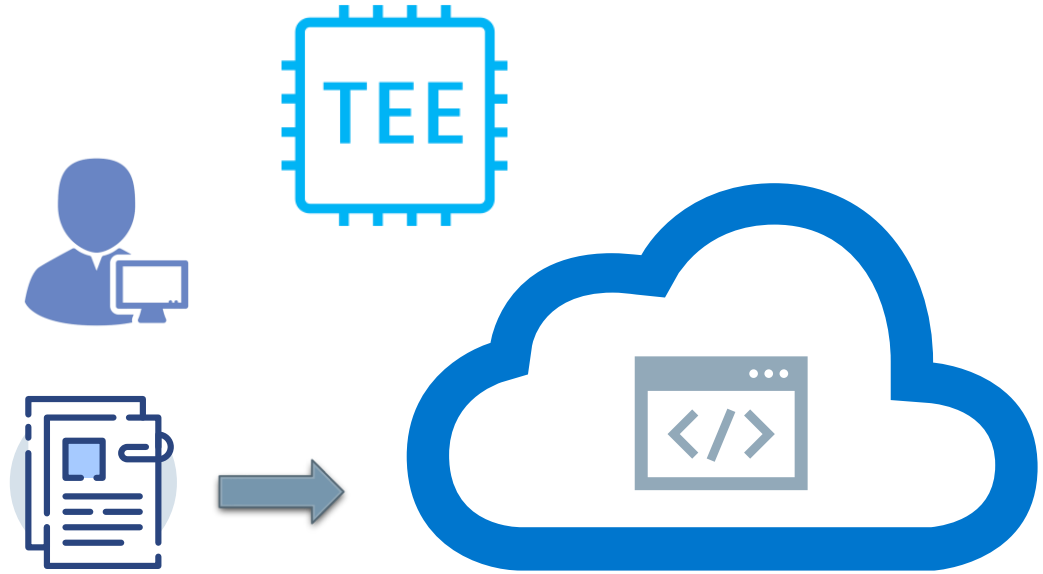
MAGE: Mutual Attestation for a Group of Enclaves without Trusted Third Parties

Guoxing Chen
Shanghai Jiao Tong University

Yinqian Zhang
Southern University of Science and Technology

Trusted execution environment (TEE)



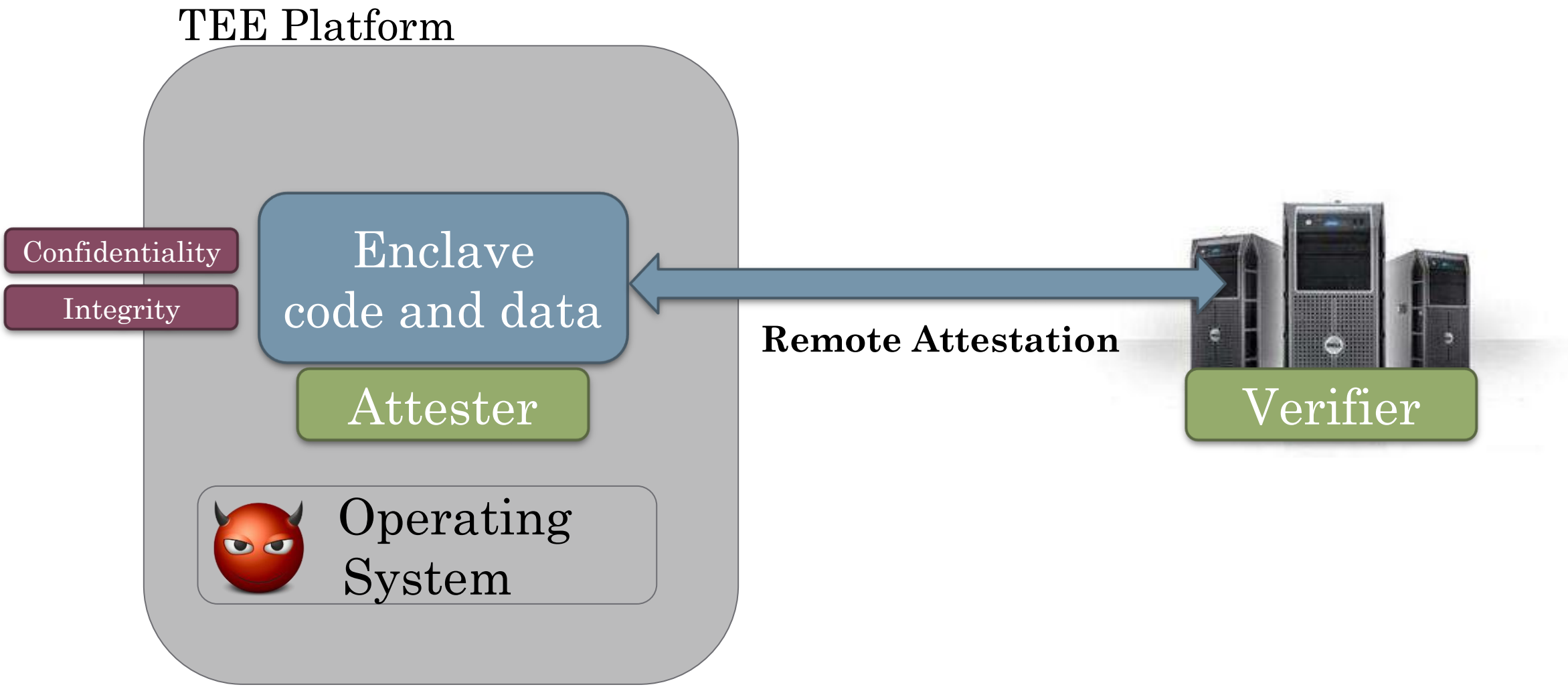
AMD
Secure Encrypted Virtualization

Google Cloud

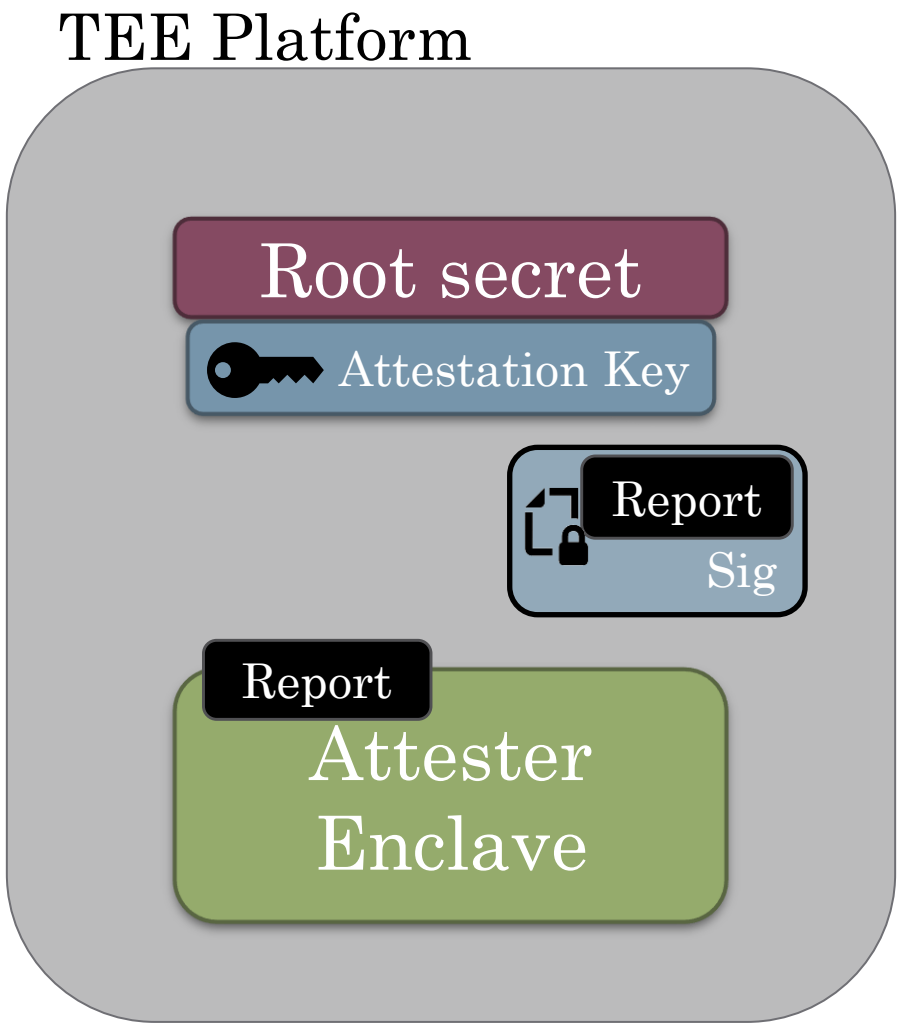
Microsoft Azure

Alibaba Cloud

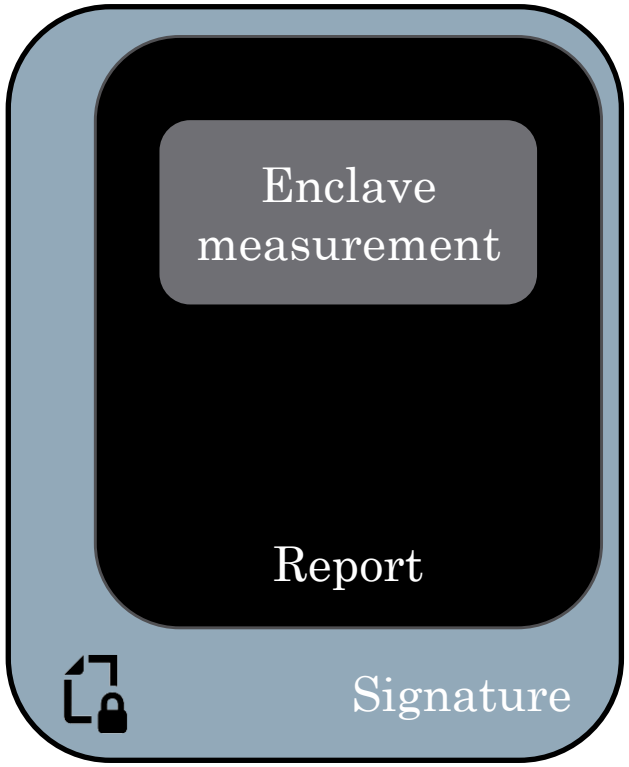
Remote attestation



Q1: Is the attester an enclave?

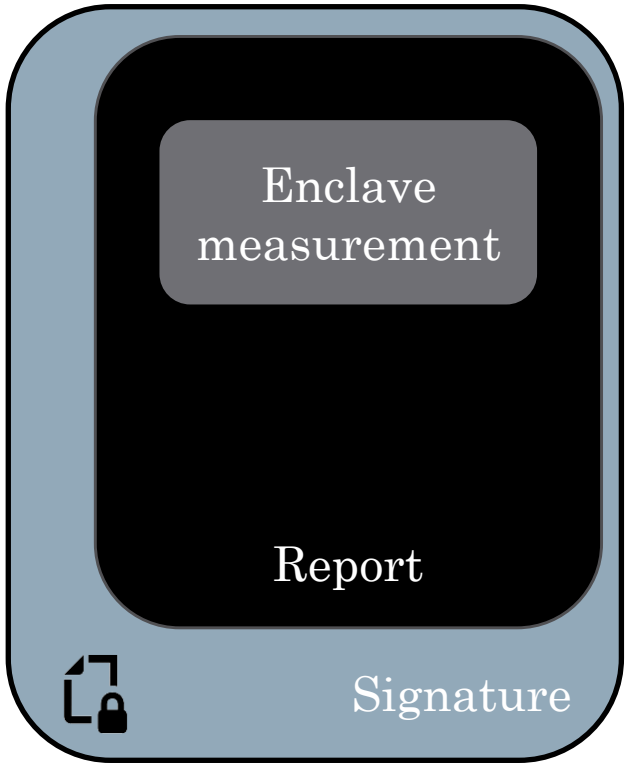


Q2: What is the attester enclave's identity?



Enclave measurement: the cryptographic hash of the initial code and data of an enclave, as the identity of the enclave.

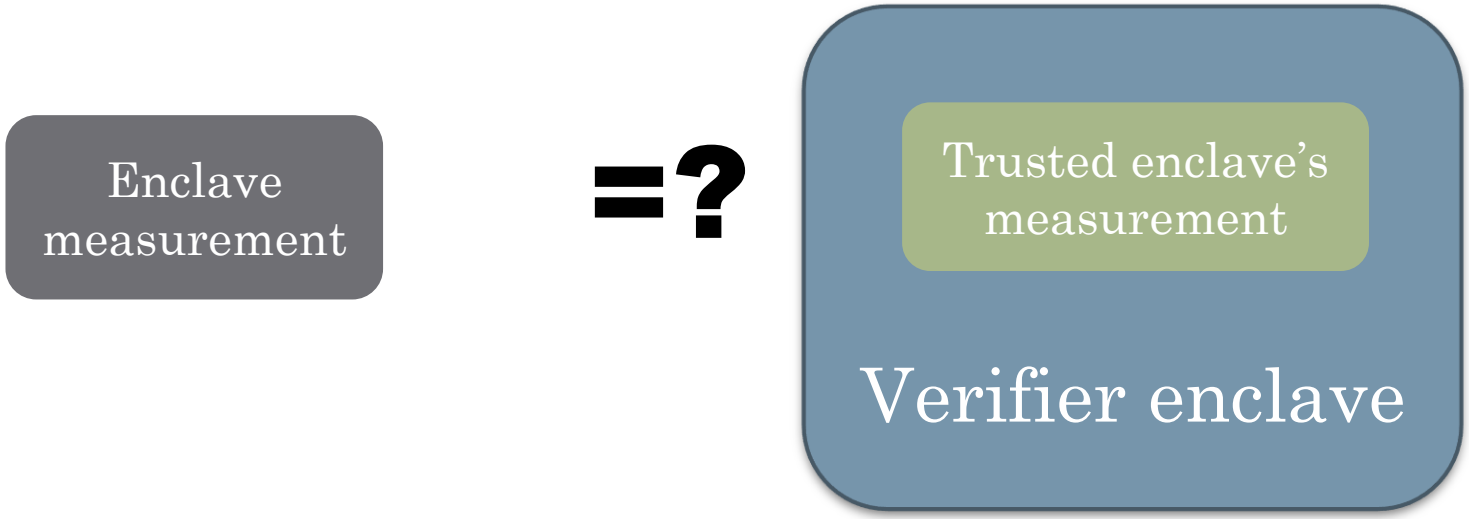
Q3: Is the identity trusted?



=?

Trusted enclave's measurement

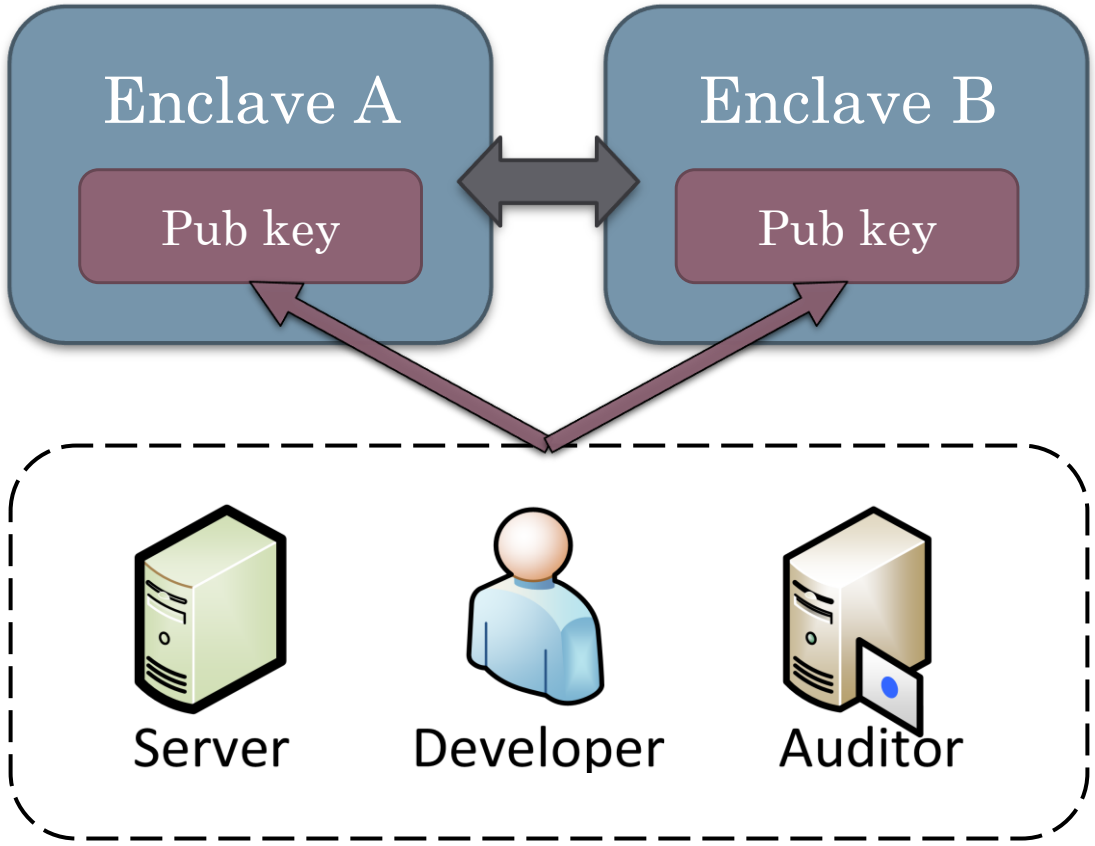
Q3: Is the identity trusted?



Mutual attestation with TTPs

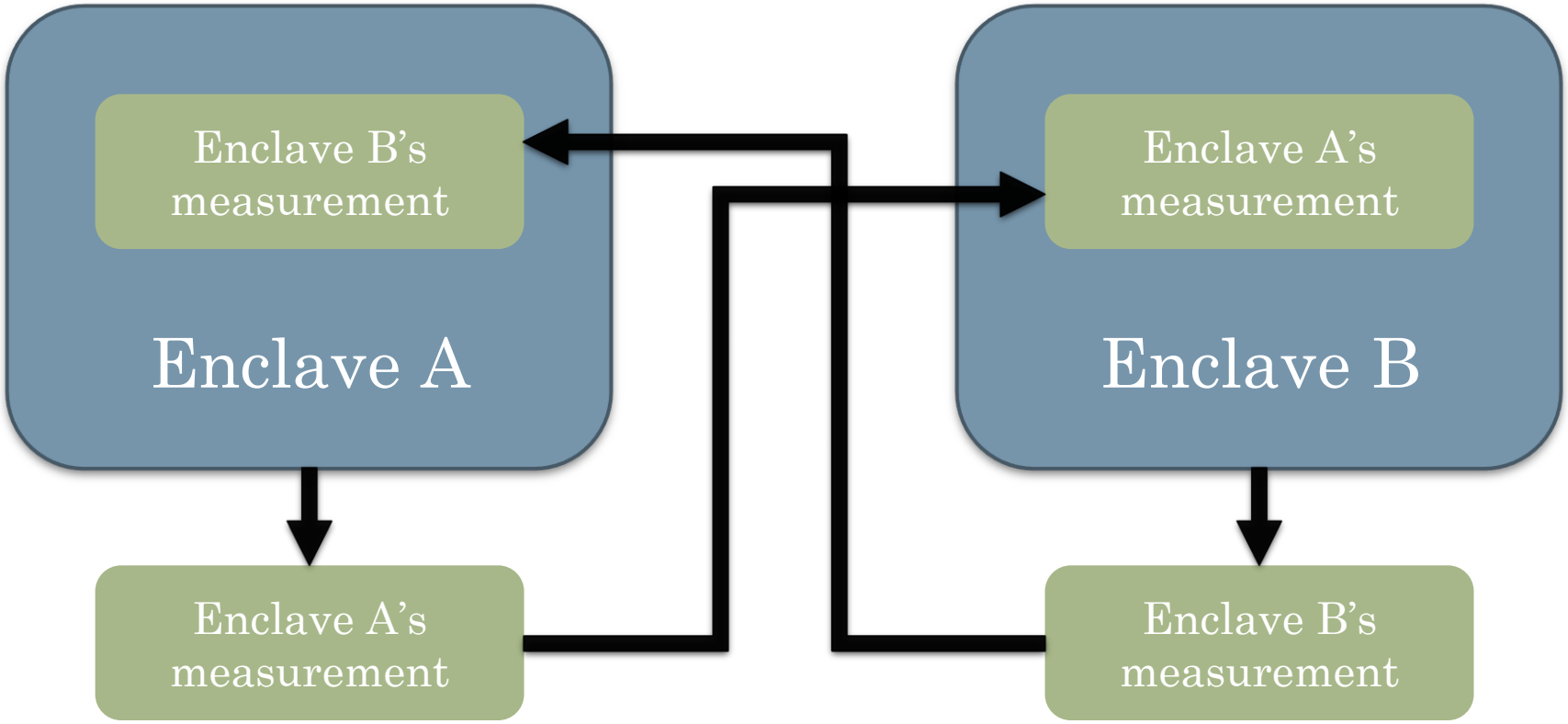
- Trusting multi-enclave applications via **mutual attestation**

- TTPs increase the TCB and might incur extra costs for running PKIs



Trusted third parties (TTPs)

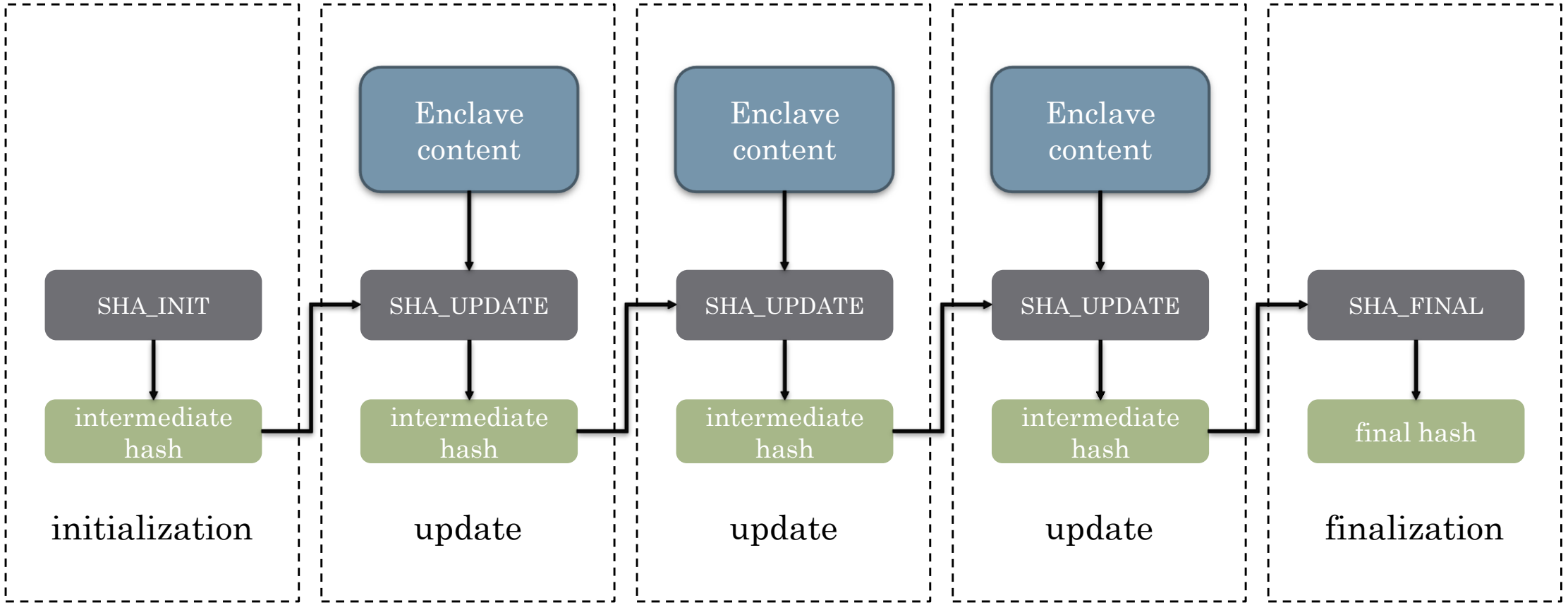
Mutual attestation without TTPs



Circular dependency

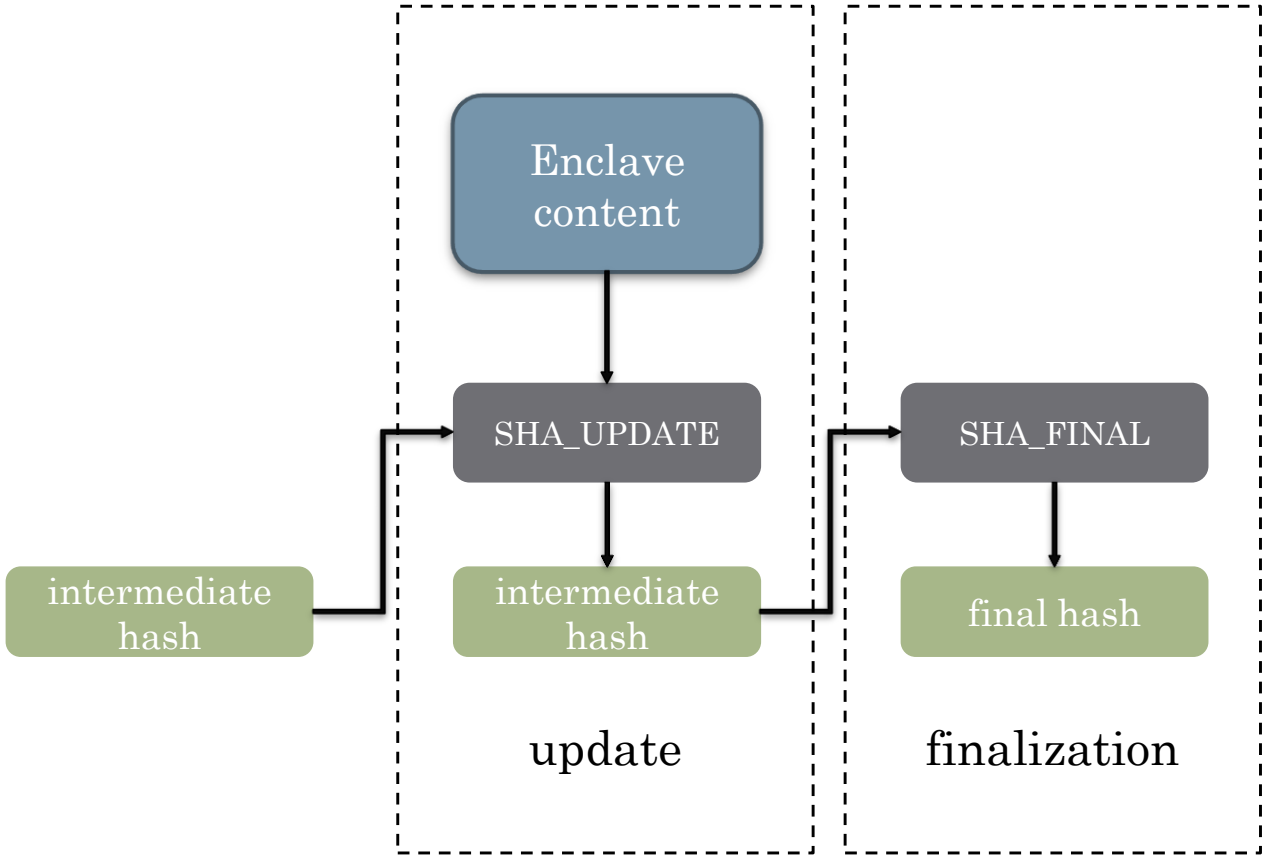
Measurement calculation

The measurement calculation (e.g., SHA-256) is deterministic and sequential



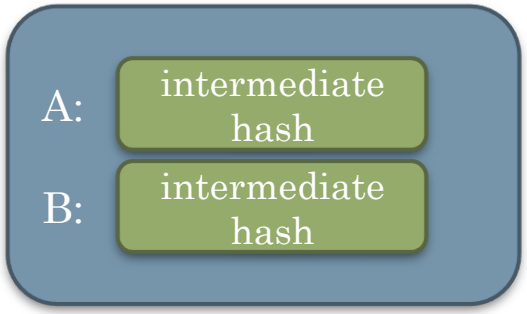
Measurement calculation

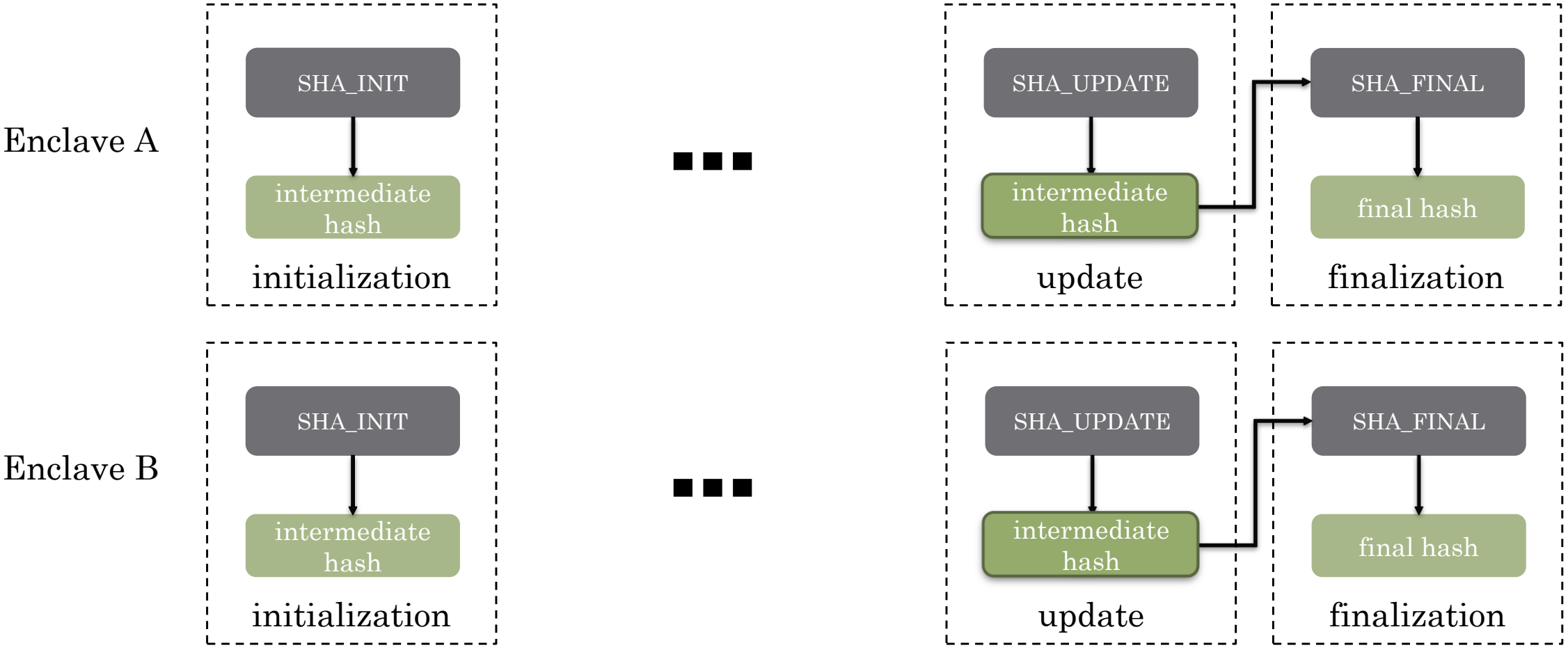
Key observation: knowing the intermediate hash and information to perform subsequent measuring operations would be sufficient to derive the final output



MAGE

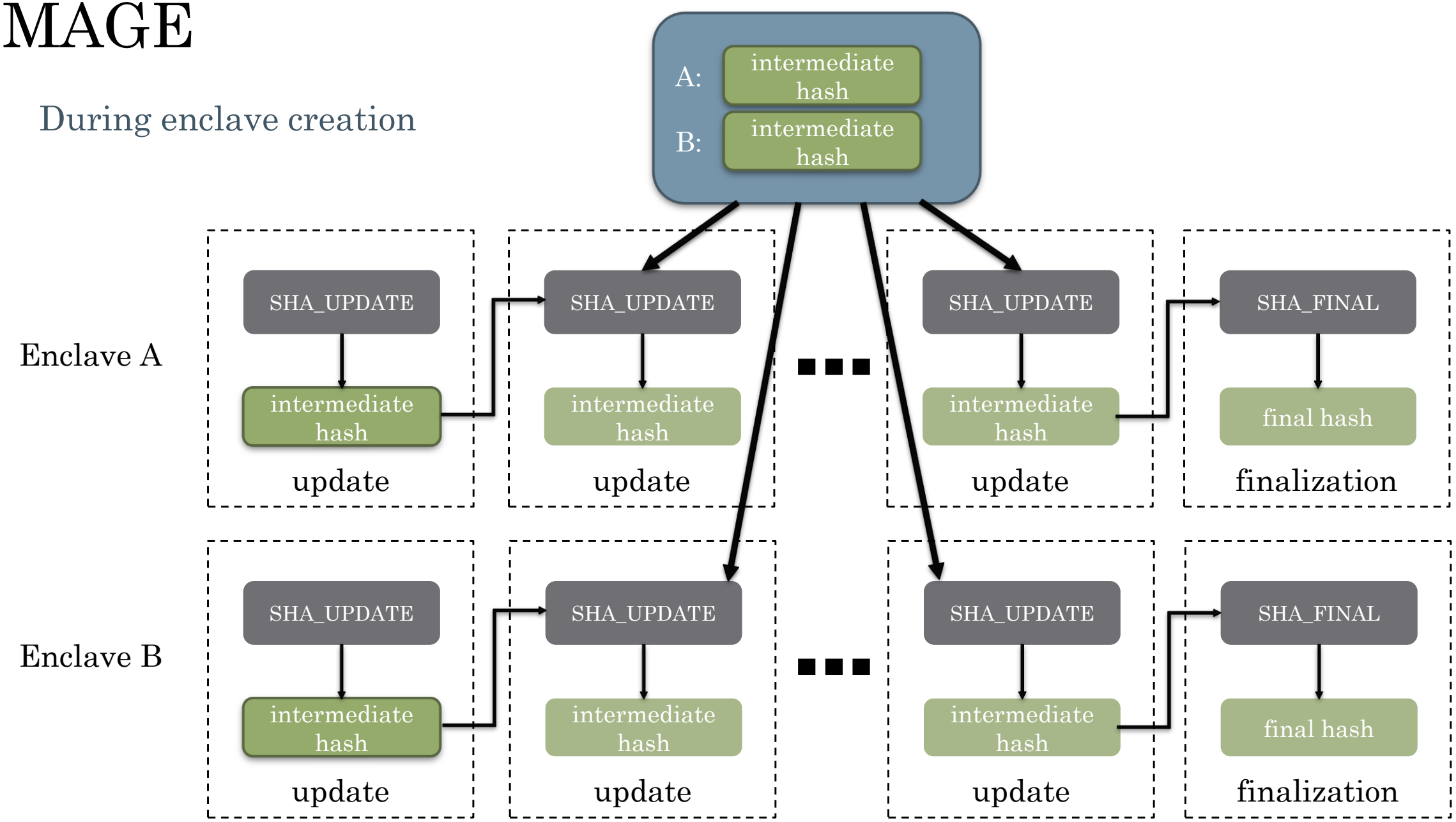
During enclave creation
Introduce an **common part**
at the end of each enclave





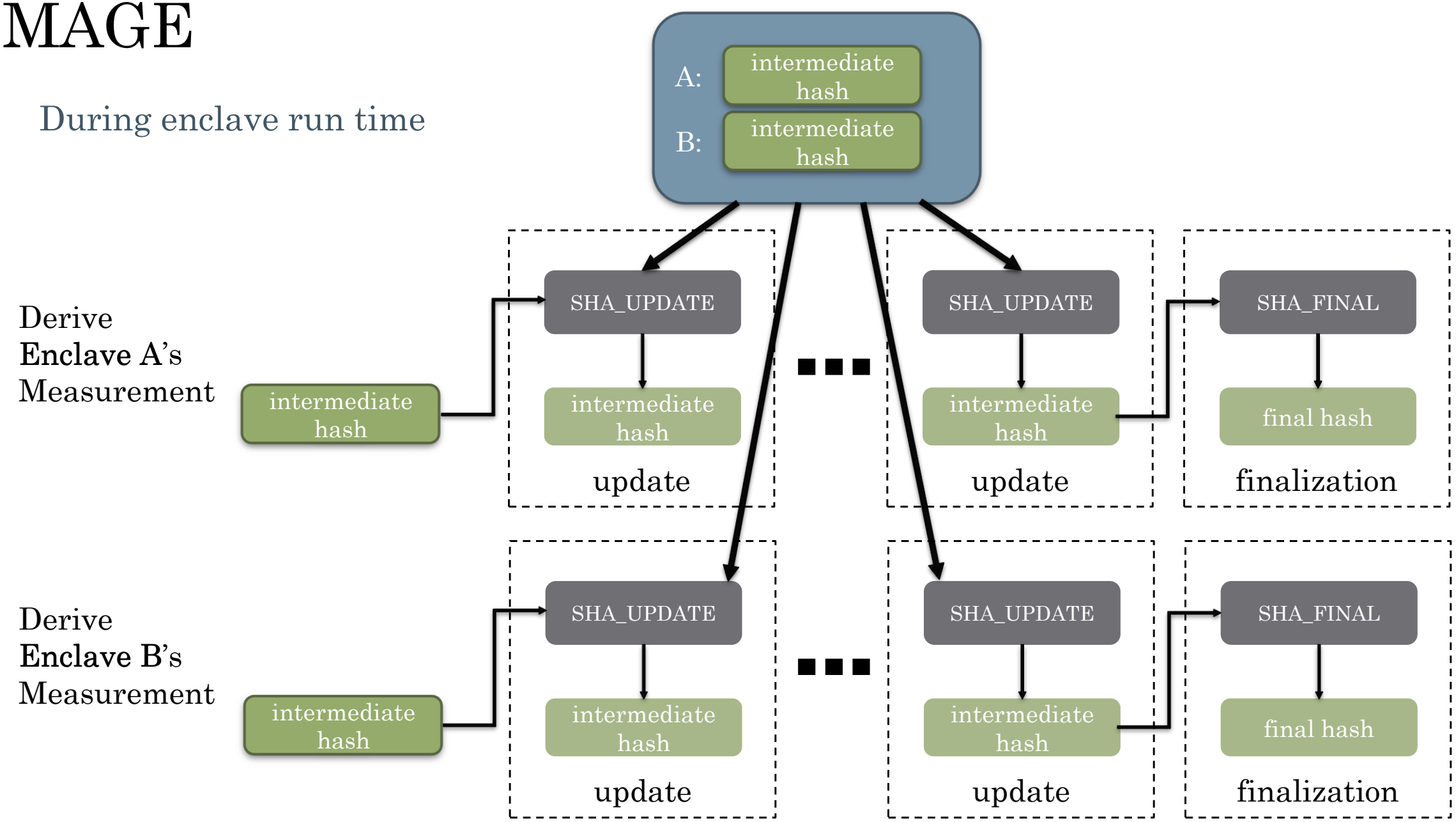
MAGE

During enclave creation



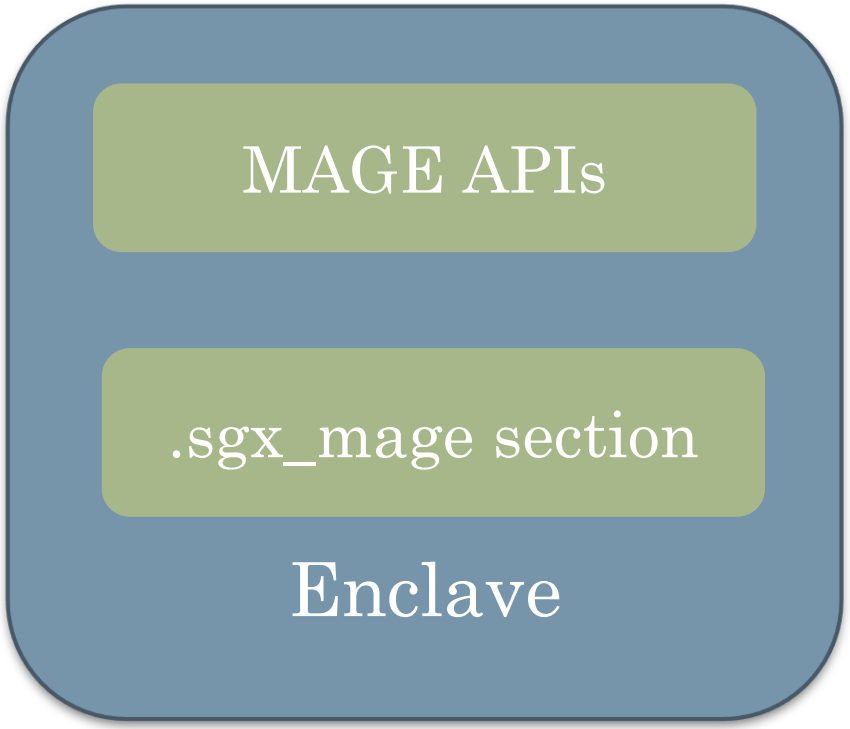
MAGE

During enclave run time



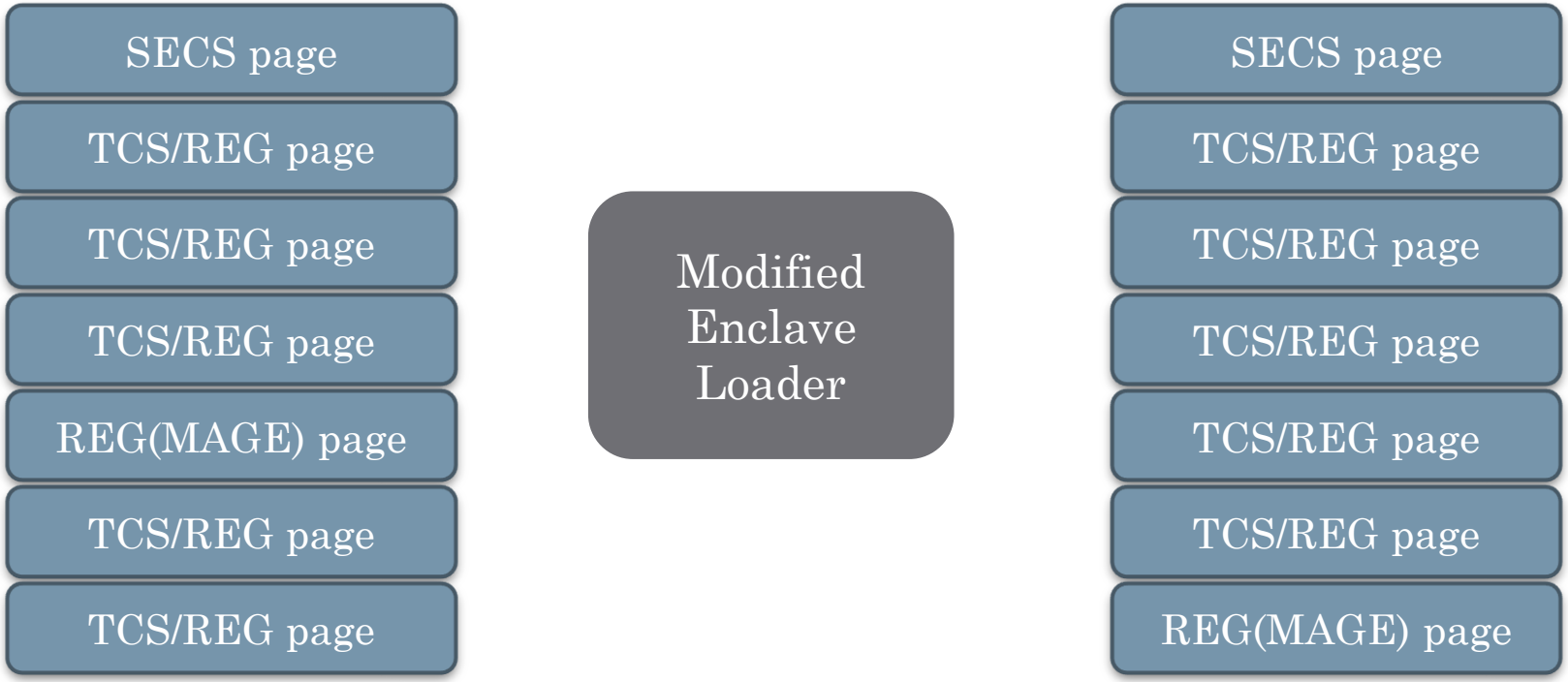
Implementation for Intel SGX

- MAGE library:
  - Reserve a read-only data section, named .sgx_mage
  - Provide APIs for deriving measurements from .sgx_mage



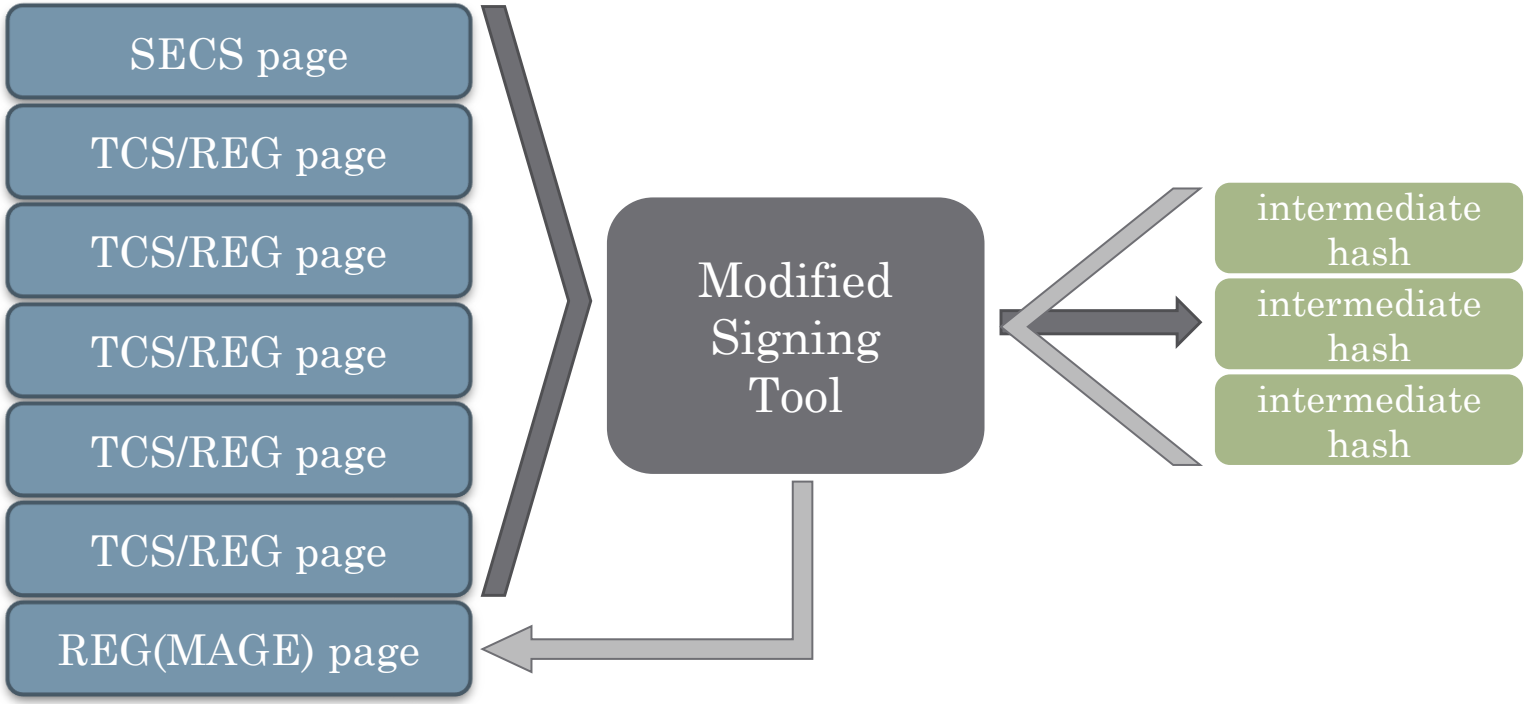
Implementation for Intel SGX

- Modified enclave loader:
  - Load .sgx_mage section after all other enclave code and data



Implementation for Intel SGX

- Modified signing tool:
  - Extract intermediate hashes from enclaves.
  - Insert intermediate hashes into .sgx_mage section



Performance

- Memory overhead
  - Linear with the number of trusted enclaves
  - 48 bytes to store auxiliary information (e.g., intermediate hashes, page metadata) for deriving one enclave measurement
  - One 4KB page could support 85 enclaves

- Measurement derivation efficiency
  - Linear with the size of .sgx_mage section
  - 21.7 microseconds to derive one measurement when .sgx_mage section consists of one page

Discussion

- Alternative designs
  - Extending MAGE with untrusted storage for better scalability.
- Extensions to other TEEs
  - Even between different types of TEEs.
- Supporting enclave updates/private code

Thank You!

GitHub repo https://github.com/donnod/linux-sgx-mage

Guoxing Chen guoxingchen@sjtu.edu.cn
Yinqian Zhang yinqianz@acm.org