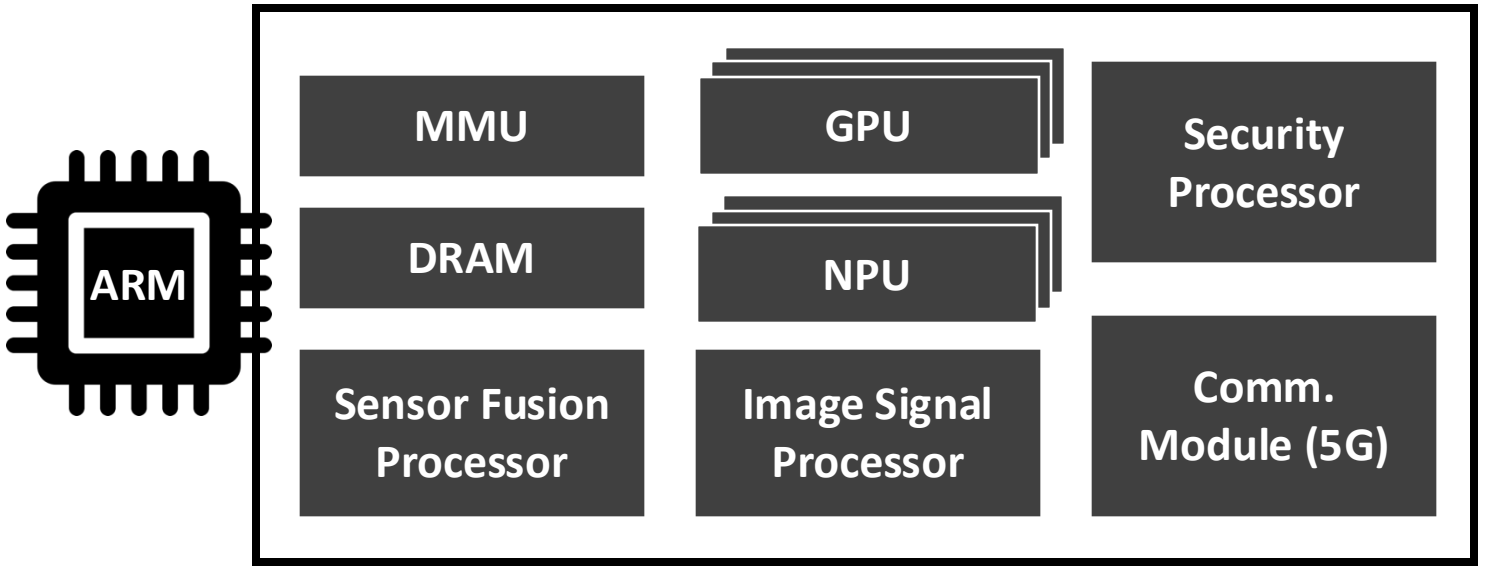
[1]Georgia Institute of Technology, [2]George Mason University

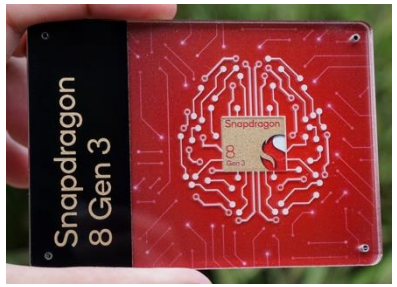
fsang@gatech.edu

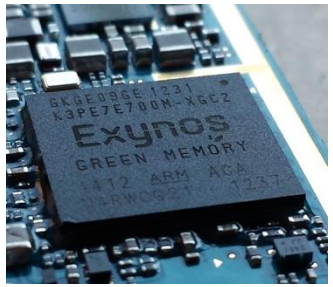
Georgia Tech College of Computing
School of Cybersecurity and Privacy

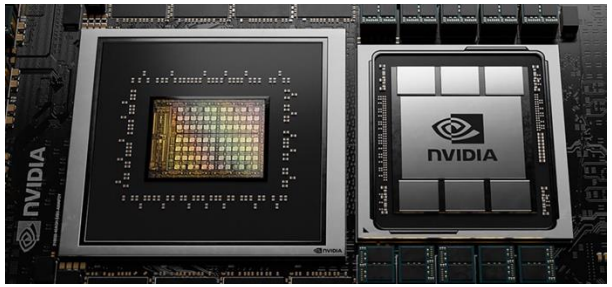
Arm – Architectural Trend in Mobile SoCs

An increasing integration of devices

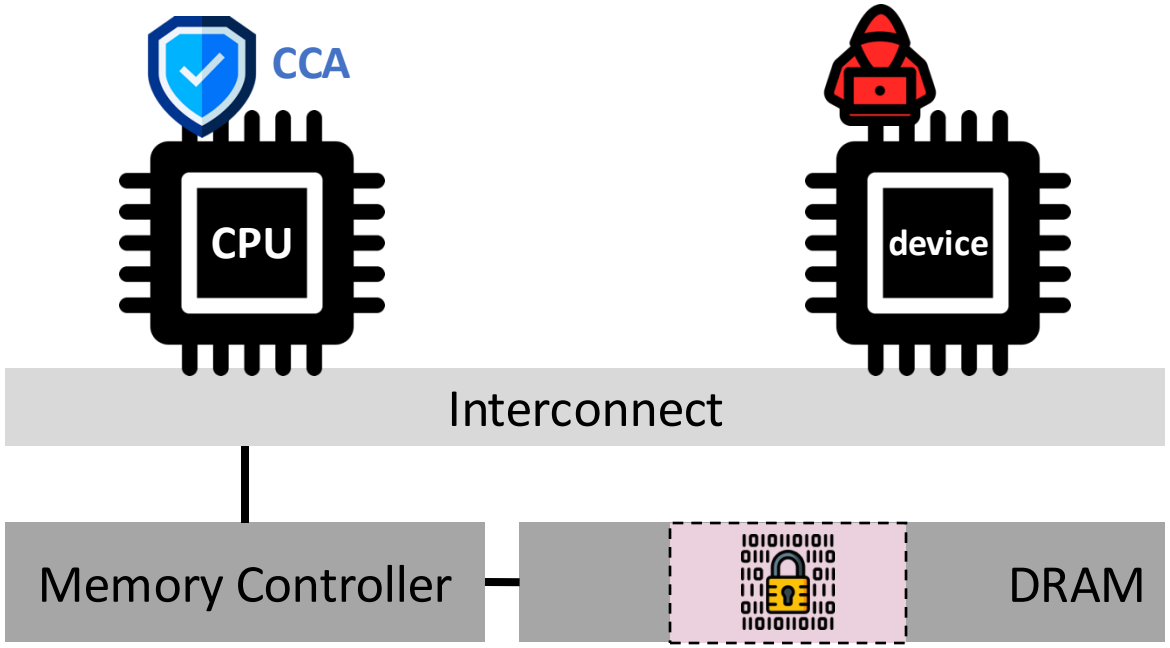




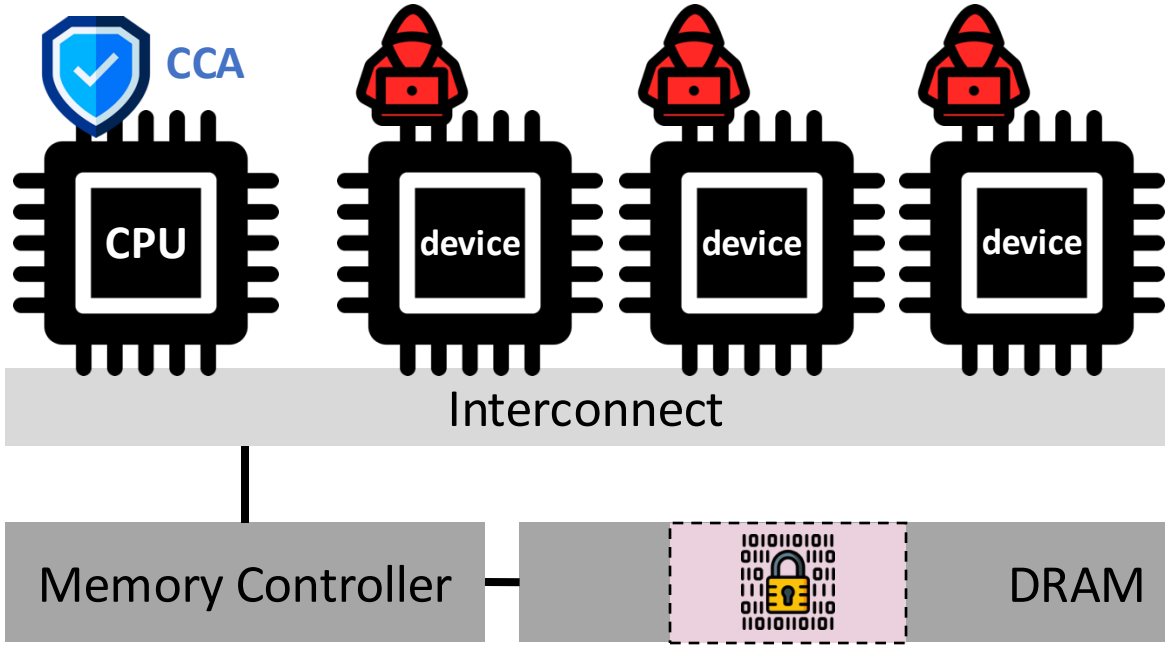




Device Access in CCA

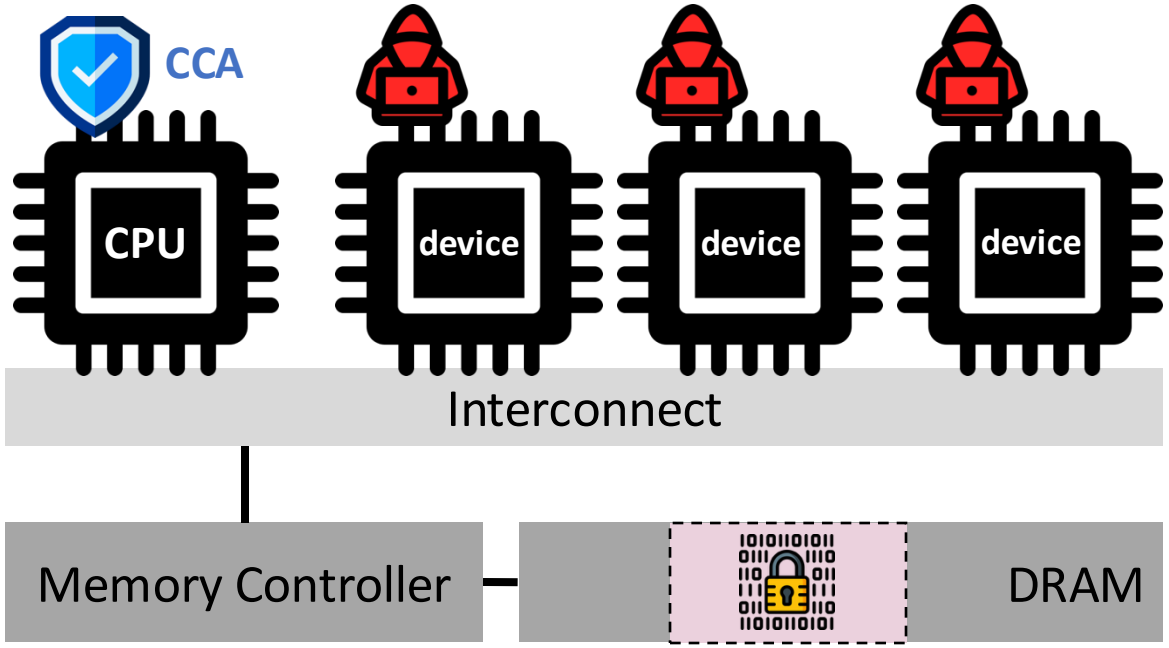


Device Access under the Architectural Trend



→ ***Arm CCA struggles to keep up with the architectural trend.***

Device Access under the Architectural Trend



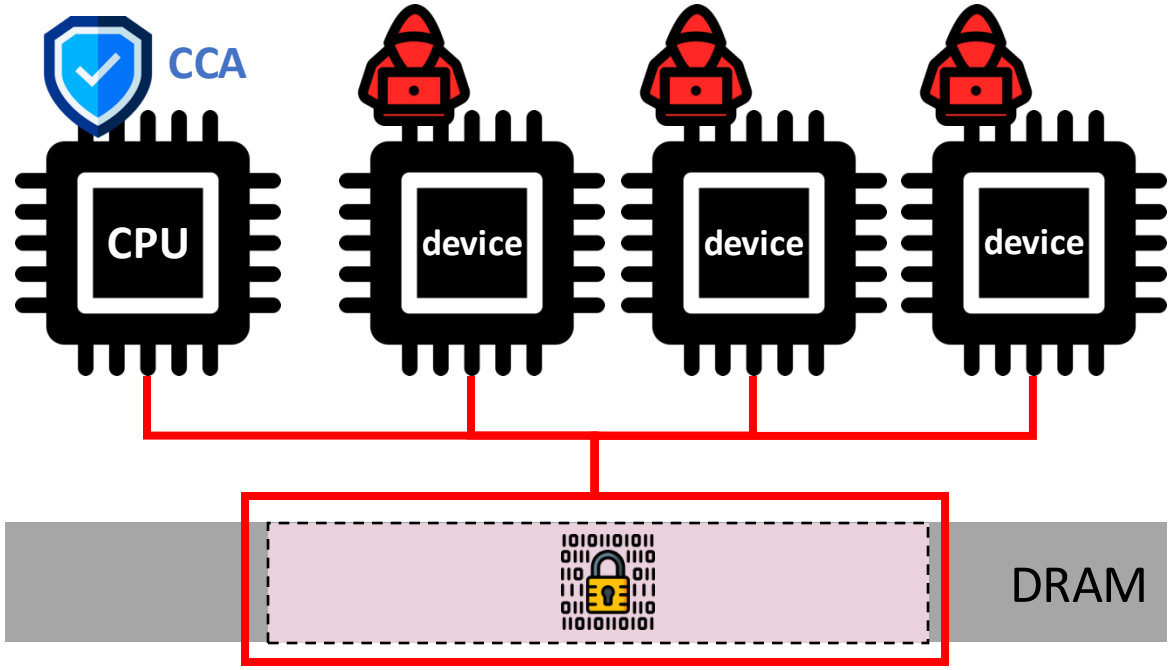
+ Robust security
- I/O performance and scalability
- Dynamic device management
- Power efficiency

→ ***Crucial for mobile platforms***

→ ***Crucial for CCA wide adoption***

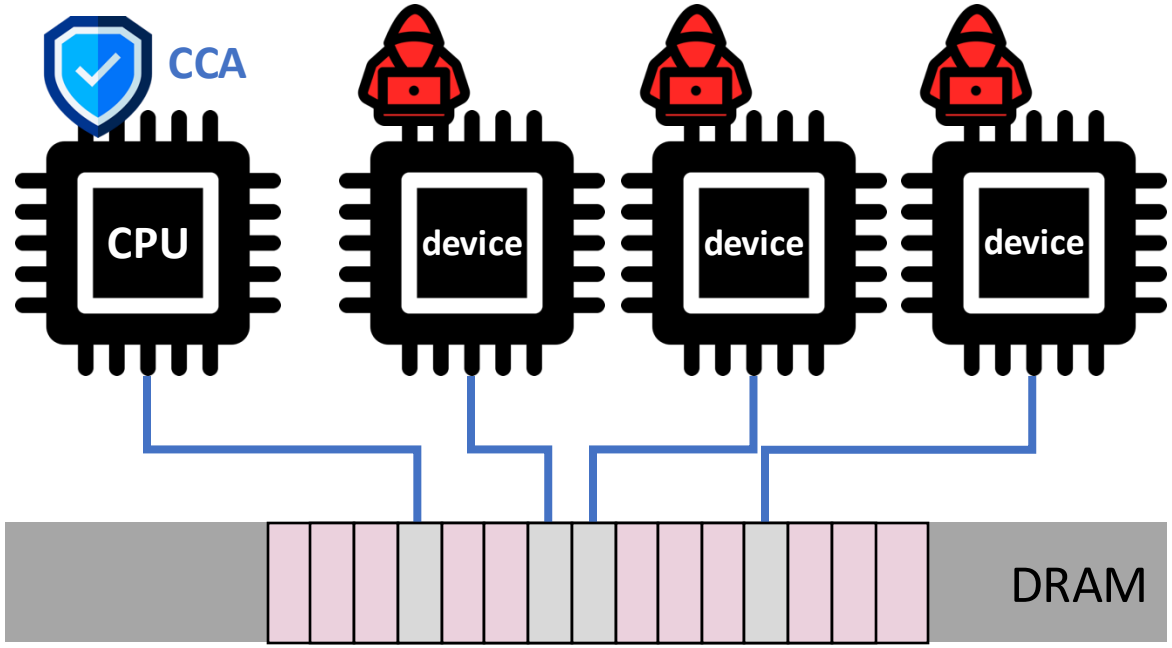
→ ***Arm CCA struggles to keep up with the architectural trend.***

Device I/O Performance and Scalability



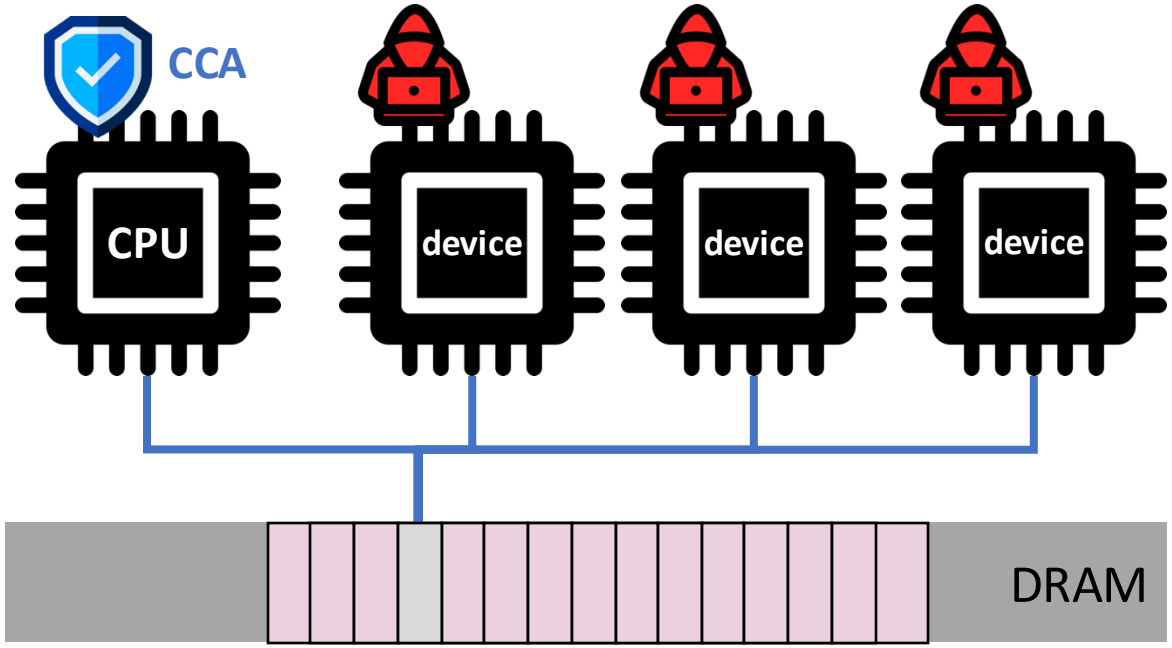
Encryption and decryption for each memory access

Device I/O Performance and Scalability



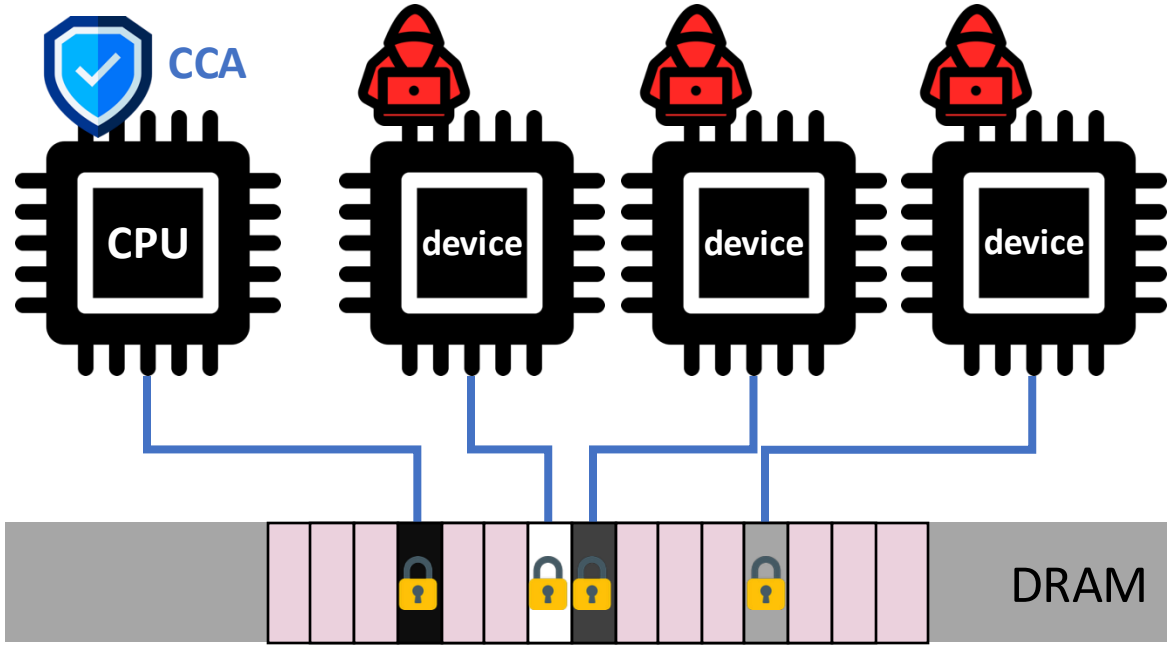
Memory Deduplication

Device I/O Performance and Scalability



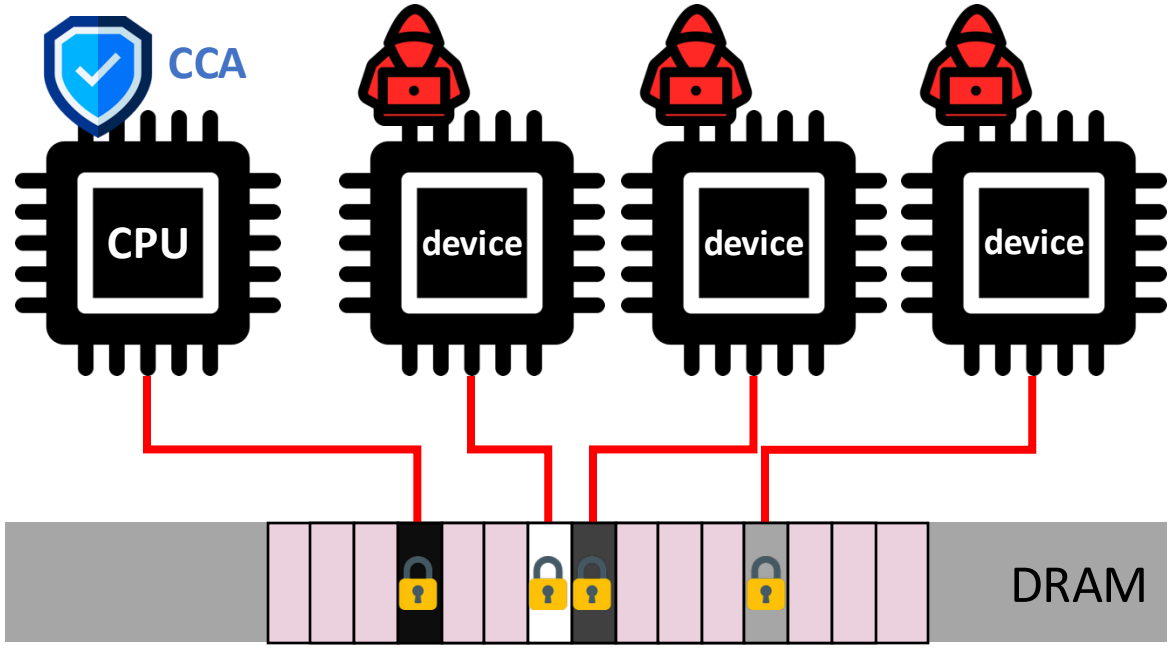
Memory Deduplication

Device I/O Performance and Scalability



Memory Encryption

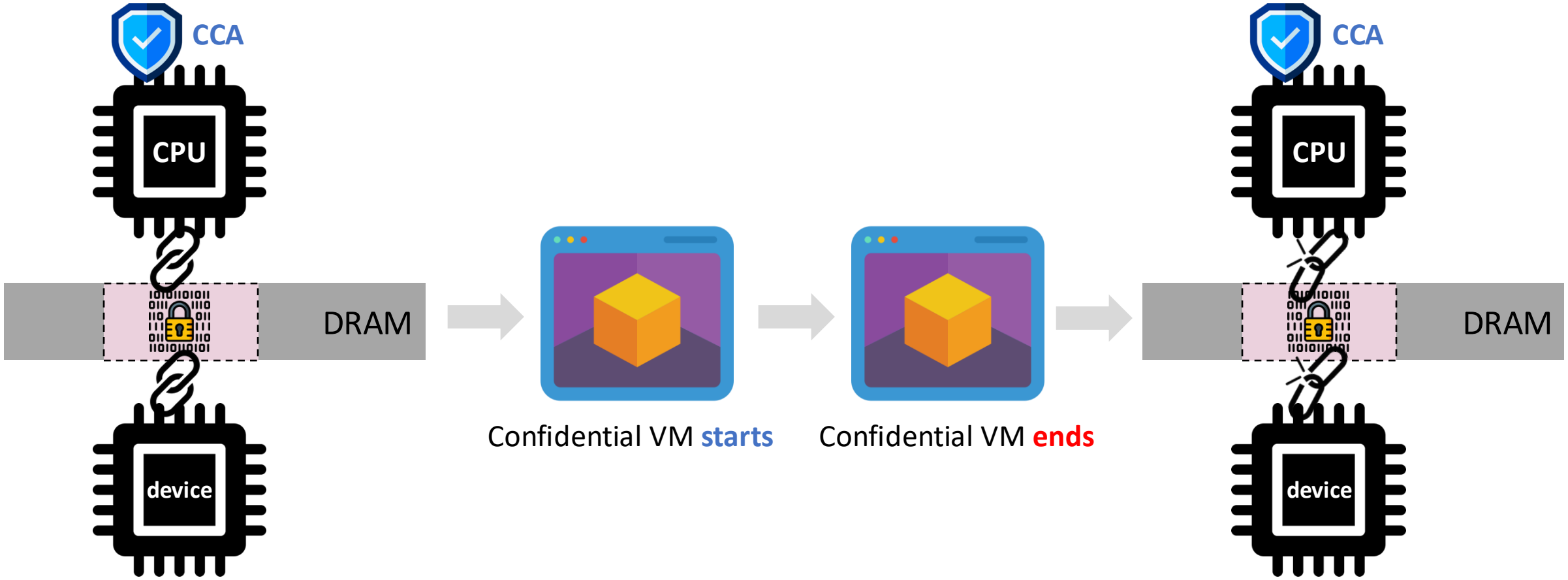
Device I/O Performance and Scalability



Memory Deduplication

Dynamic Device Management

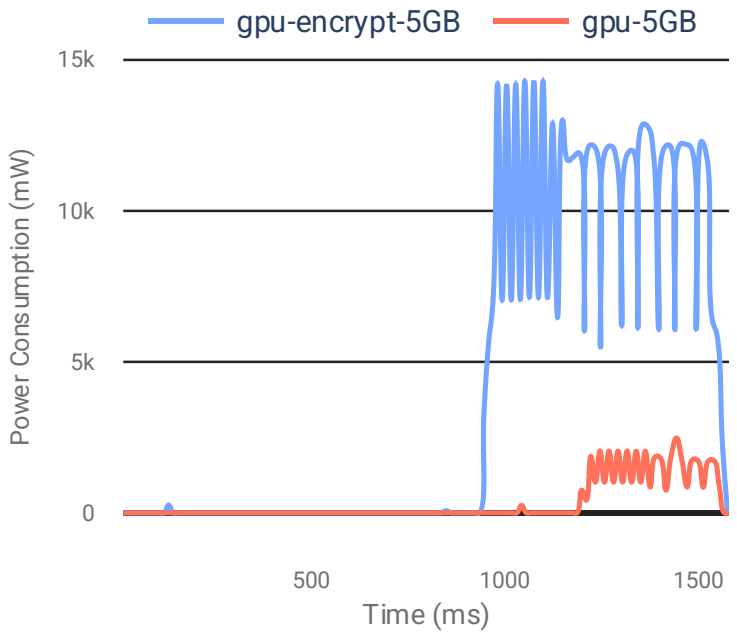
Device is bond to the entire lifespan of the confidential VM



Power Efficiency

Overhead incurred by memory encryption on mobile SoC

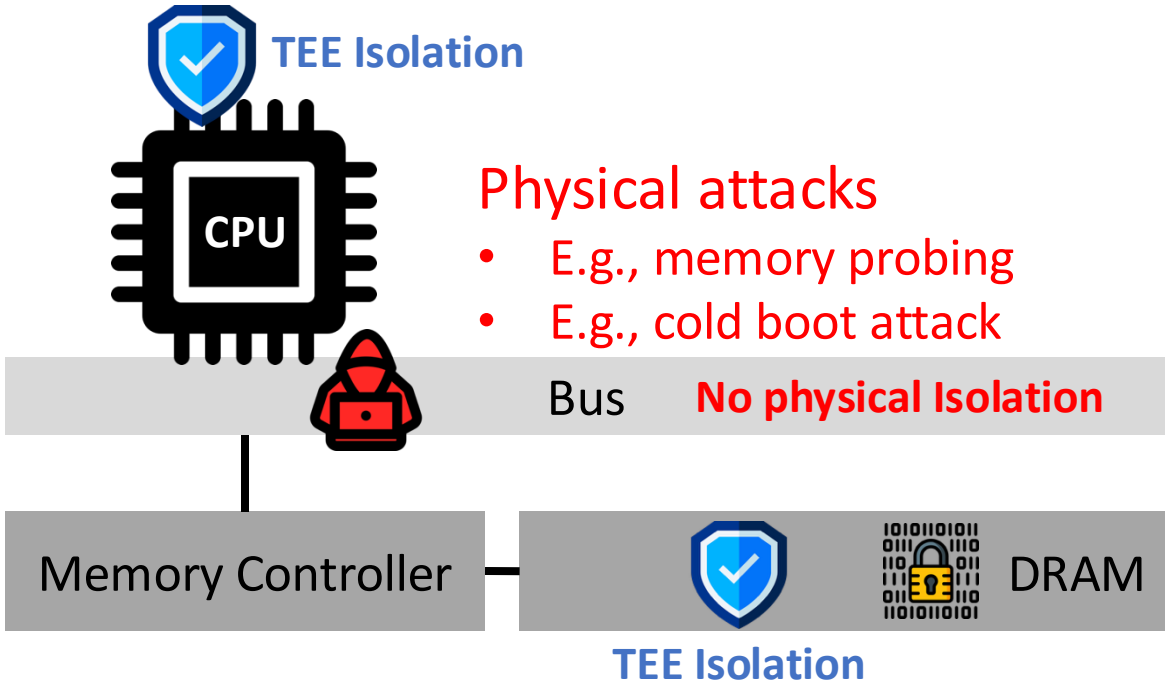
- Increased power usage
- Decreased throughput



Copying 5GB of memory with and without encryption

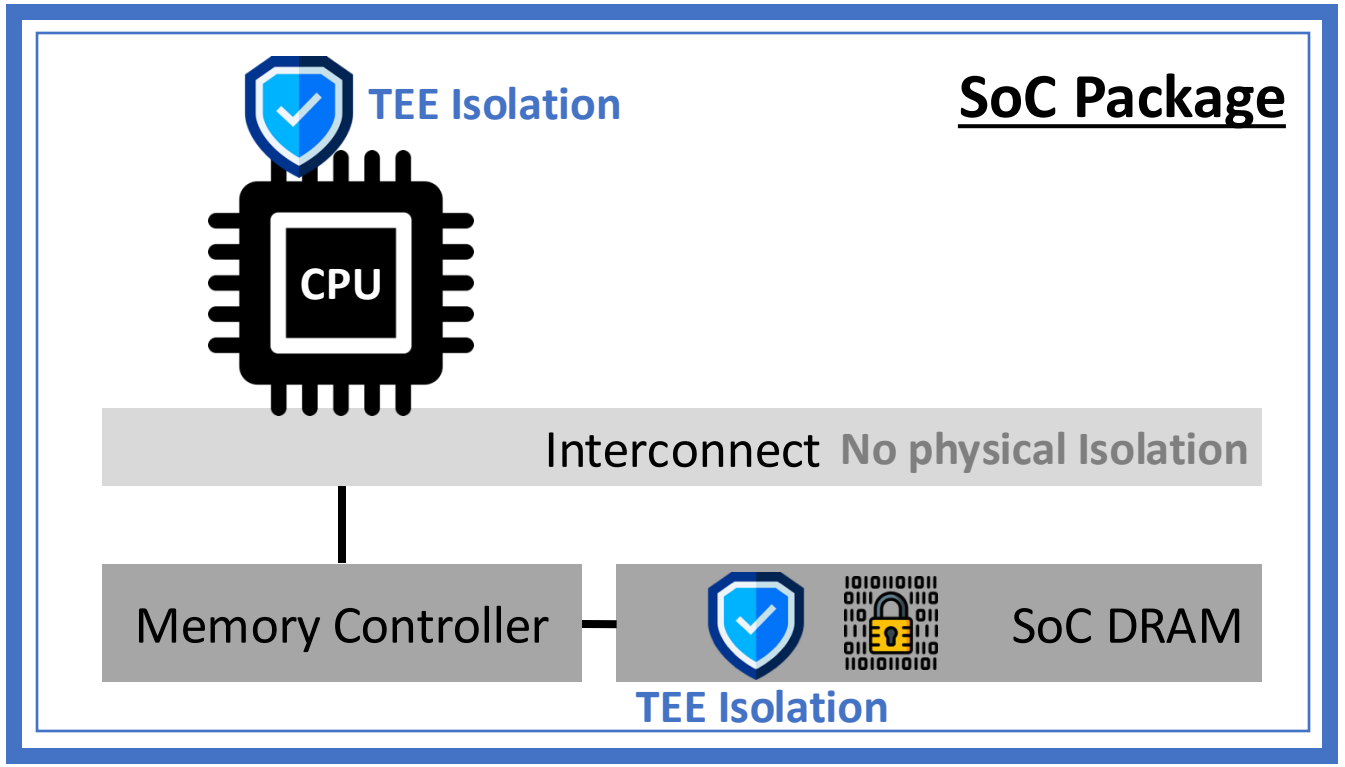
128-bit AES-GCM on Apple M1 SoC with 16GB unified memory

Memory Encryption in TEEs



Mobile Arm SoC

Integrated Memory in SoC

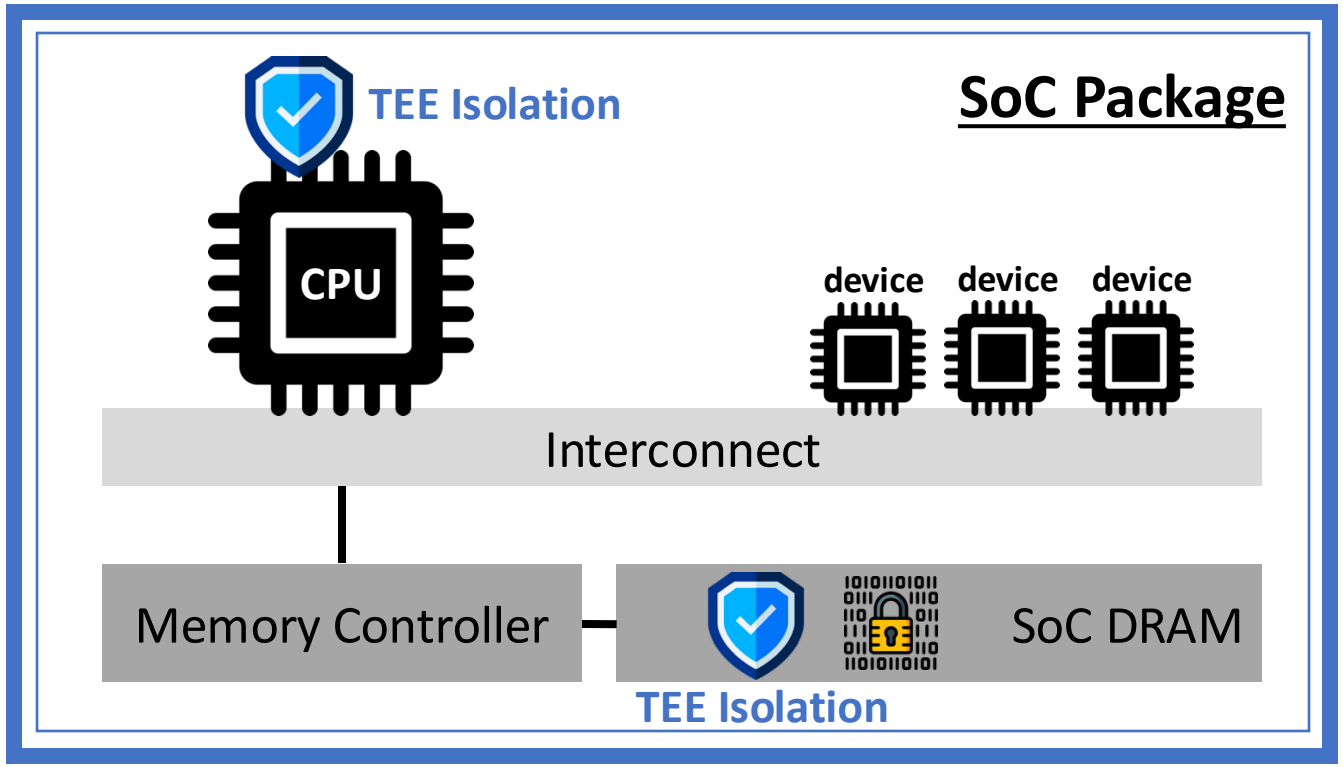


- Compact and integrated
- Advanced packaging technology
- Security features
  - E.g., tamper detection

Physical attacks
- E.g., memory probing
- E.g., cold boot attack

Mobile Arm SoC

Integrated and Unified Memory in SoC



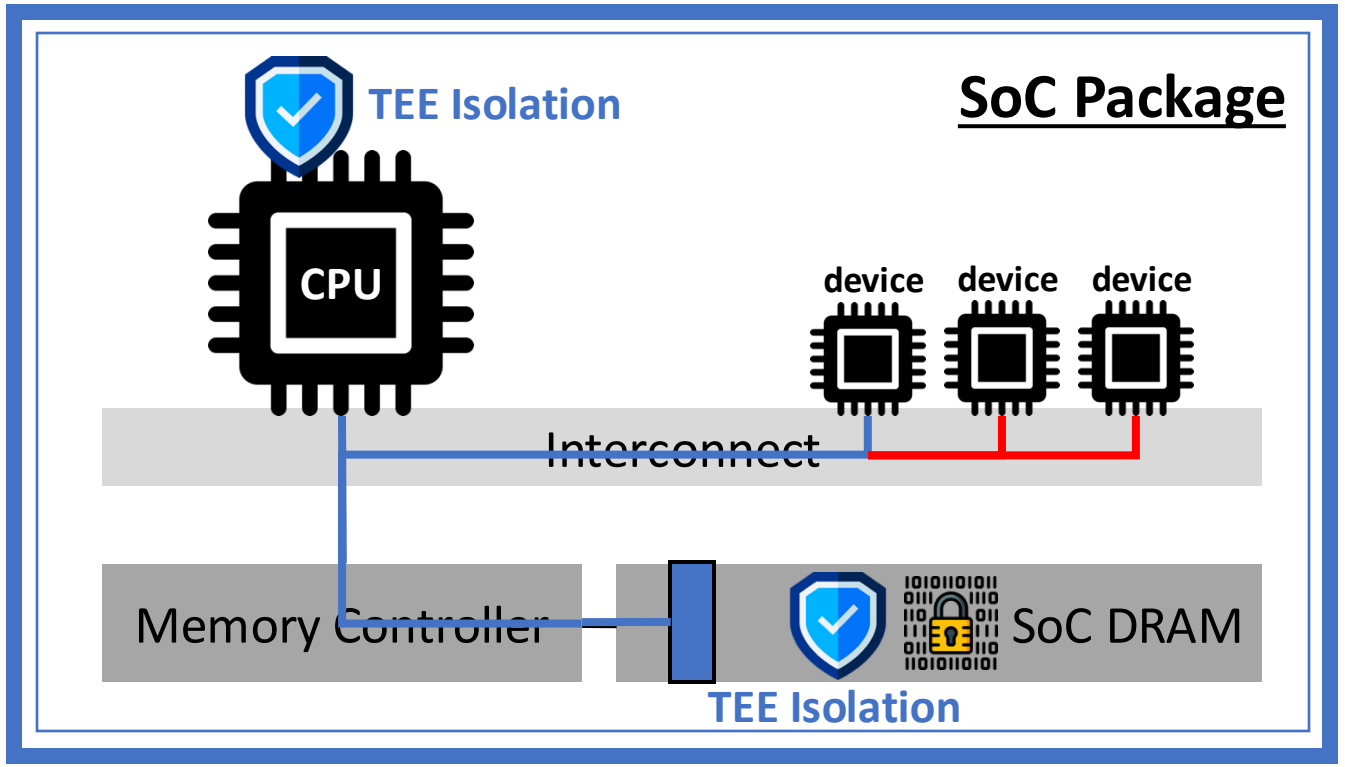
- Compact and integrated
- Advanced packaging technology
- Security features
  - E.g., tamper detection

Physical attacks

- E.g., memory probing
- E.g., cold boot attack

Mobile Arm SoC

Integrated and Unified Memory in SoC



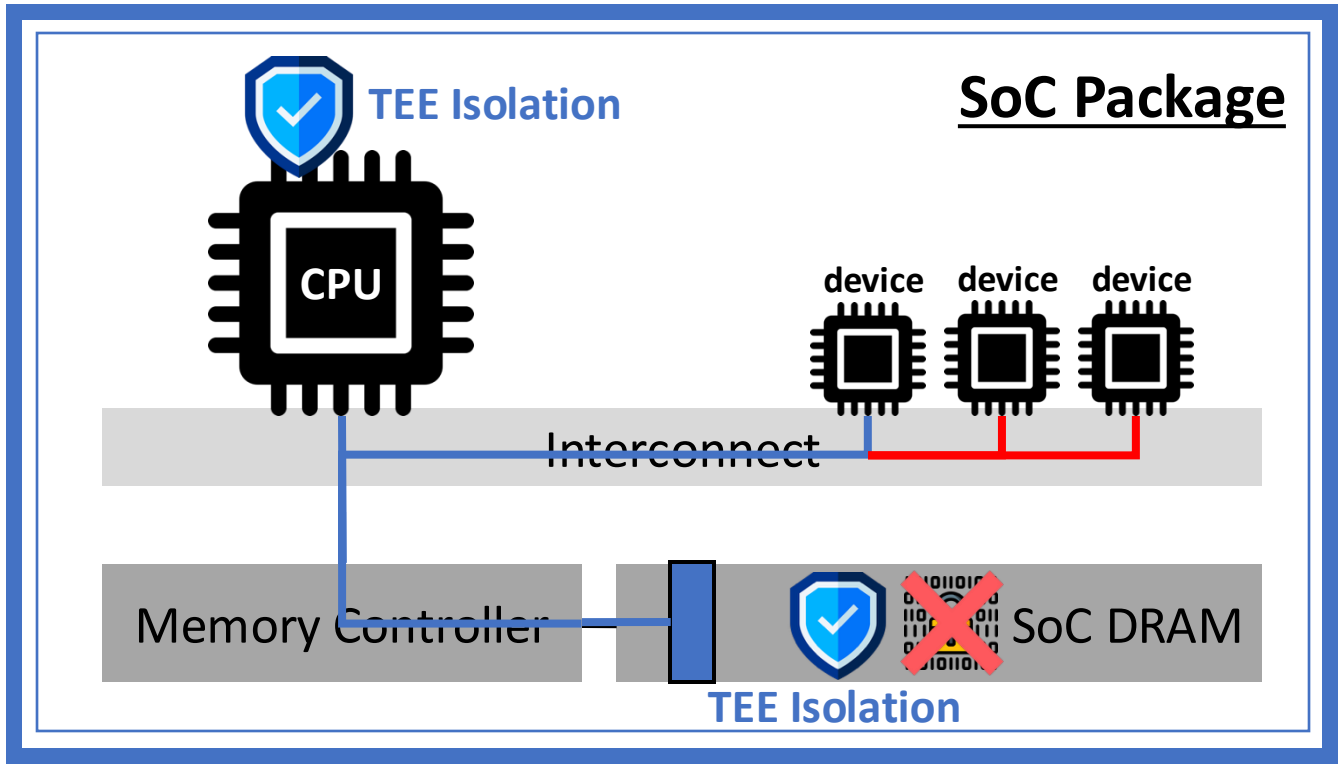
- Compact and integrated
- Advanced packaging technology
- Security features
  - E.g., tamper detection

Physical attacks

- E.g., memory probing
- E.g., cold boot attack

Mobile Arm SoC

Secure device I/O by isolation without memory encryption



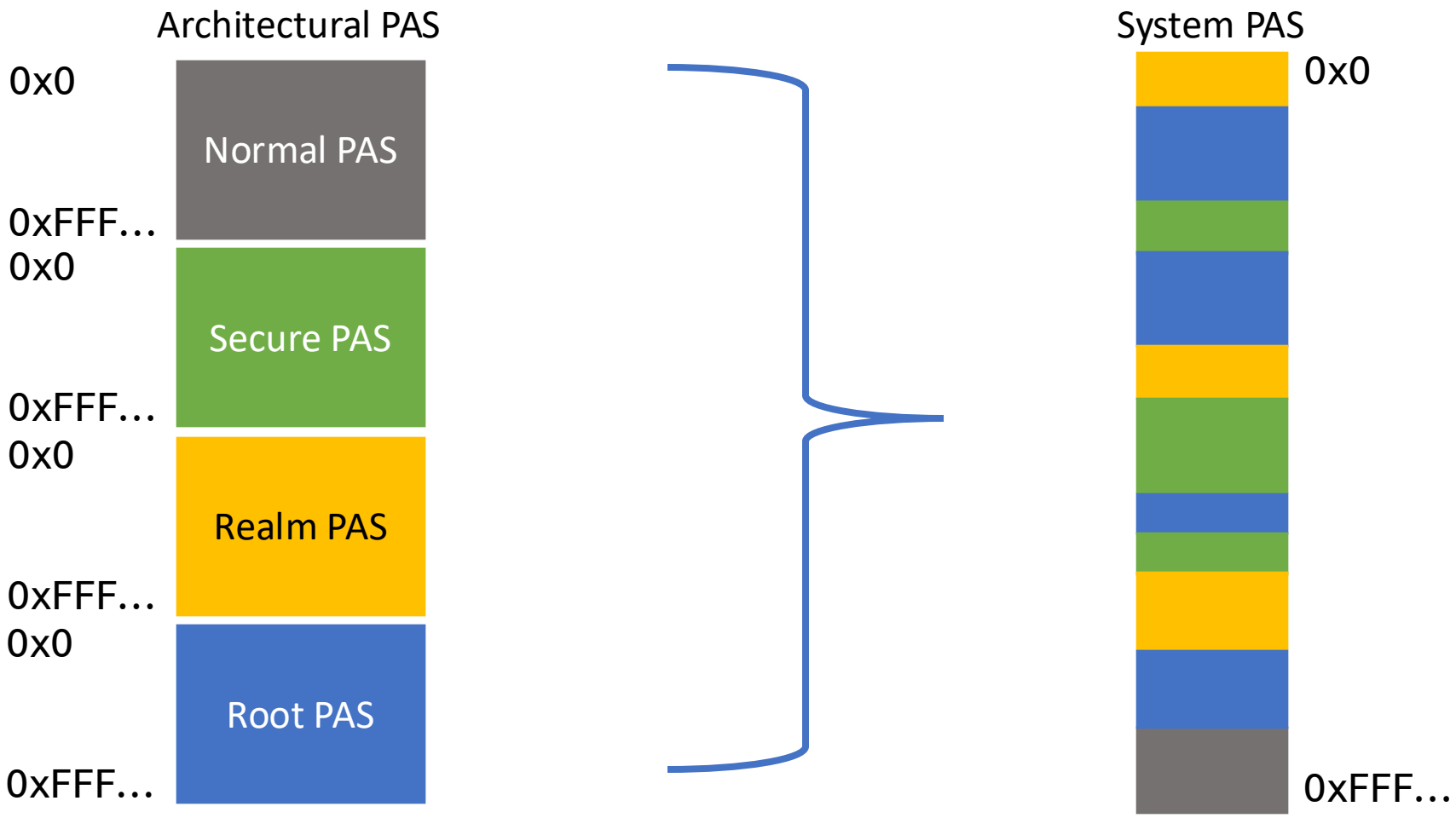
- Compact and integrated
- Advanced packaging technology
- Security features
  - E.g., tamper detection

Physical attacks

- E.g., memory probing
- E.g., cold boot attack

Arm Confidential Compute Architecture (CCA)

Physical Address Spaces (PAS)



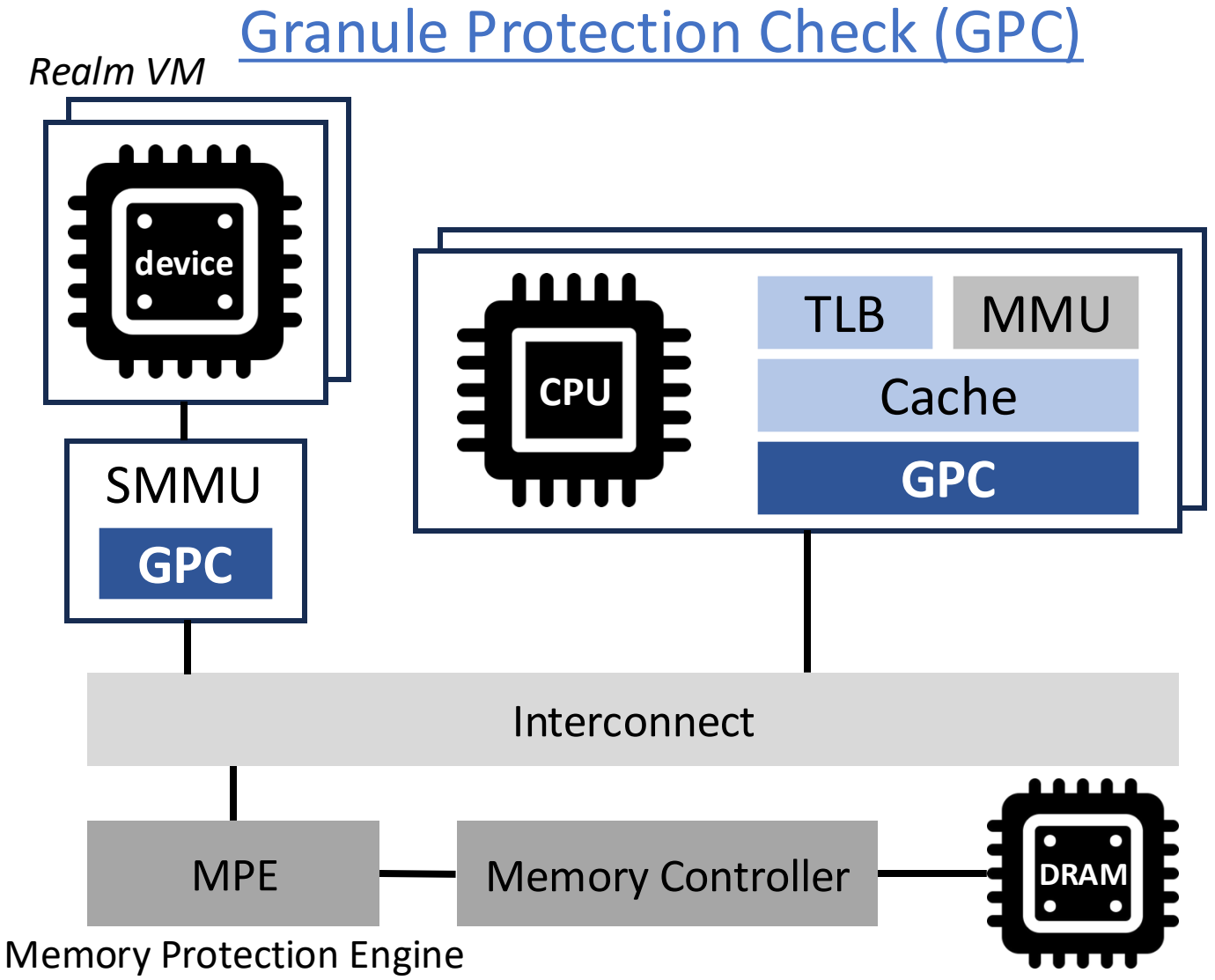
Arm Confidential Compute Architecture (CCA)

Granule Protection Check (GPC)

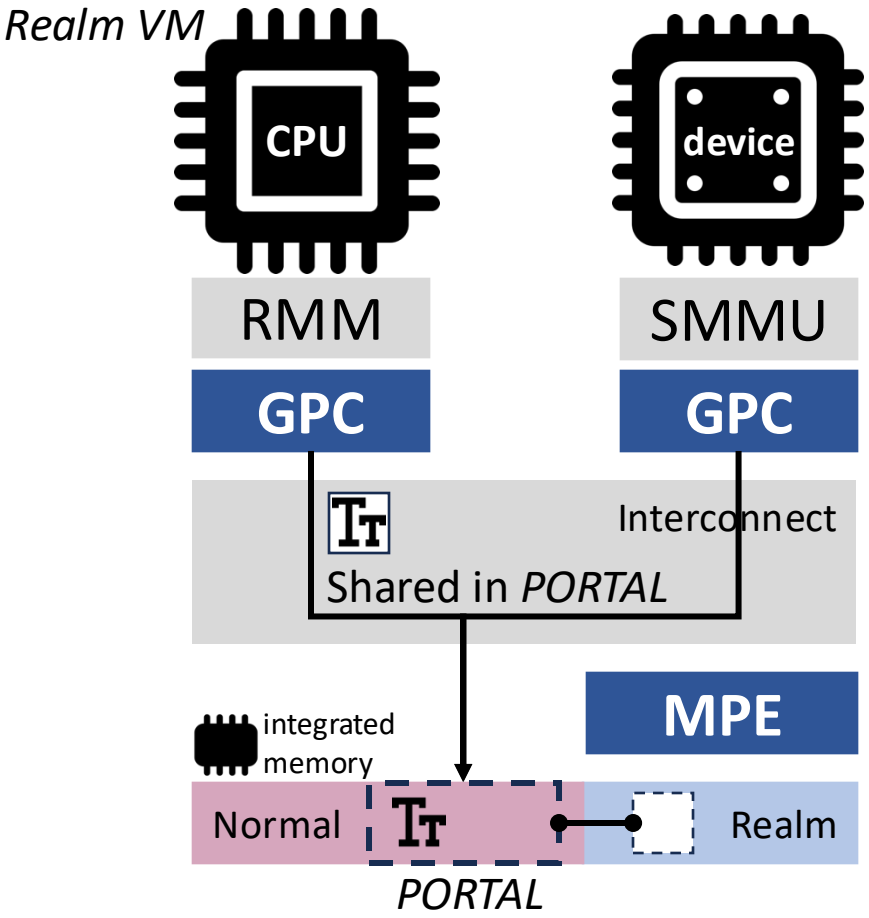
Security State	Normal PAS	Secure PAS	Realm PAS	Root PAS
Normal	✓	✗	✗	✗
Secure	✓	✓	✗	✗
Realm	✓	✗	✓	✗
Root	✓	✓	✓	✓

Granule Protection Table (GPT) stores PAS to world assignments and is managed in the Root world.

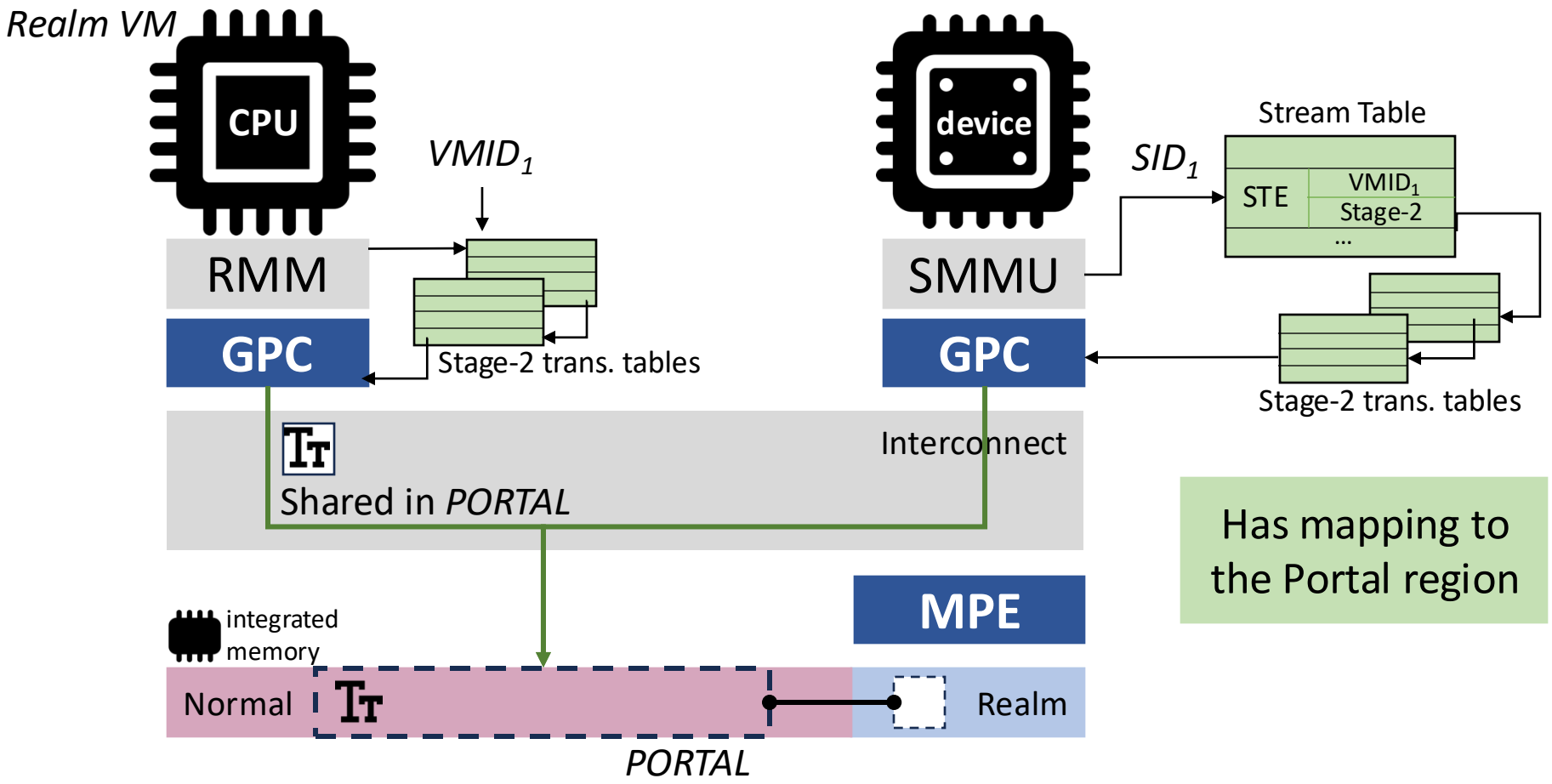
Arm Confidential Compute Architecture (CCA)



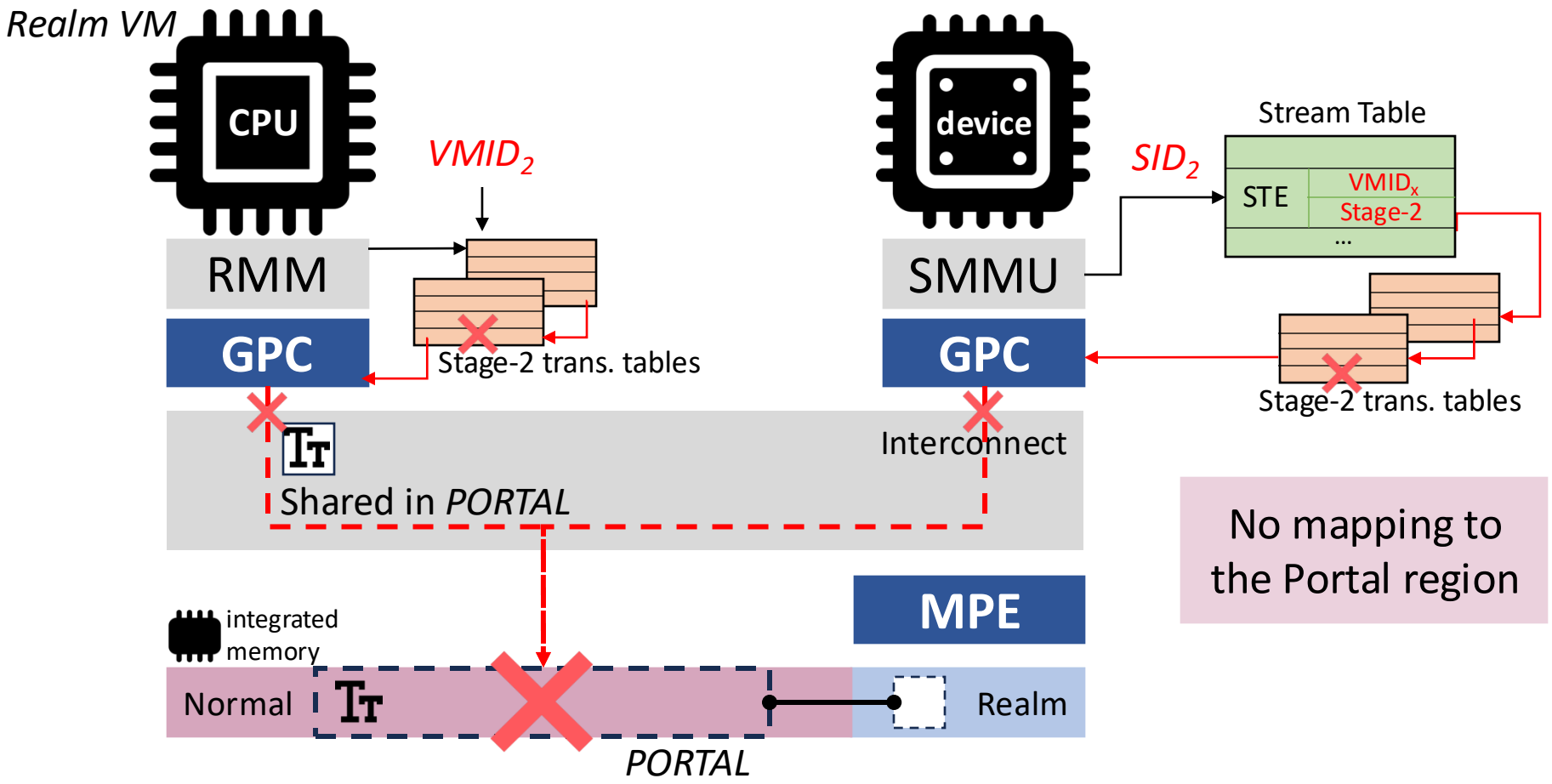
High Level Approach



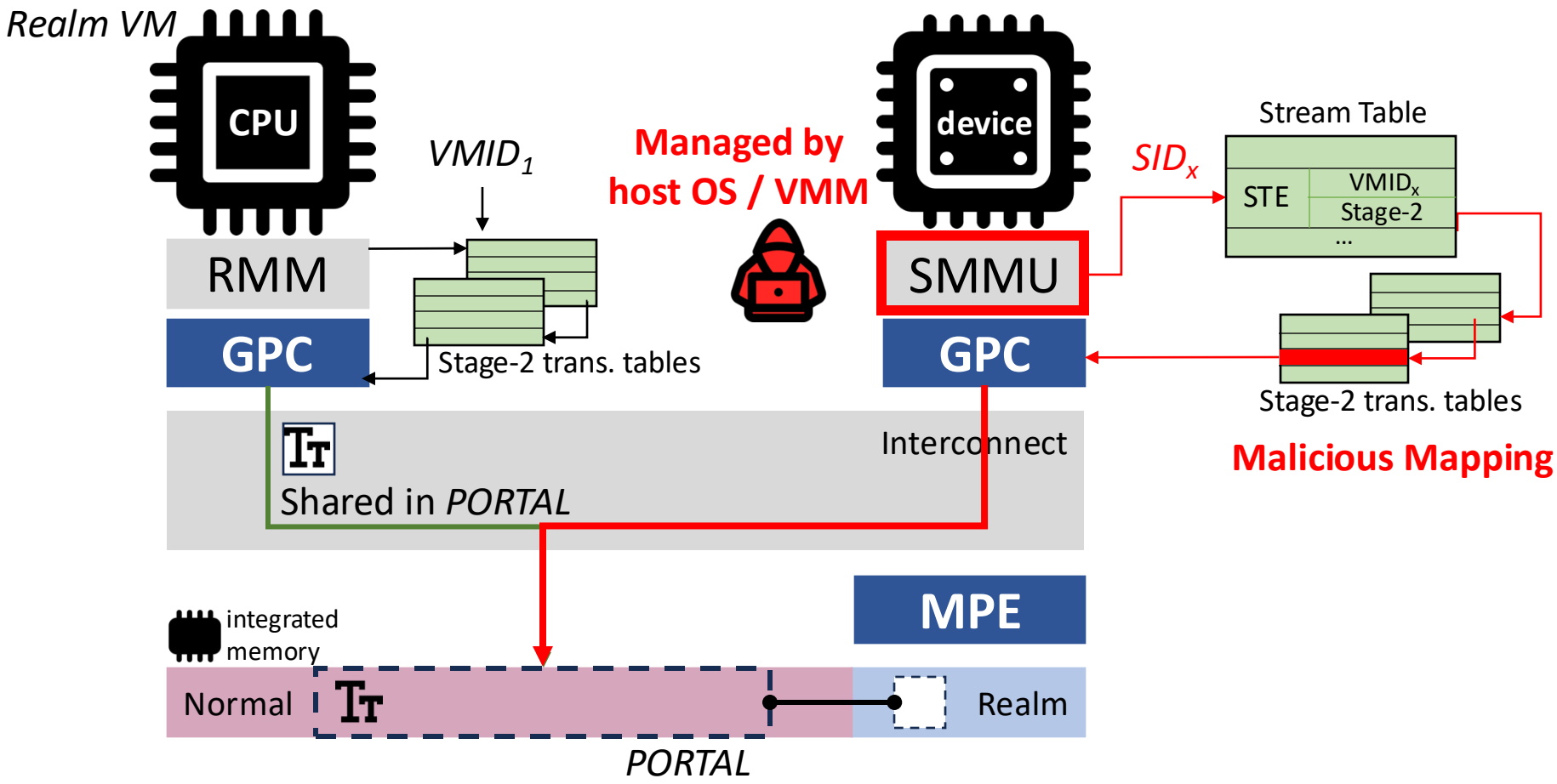
Protected Memory Region



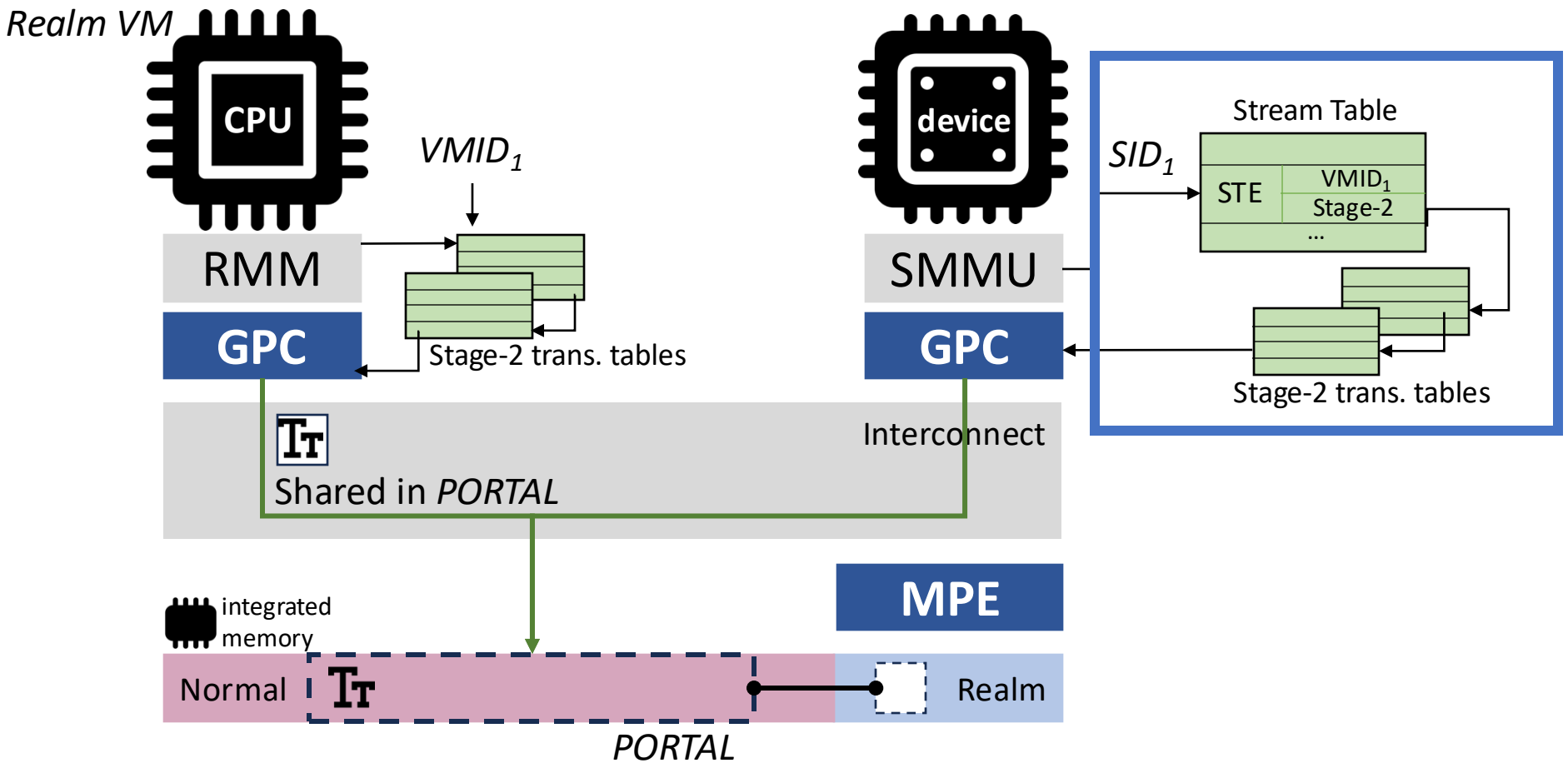
Protected Memory Region



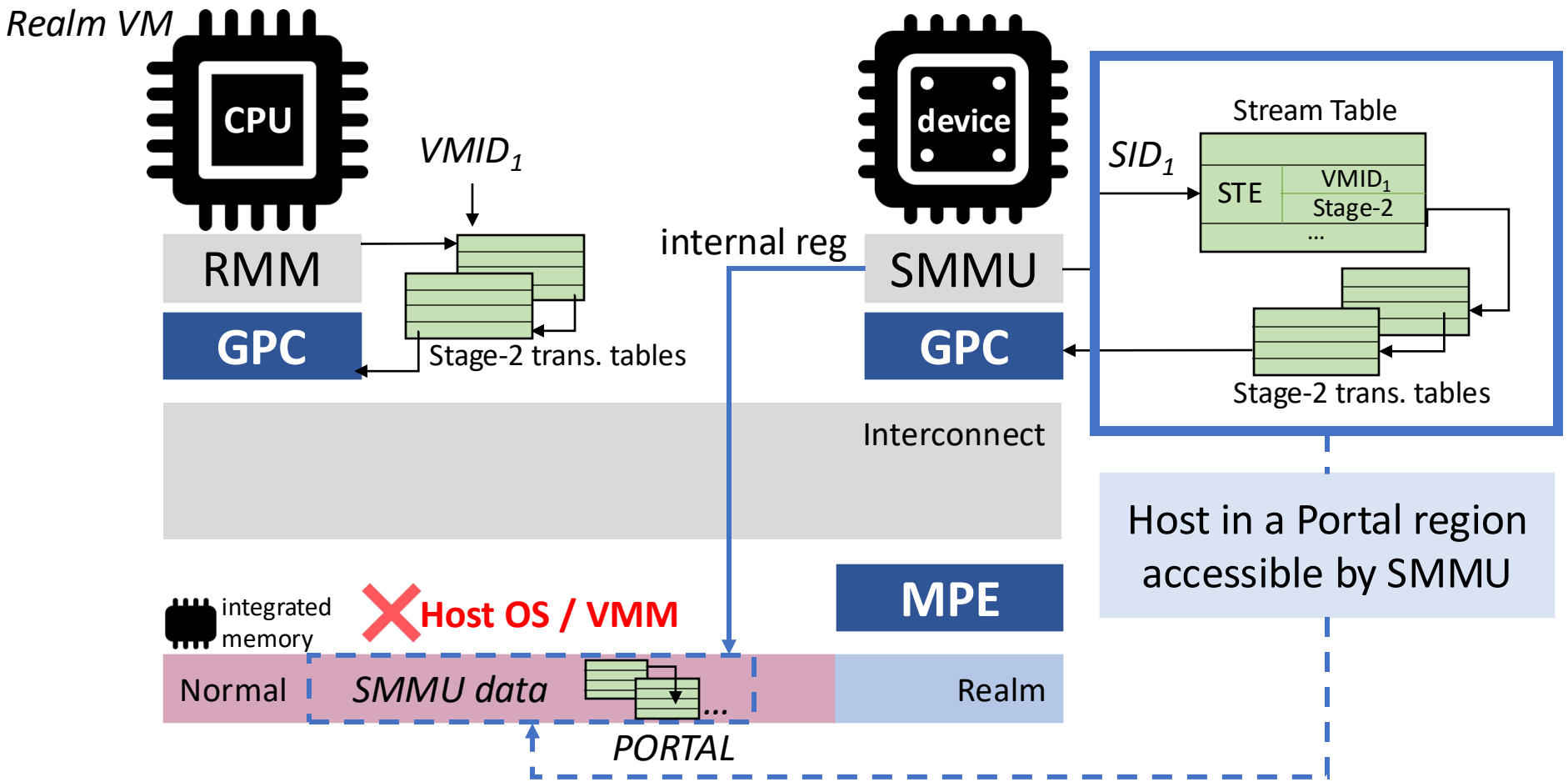
SMMU Managed by Untrusted Host OS / VMM



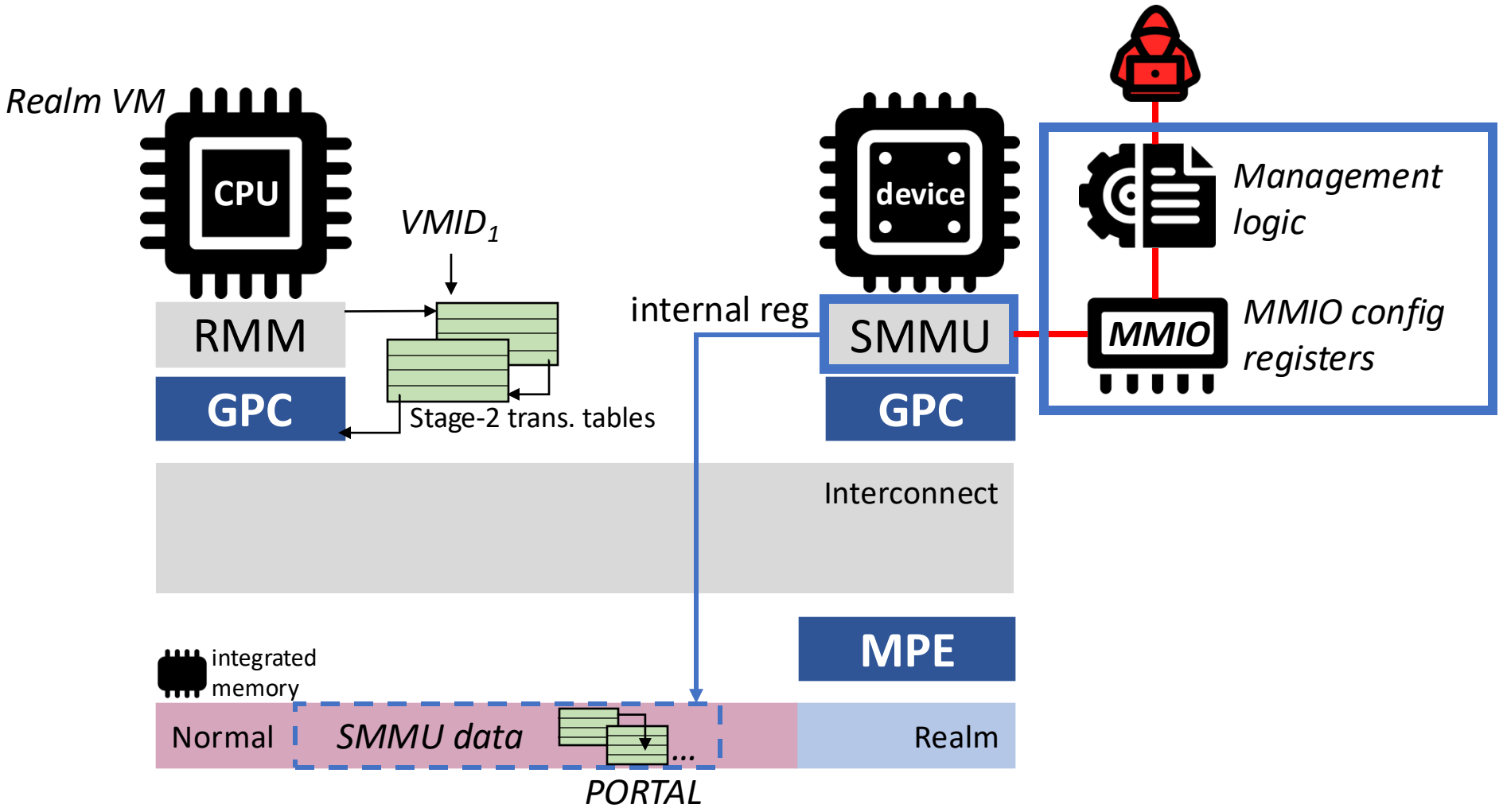
Protection of SMMU Data Structures



Protection of SMMU Data Structures

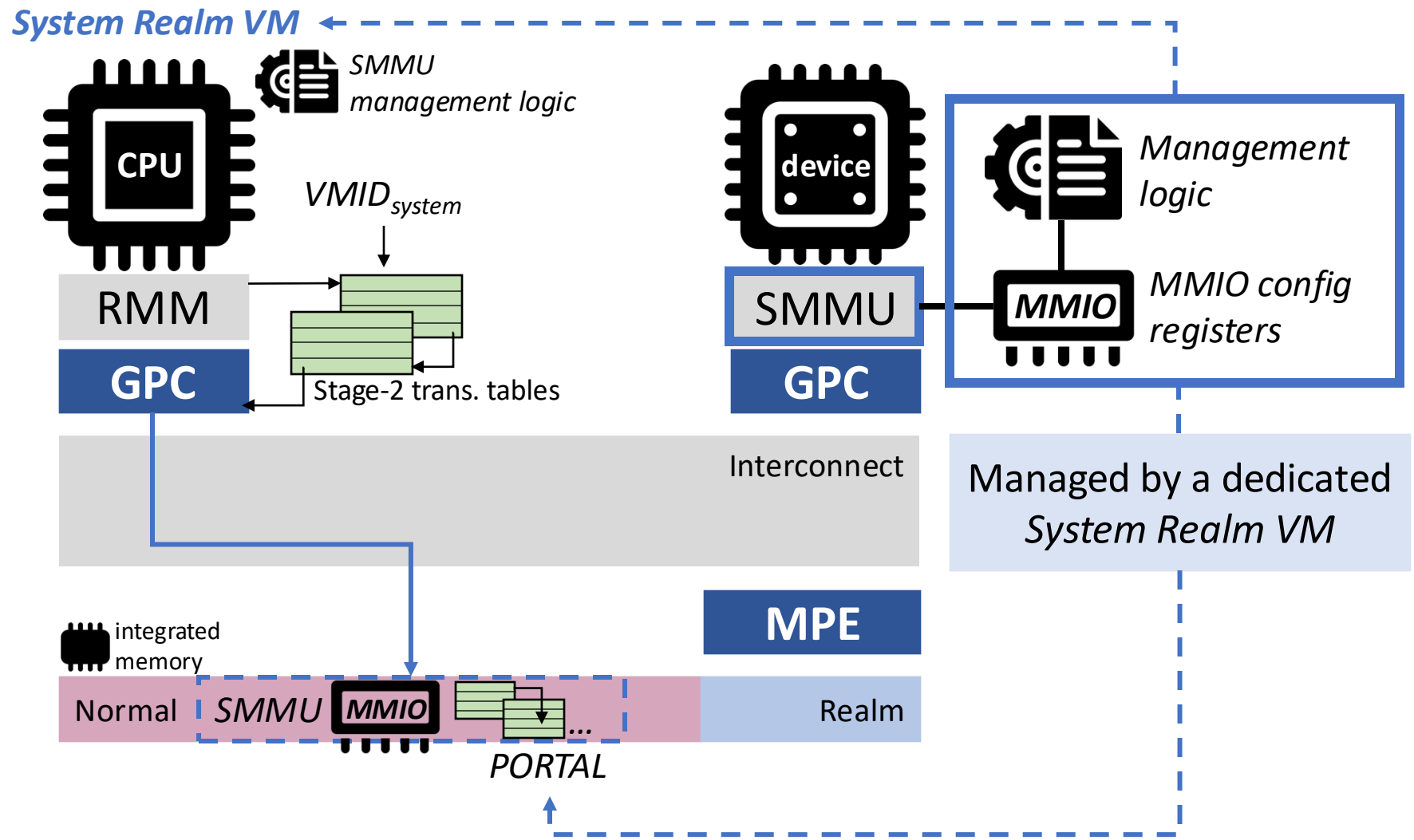


Protection of SMMU Management



Protection of SMMU Management

Manage SMMU *on behalf of* host and other Realms



Implementation

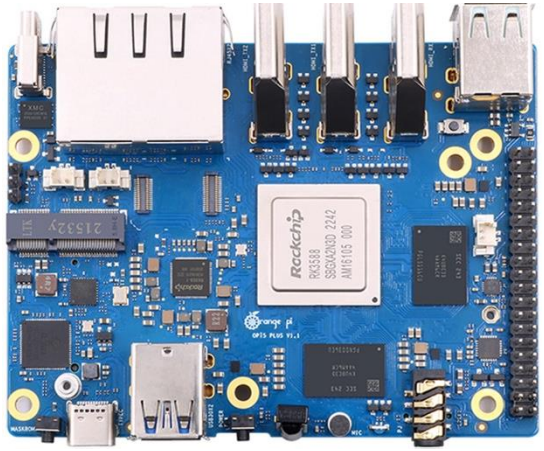
Functionality Prototype

- Arm FVP_Base_RevC2XAEMvA with RME support
- A connected test engine
  - Simulates a DMA-capable peripheral
  - An SMMU that supports RME
- **0.5MB** memory for device GPTs
- A reference implementation of the System Realm

Implementation

Performance Prototype

- Migrate FVP prototype to Orange Pi 5 Plus
  - RK3588 SoC
  - 8-core 64-bit Arm processor (4-core A76 and 4-core A55)
  - Arm Mali-G610 GPU
  - 8GB of shared DRAM
- Emulation of Arm CCA (Armv9) with Armv8 features



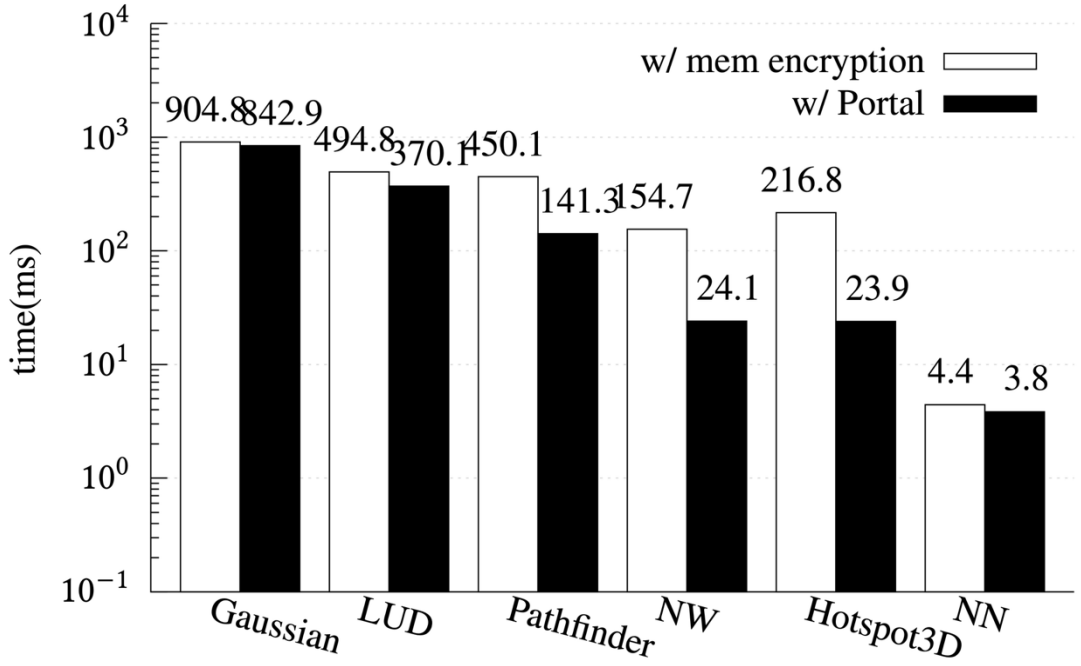
Performance Evaluation

- Performance of GPU tasks
- Rodinia GPU benchmark
- AES-GCM-based encrypted memory
- **3.71× (1.07×-9.07×)** performance

Overhead due to memory encryption
- Simpler processing logic
- Larger data size

Portal's advantage
+ Data intensive applications
+ Frequent transmission of larger data size

Application	Problem Size	Data Buffers	Memory
Gaussian	1024 × 1024 nodes	3	8.39 MB
LUD	2048 × 2048 nodes	1	16.00 MB
Pathfinder	100000 × 100 points	4	40.46 MB
NW	2048 × 10 nodes	2	16.79 MB
Hotspot3D	512 × 512 × 8 nodes	3	25.16 MB
NN	42764 nodes	2	0.51MB



Thank you!

PORTAL

Fast and Secure Device Access with Arm CCA
for Modern Arm Mobile System-on-Chips (SoCs)

Fan Sang[1], Jaehyuk Lee[1], Xiaokuan Zhang[2], Taesoo Kim[1]

[1]Georgia Institute of Technology, [2]George Mason University

fsang@gatech.edu

Georgia Tech College of Computing
School of Cybersecurity
and Privacy