明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

# TS-Perf: Performance measuring method in the TEE (Trusted Execution Environment) of various CPUs

## RISC-V Day Tokyo Summer 2024
## August/1

IISEC: Institute of Information Security（情報セキュリティ大学院大学）
Kuniyasu Suzaki（須崎 有康）

# Who am I ? (Kuniyasu Suzaki)

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

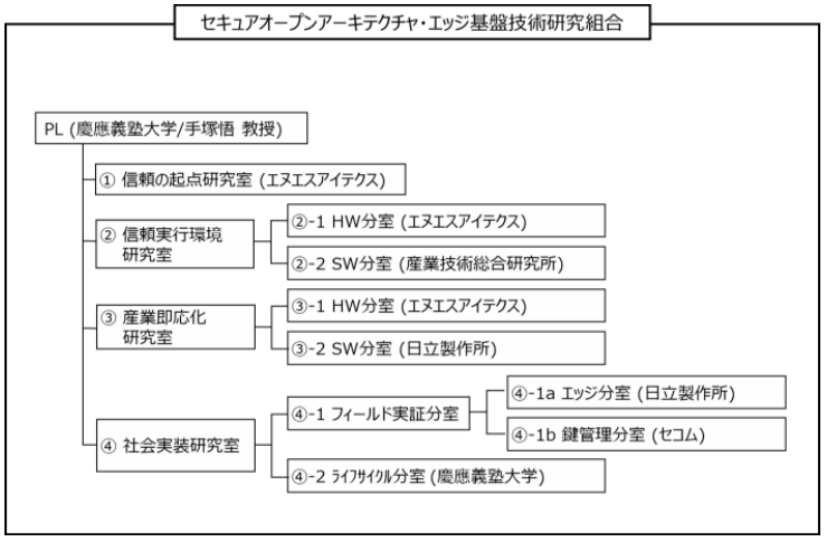
■ Professor, IISEC: Institute of Information Security (Graduate School) from 2022/9/1

● Former : AIST (National Institute of Advanced Industrial Science and Technology)

Joined a national project (2018-2023) for RISC-V based TEE research at TRASIO (Technology Research Association of Secure IoT Edge application based on RISC-V Open architecture)

◆TRASIO members were Hitachi, NSITEXE (Current Denso), SECOM, Keio University, and AIST.

**研究体制図**




- セキュアオープンアーキテクチャ・エッジ基盤技術研究組合 (TRASIO)
- NEDOプロジェクト「セキュアオープンアーキテクチャ基盤技術とそのAIエッジ応用研究開発 FY2018-2022」

# Contents



- What is TEE (Trusted Execution Environment) ?
  - RISC-V TEE “Keystone” (based on PMP: Physical Memory Protection)
- Why is measuring performance difficult on TEE?
- TS-Perf
  - Used Techniques
    - ◆Portable Library which offers same APIs.
    - ◆Separate Compilation
    - ◆Report after TEE process termination  because of communication overhead between TEE and REE.
- Conclusion

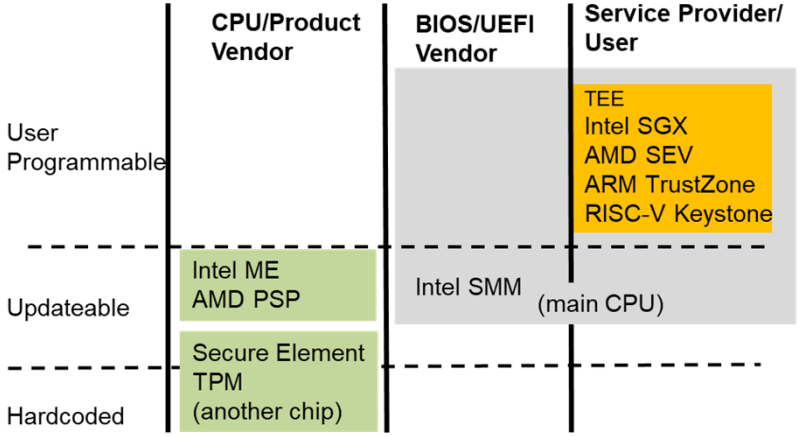
This presentation is based on

- TS-Perf: General Performance Measurement of Trusted Execution  Environment and Rich Execution Environment on Intel SGX, Arm TrustZone, and RISC-V Keystone [IEEE Access 2021]
- Library Implementation and Performance Analysis of GlobalPlatform TEE Internal API for Intel SGX and RISC-V Keystone [TrustCom 2020]

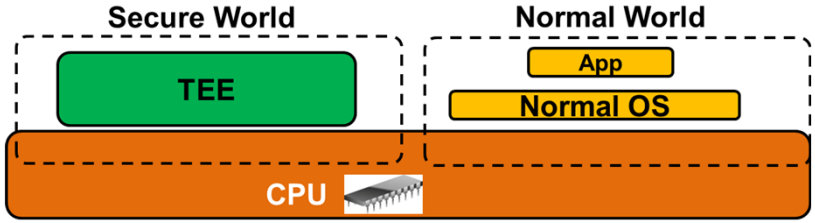
# What is TEE? (1/2)



- TEE (Trusted Execution Environment) is one of HIEE(Hardware-assisted Isolated Execution Environments)
  - HIEE includes
    - ◆X86 SMM (System Management Mode) used by BIOS/UEFI
    - ◆Intel ME (Management Engine)  and TPM which are anther chip.
  - TEE is featured to be programable by third party.




- TEE separates CPU into two worlds.
  - Normal World (i.e., REE: Rich Execution Environment)
    - ◆Normal OS(Linux, Windows) runs
  - Secure World (i.e., TEE: Trusted Execution Environment)
    - ◆It is independent form vulnerabilities of OS and Hypervisor.
    - ◆Critical apps runs.



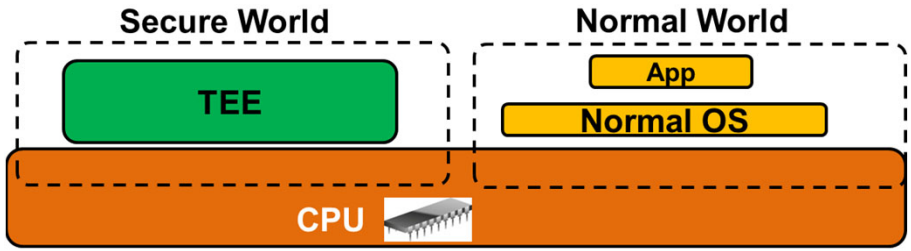

Typical Figure

# What is TEE? (2/2)



- Features:
  - (To speak radically) TEE offers **a temporal isolation execution only**.
  - Long term key managements require another method.
    - ◆Hardware Root of Trust is an anti-tamper hardware to store keys.
    - ◆Remote Attestation (method to confirm the soundness of hardware and software) is based on the keys saved in Hardware Root of Trust.

- Available CPUs
  - ARM TrustZone (Smart phone)
  - Intel SGX (PC, Server), Intel TDX(Server)
  - AMD SEV (Server)
  - RISC-V has many (later slide)




TEE's Image
(This image resembles to Arm TrustZone)

- Some TEEs are based on virtualization technology, called Confidential Computing and used on Cloud mainly.

# Apps on TEE and CC

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Critical Processing
  - Key Management
    - Android KeyMaster
  - DRM
    - Smartphone's Widevine(Google)
    - Windows Ultra HD Blu-ray Viewer uses Intel SGX
  - Personal Info
    - Fingerprint authentication
    - FIDO Authenticator
    - Hardware Wallet for Crypto Currency
- Data and Code Hiding
  - Machine Learning
  - Privacy Protection
  - Gene Data Processing

Killer Application on TEE of Smartphone.

Cannot be Killer App.

Candidate for Killer App?

- Small Memory
- Suitable for Smartphone
- Arm TrustZone

- Large Memory
- Required Server & Cloud
- Intel SGX、AMD SEV
- **Target of Confidential Computing?**

- RISC-V?

Candidate for Killer App on Cloud?

# RISC-V TEE



- TEE based on RISC-V

Academia
- Sanctum [MIT,USENIX Sec'16]
- TIMBER-V [Graz University of Technology, NDSS'19]
- MI6 [MIT,MICRO'19]
- **Keystone** [UC Berkeley, EuroSys'20]
- HECTOR-V [Graz University of Technology, arXiv'21]
- uTango [University of Minho, arXiv'21]
- Cure [Darmstadt University of Technology,USENIX Sec'21]
- CHERI-TrEE [University of Cambridge, IEEE S&P'23]
- HPMP (Hybrid Physical Memory Protection) [Shanghai Jiao Tong University, MICRO'23]

Industry
- MultiZone [HexFive]
- SiFive Shield / World Guard [SiFive]
- AP-TEE（Application Processor –TEE) [RISC-V International TEE WG]
- CoVE (Confidential Virtual Machine for RISC-V) [Rivos Inc., arXiv'23]

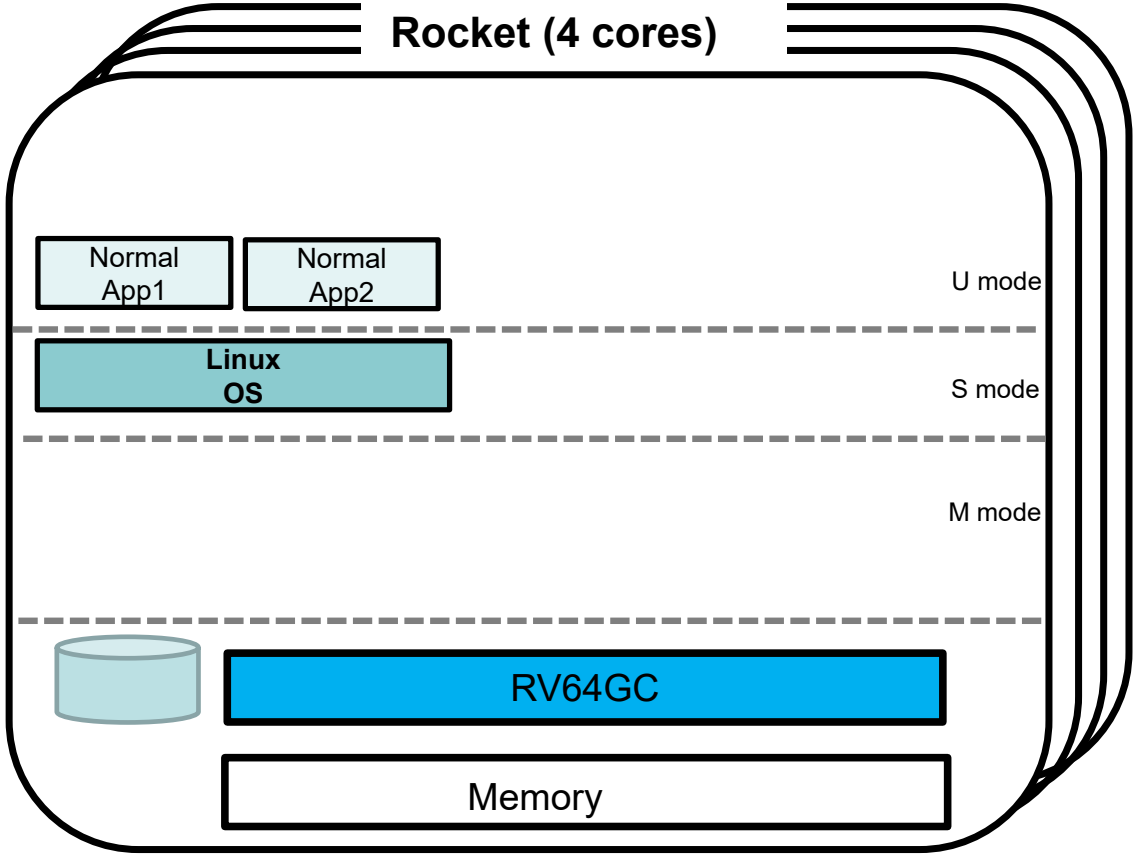
Many implementations require hardware extension Keystone and MultiZone use PMP (Physical Memory Protection) which is default function of RISC-V.

# RISC-V TEE "Keystone"

- TEE developed by UC Berkeley
  - The developments are lead by RISC-V core members (Prof. Krste Asanović)
  - PMP(Physical Memory Protection), which is defined by Privileged Architecture Specification, is utilized.
  - A Project of CCC(Confidential Computing Consortium)

# Normal 64bit RISC-V

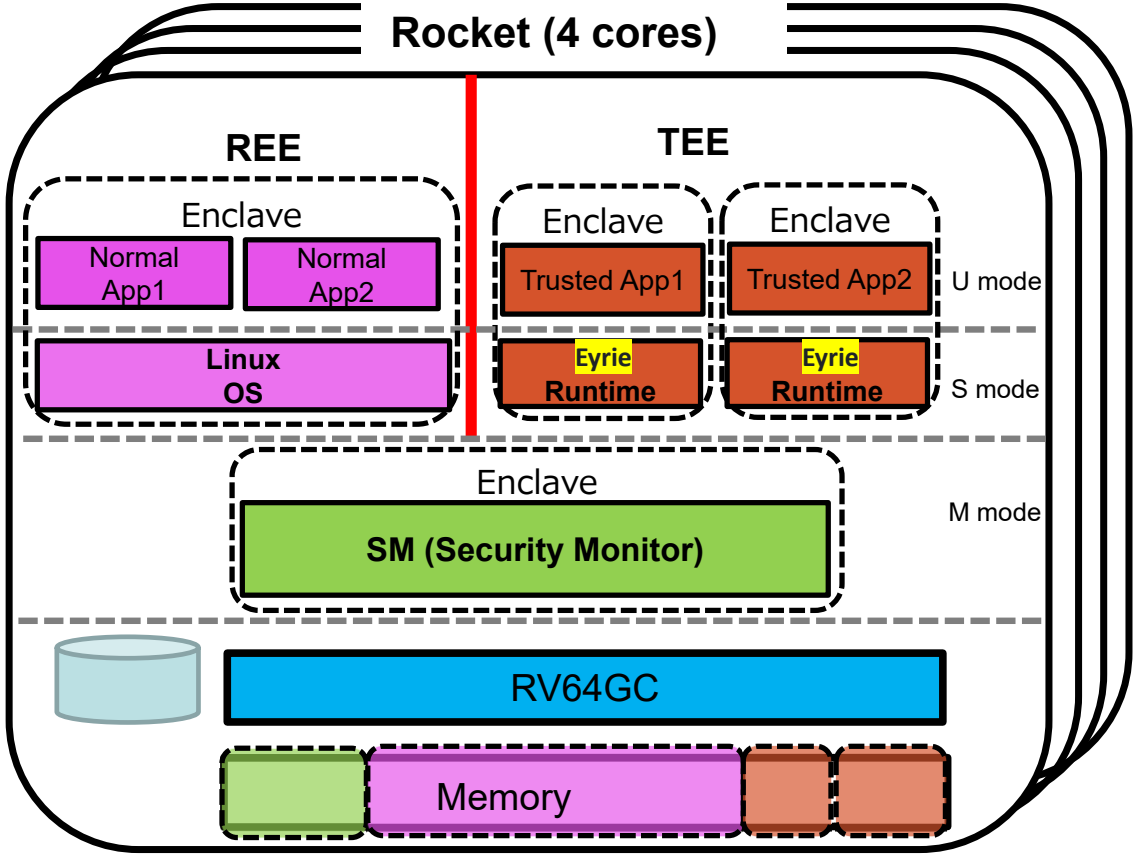





- This figure assumes Linux on 64bit Rocket (4 cores)
  - Apps uses User Mode
  - Linux Kernel uses Supervisor Mode
  - Interrupts go to M mode and the handlers runs in Supervisor mode. (This figure omits the parts)

# Keystone on RISC-V






- No Hardware modification
- Memory Protection by PMP
  - PMP can separate memory regions and execution environments.
  - PMP has priority (high – low).
- Each PMP offers “Enclave”
  - The highest PMP is used by “Secure Monitor” (M mode)
  - The lowest PMP is used by “Linux” as REE
  - In this figure 2 TEEs (Enclaves) use PMP.

# Why is measuring performance difficult on TEE?



■ There are 3 problems.

1. Most TEE assumes original SDK (Software Development Kit), which makes difficult to compare the performance.
   - RISC-V Keystone assumes “Eyrie” as an OS environment, which is not POSIX.
2. Different binaries between TEE and REE
   - Application’s performance on TEE and REE can not be easily compared because most binaries are build for TEE and REE.
3. The communication overhead is heavy between TEE and REE.
   - TEE has no display and needs to communicate to the REE, but the overhead is heavy. The measurement results cannot report immediately because it affects the TEE performance.

TS-Perf solved these problems.

# Problem 1: different TEE SDKs



- This problem is solved by offering the same API library.

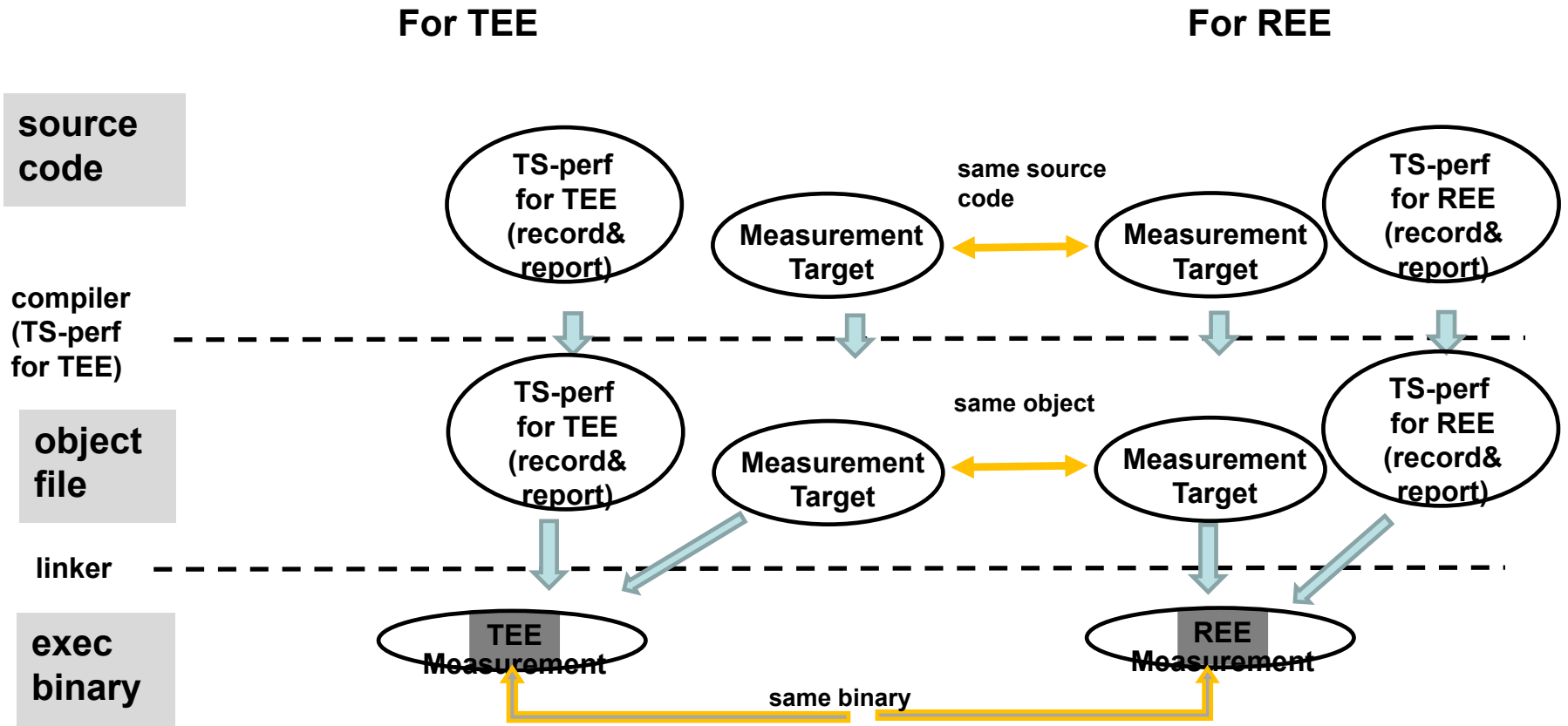
- We developed a portable library of GlobalPlatform's TEE Internal API because the specification is opened and widely used on most TEEs on smartphones (Arm TrustZone).
  - The portable library is developed for RISC-V Keystone and Intel SGX.
  - Using the portable library, we can compare the same software on 3 TEE architectures (RISC-V Keystone, Intel SGX, and Arm TrustZone).

- Library Implementation and Performance Analysis of GlobalPlatform TEE Internal API for Intel SGX and RISC-V Keystone [TrustCom 2020]

# Problem 2: Different binaries between TEE and REE

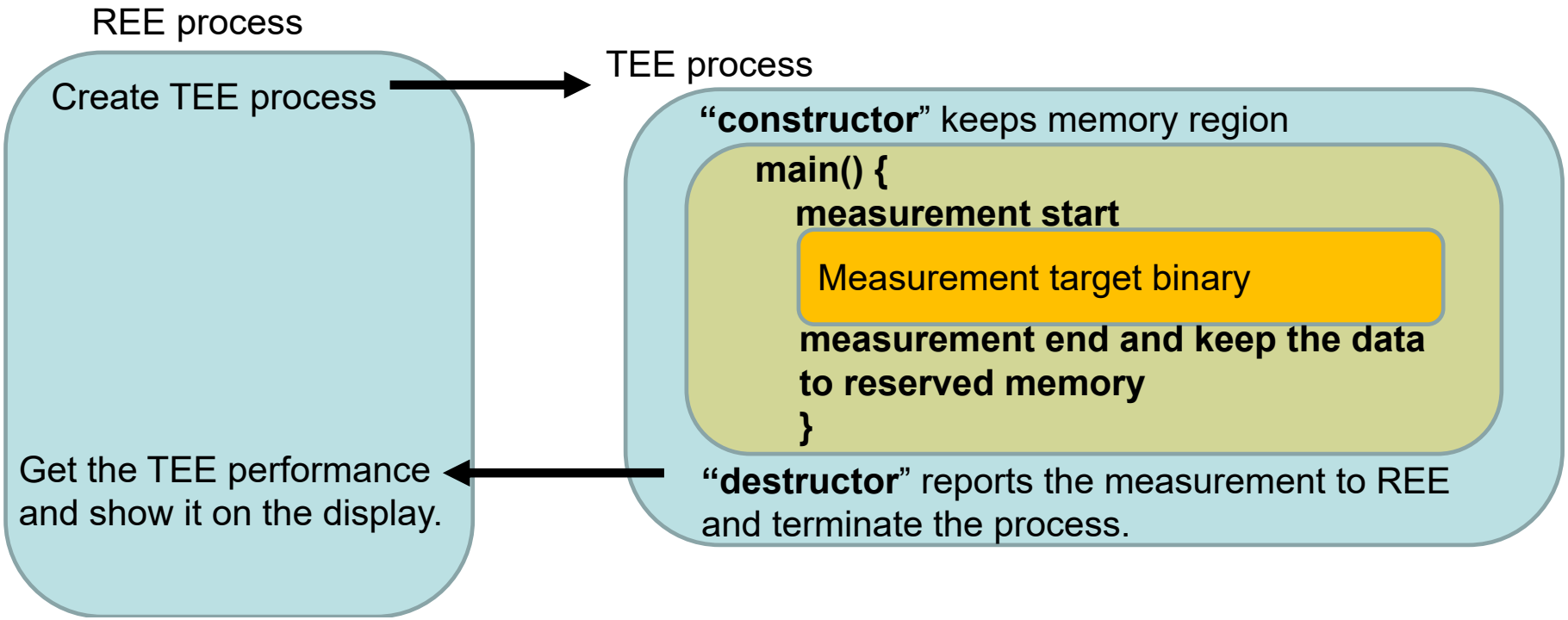


- This problem is solved by "**separate compilation**" to compare the same binary performance between TEE and REE.



# Problem 3: Heavy communication overhead between TEE and REE

- This problem is solved by the performance reporting just before the termination of the process.
- We utilize GCC; "**profile option**", "**constructor**" and "**destructor**".
  - "**constructor**" keeps memory region to log the **measurement of profile option**.
  - "**destructor**" reports the measurement results from TEE to REE at the end of TEE process.



# Performance measuring between different TEEs and REEs



- Three TEE architectures (Arm Trust Zone, Intel SGX, and RISC-V Keystone)

| | CPU | Core | Mem (GB) | REE | TEE |
|---|---|---|---|---|---|
| Raspberry Pi3 B+ [43] | Cortex -A53 | 4 | 1 | Linux 4.14.56 | TrustZone (OP-TEE 3.8.0) |
| Intel NUC 7BJYH [44] | Pentium J5005 | 4 | 8 | Linux 5.3.0 | SGXv2 (SDK v2.8) |
| SiFive Unleashed [45] | U540 | 4 | 8 | Linux 4.15.0 | Keystone v0.3 (Eyrie runtime) |

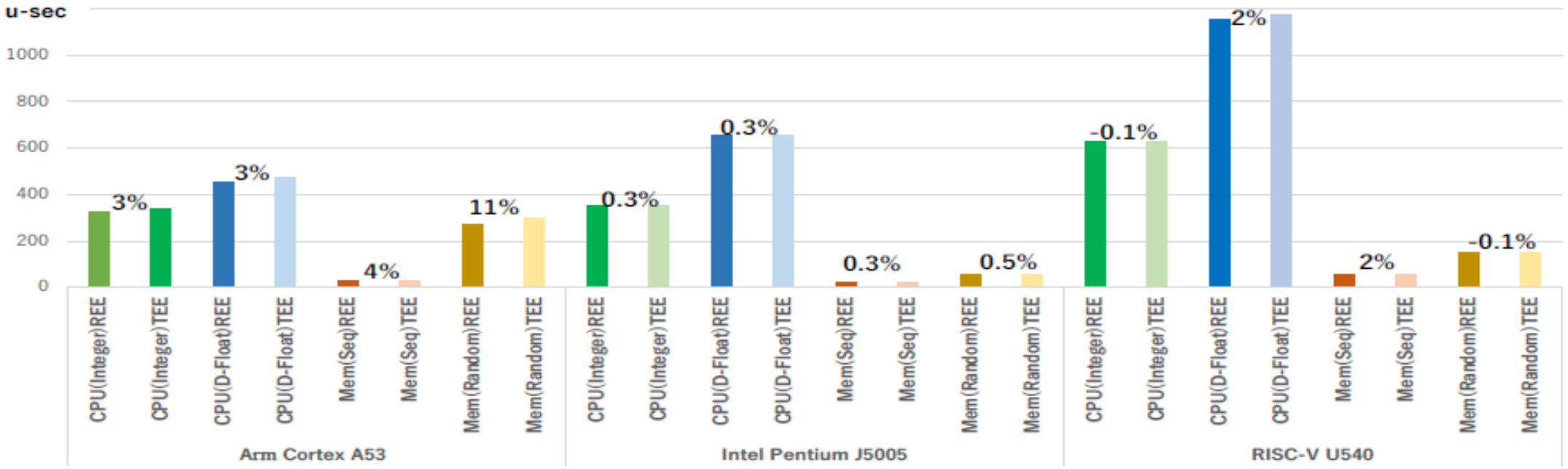
- CPU time counter

| | Counter | Instruction | Frequency (MHz) |
|---|---|---|---|
| Intel x86-64 (Pentium J5005) | TSC | rdtsc | 1,500 |
| Arm Cortex-A (Cortex-A53) | CNTVCT_EL0 | mrs | 19.2 |
| RISC-V RV64 (SiFive U540) | HPM | rdcycle | 1,000 |

# Performance measuring between different TEEs and REEs

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

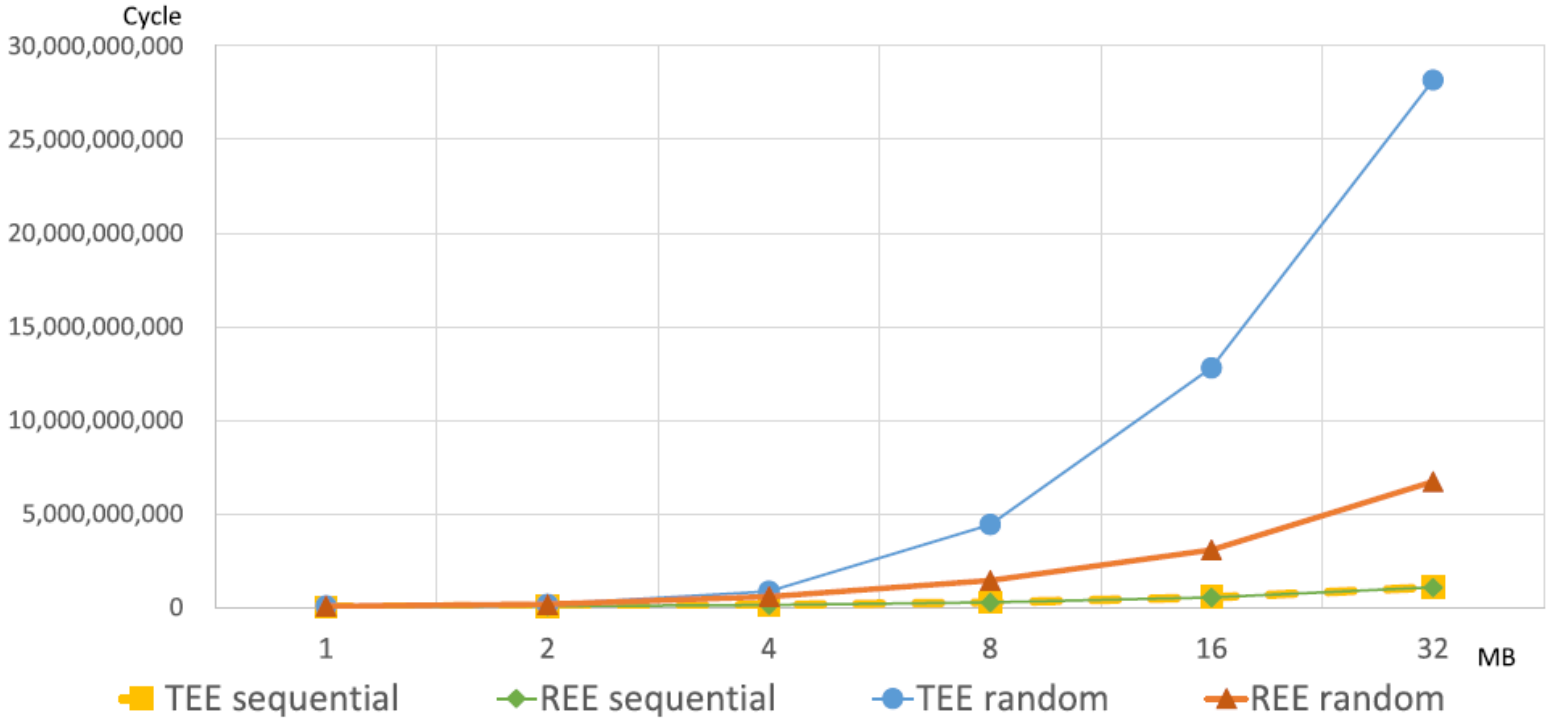
- Performance Comparison between TEE and REE on Arm Cortex-A, Intel X86-64, and RISC-V U540



# Measuring the affect of memory encryption on Intel SGX



- Measuring wide memory sequential access and random access
  - This result shows the performance difference appears over the cache size (4MB L2).



# Conclusions



- Measuring TEE performance had 3 problems.
  1. Different programming style.
  2. Different binary between TEE and REE
  3. Heavy communication overhead between TEE and REE
- How to Solve by TS-Perf
  1. Provide a portable GlobalPlatform API by a library.
  2. Separate Compilation allows to compare the true binary performance between TEE and REE.
  3. GCC customization to report the performance results after process termination
- TS-Pers measures performance between TEE and REE.
  - Measuring true difference of TEE and REE.

This presentation is based on

- TS-Perf: General Performance Measurement of Trusted Execution Environment and Rich Execution Environment on Intel SGX, Arm TrustZone, and RISC-V Keystone [IEEE Access 2021]
- Library Implementation and Performance Analysis of GlobalPlatform TEE Internal API for Intel SGX and RISC-V Keystone [TrustCom 2020]