DMA: Mutual Attestation Framework for Distributed Enclaves

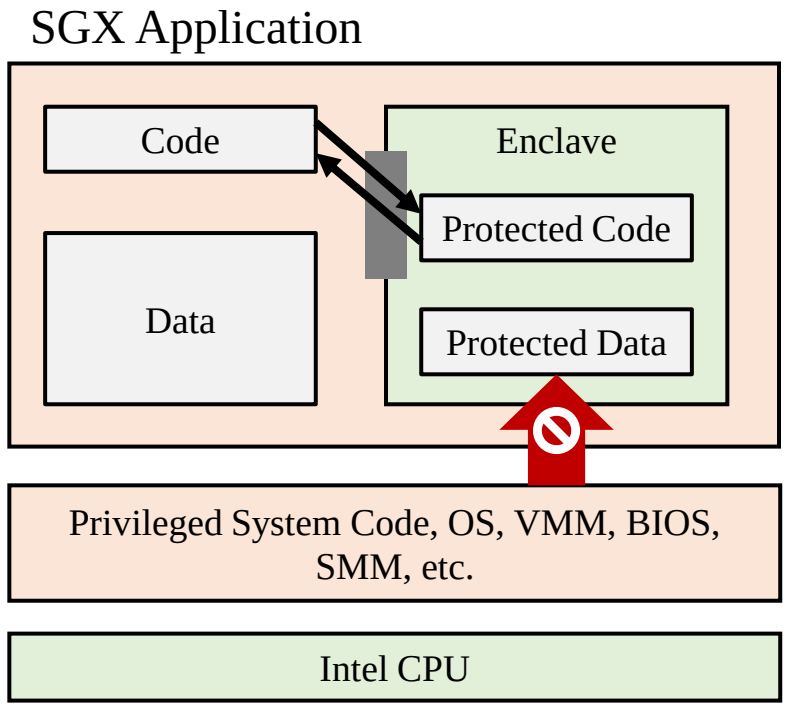
Peixi Li
Nanjing University of Aeronautics and Astronautics

Xiang Li
City University of Hong Kong

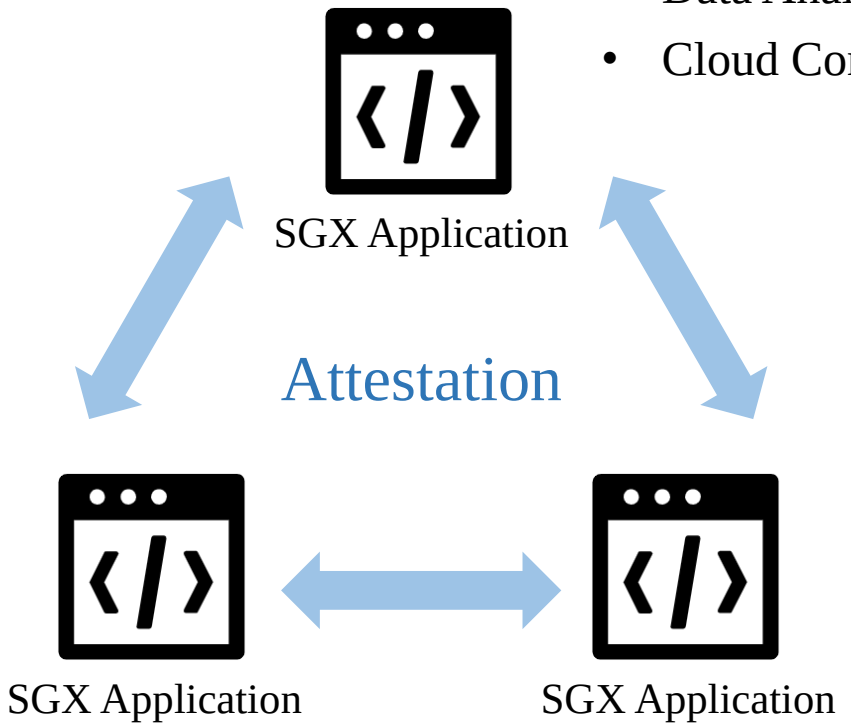
Liming Fang
Nanjing University of Aeronautics and Astronautics

Intel SGX

- Confidentiality
- Integrity



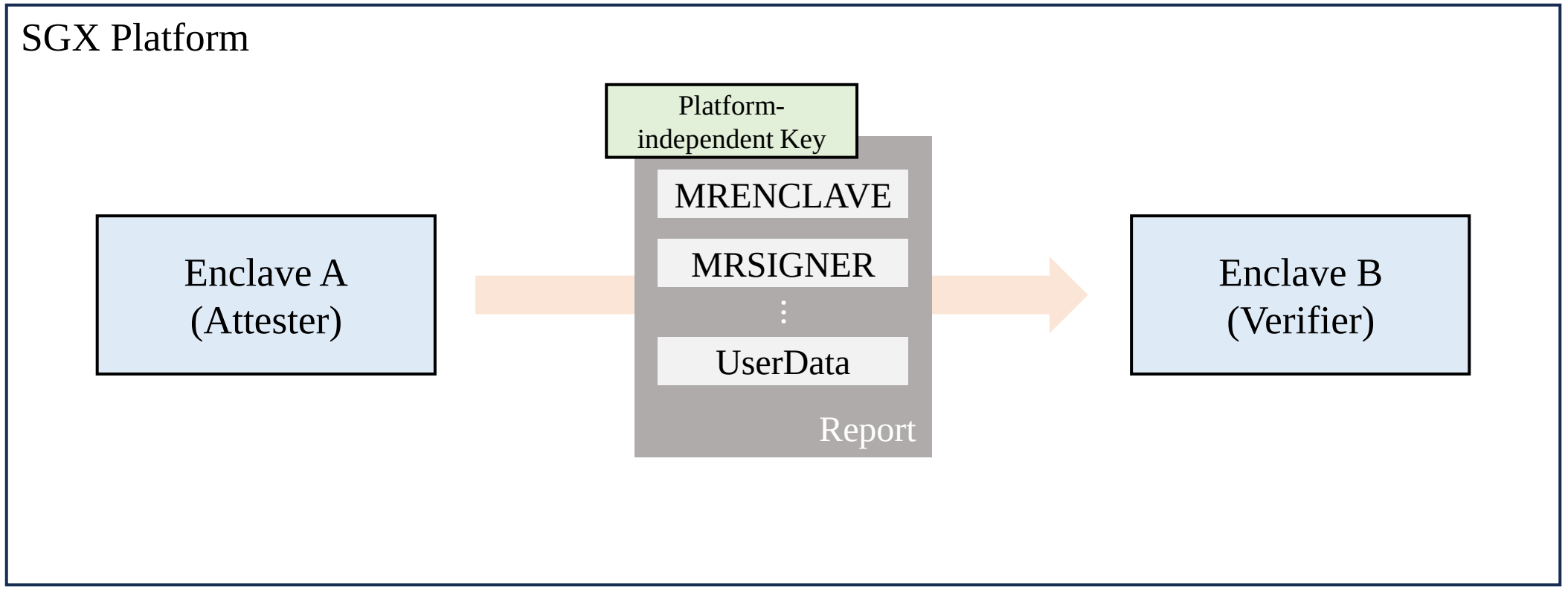
- Machine Learning
- Data Analytics
- Cloud Computing



- MRENCLAVE - Initial code and data
- MRSIGNER - Enclave's authorship

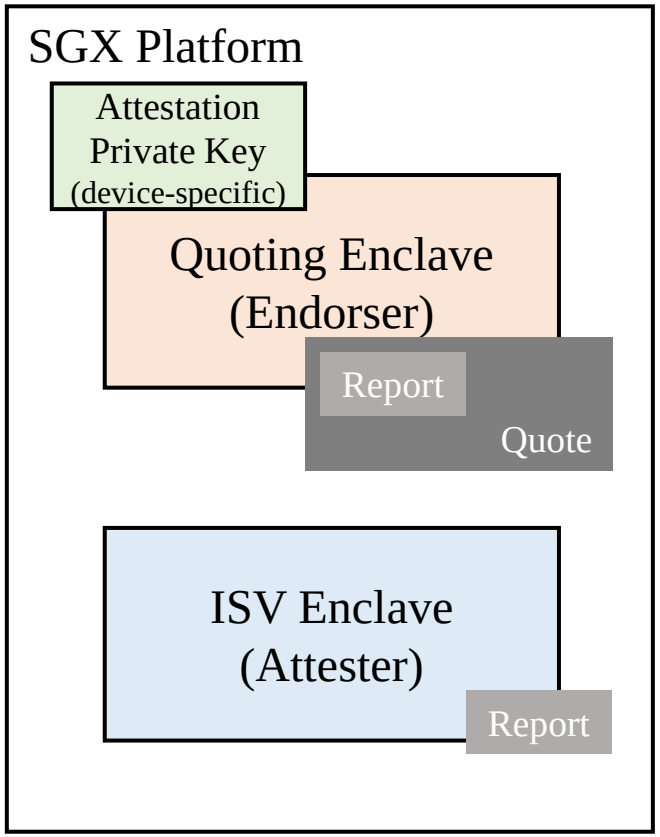
Attestation

- Local Attestation (LA)

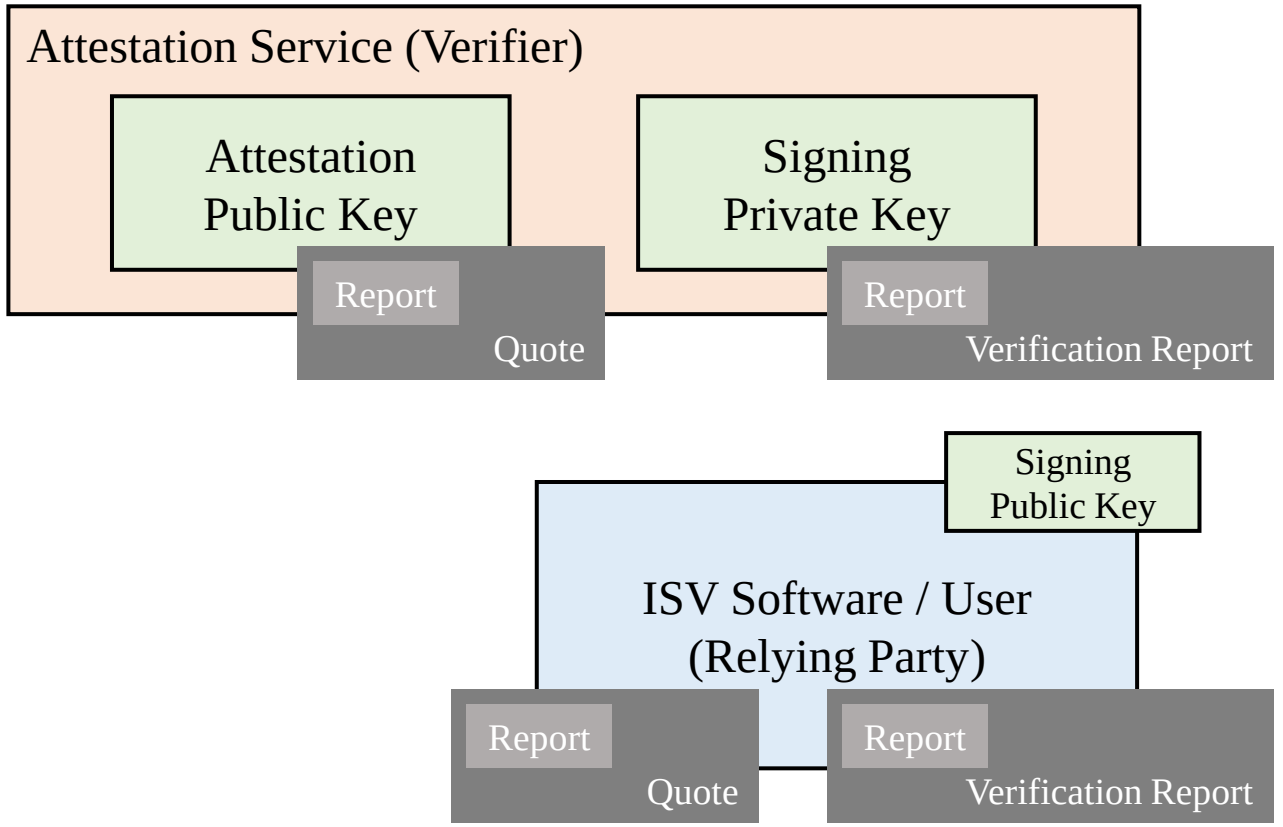


Attestation

- Remote Attestation (RA)

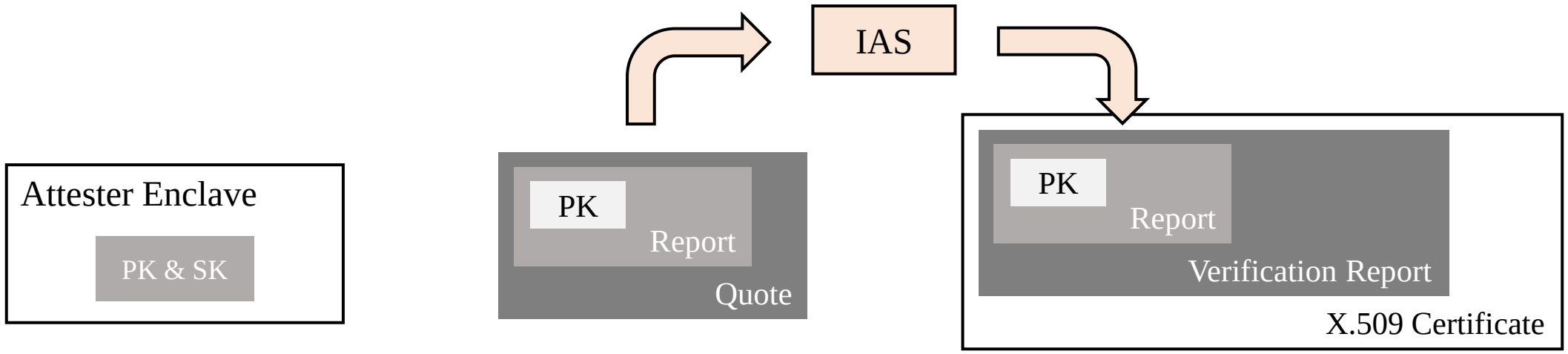


- Intel Enhanced Privacy ID (Intel EPID)
- Intel Data Center Attestation Primitives (Intel DCAP)



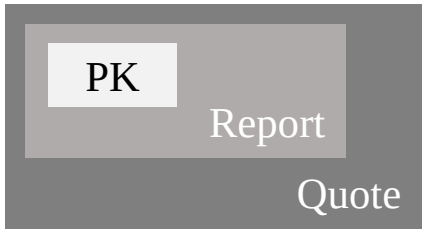
Attestation with TLS handshake

- RA-TLS integrate RA with TLS handshake to prevent MITM attacks
  - Generate a key pair at enclave startup
  - Bind the public key to report
  - Embed the verification report to the channel's certificate
- Results an attested secure channel



Issues

- Lack of evidence freshness
  - The quote is bound to enclave, but not the channel
  - Possible relay and replay of the quote



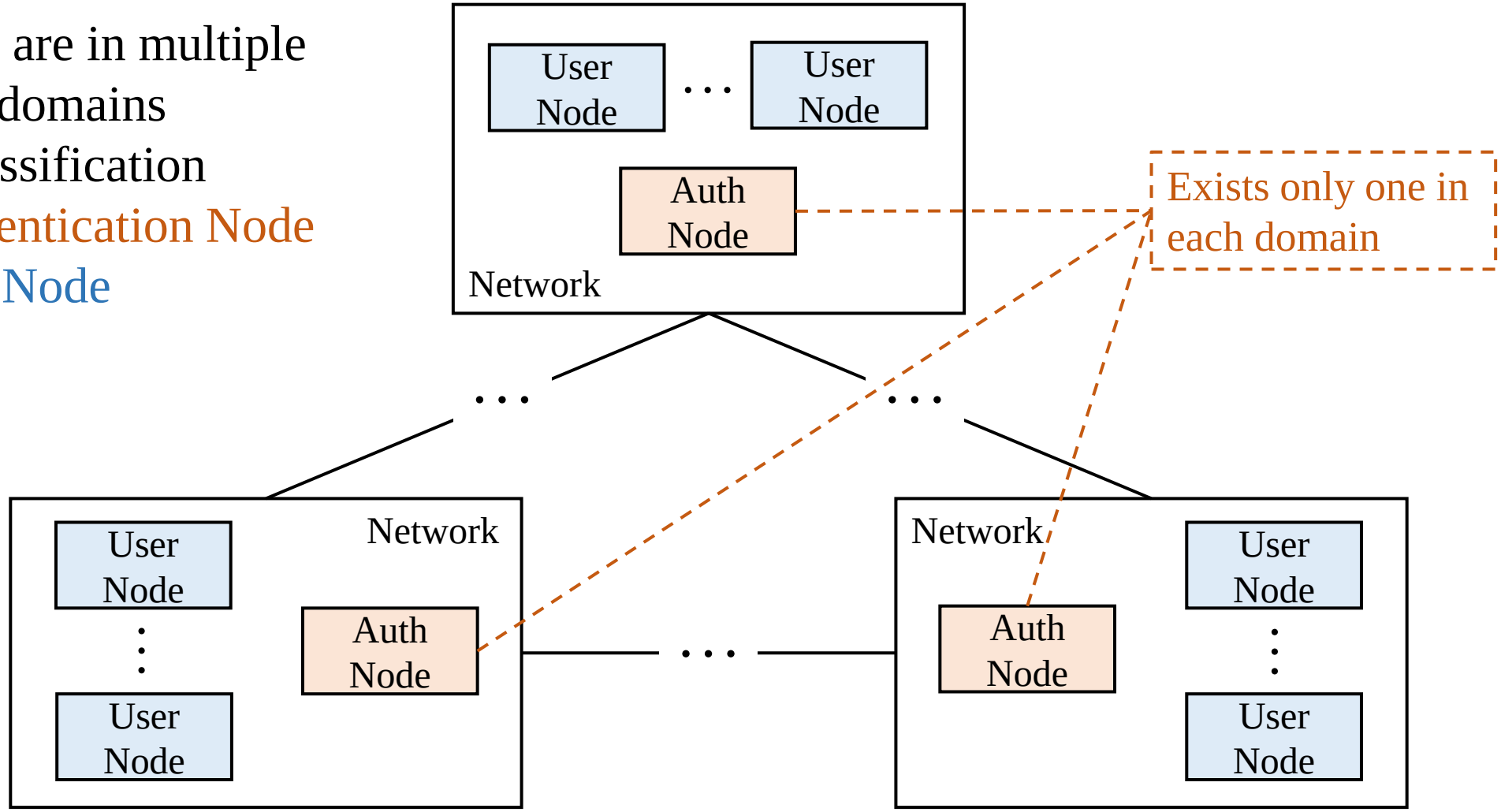
DMA

A Decentralized Mutual Attestation Framework

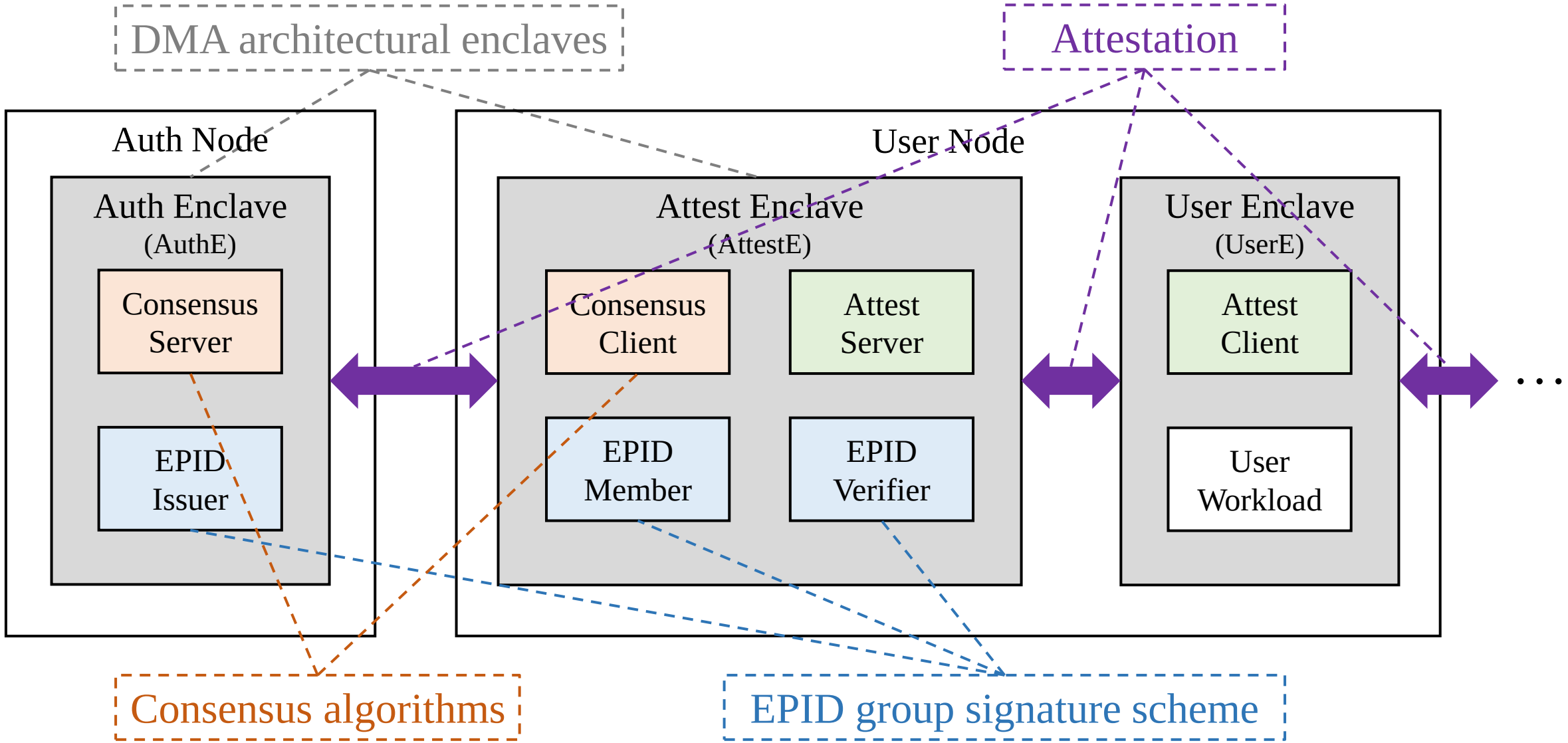
- Lack of scalability and efficiency
  - Managing trust becomes more complex
  - Unique attestation service may cause performance issues

Architecture

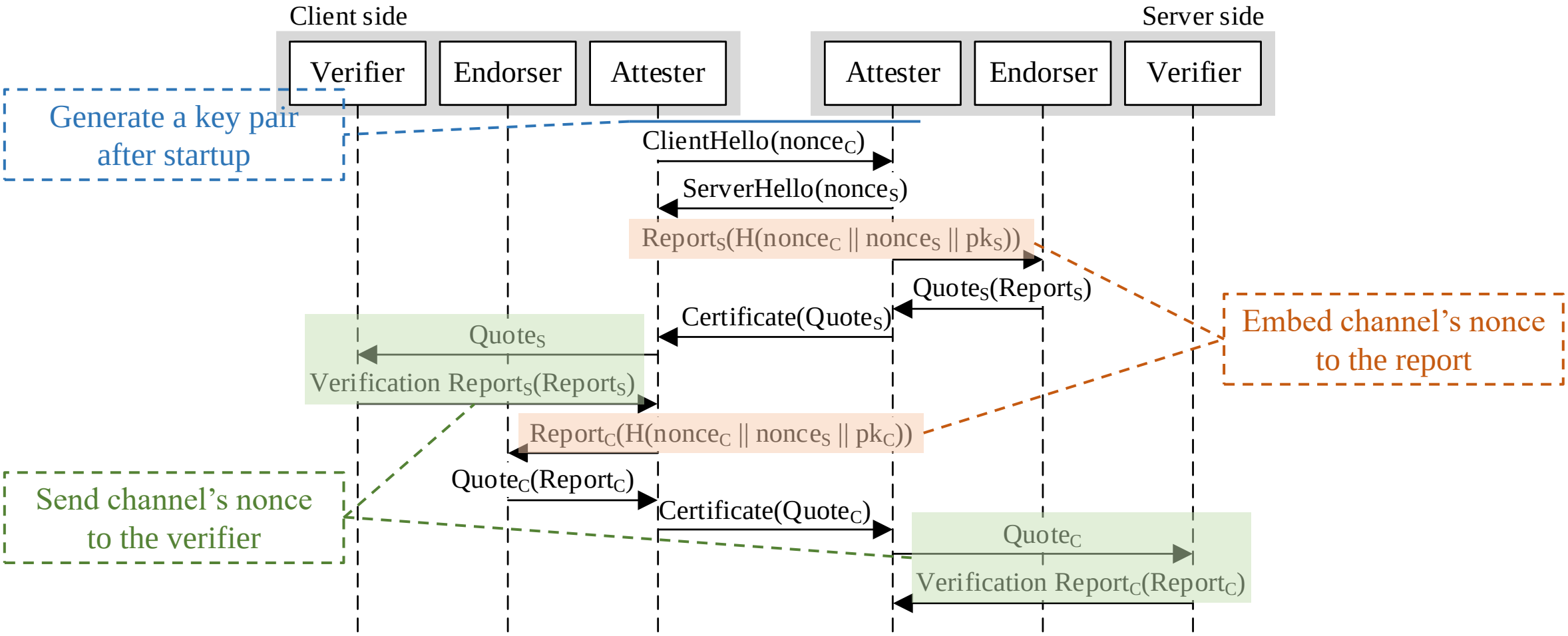
- Enclaves are in multiple network domains
- Node classification
  - Authentication Node
  - User Node



Architecture



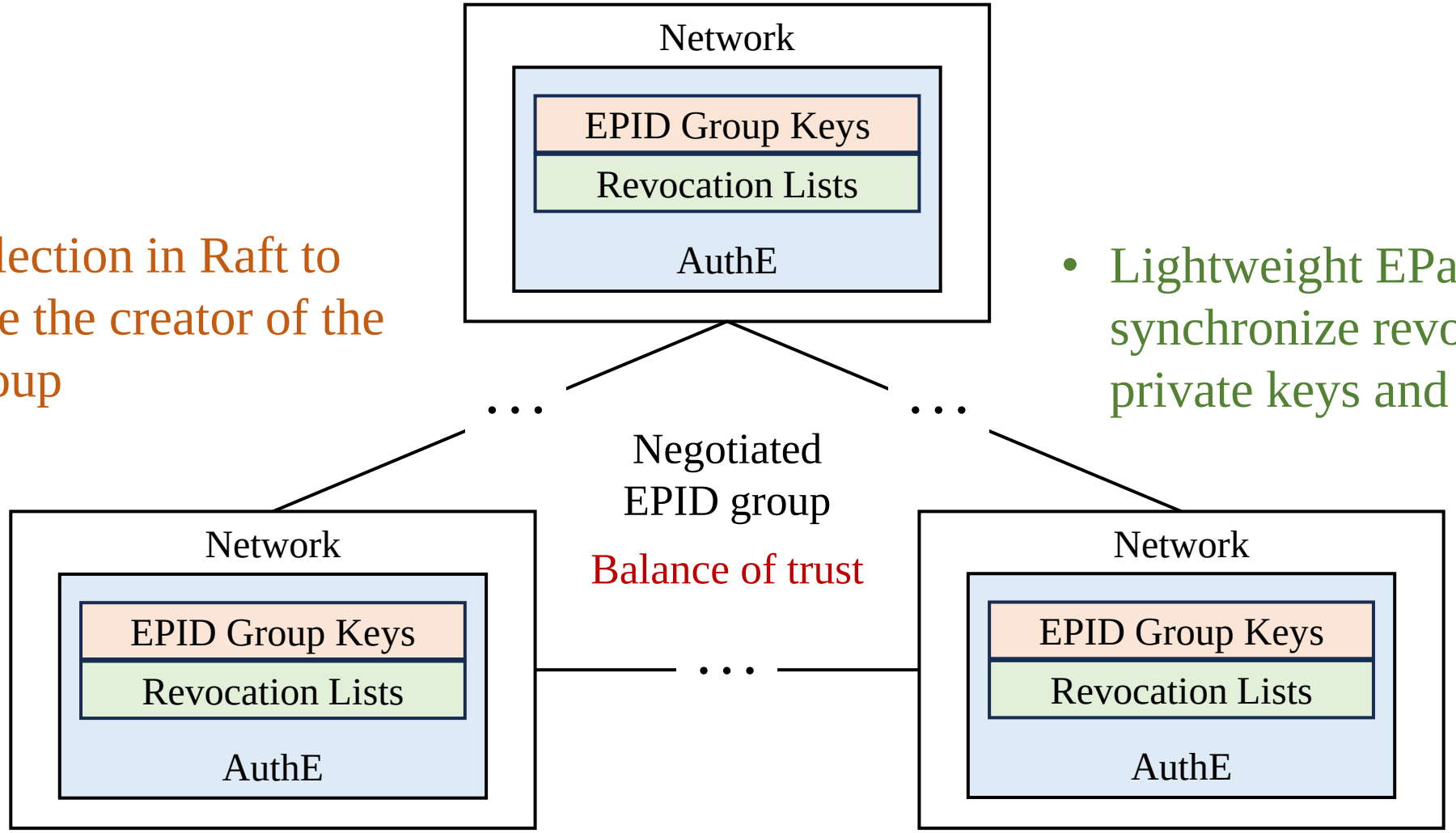
Establish trust between enclaves



In the original SGX attestation, the Endorser is QE, and the Verifier is IAS
In DMA attestation, the Endorser and the Verifier are both AttestEs

Transferring distributed trust

- Leader election in Raft to determine the creator of the EPID group



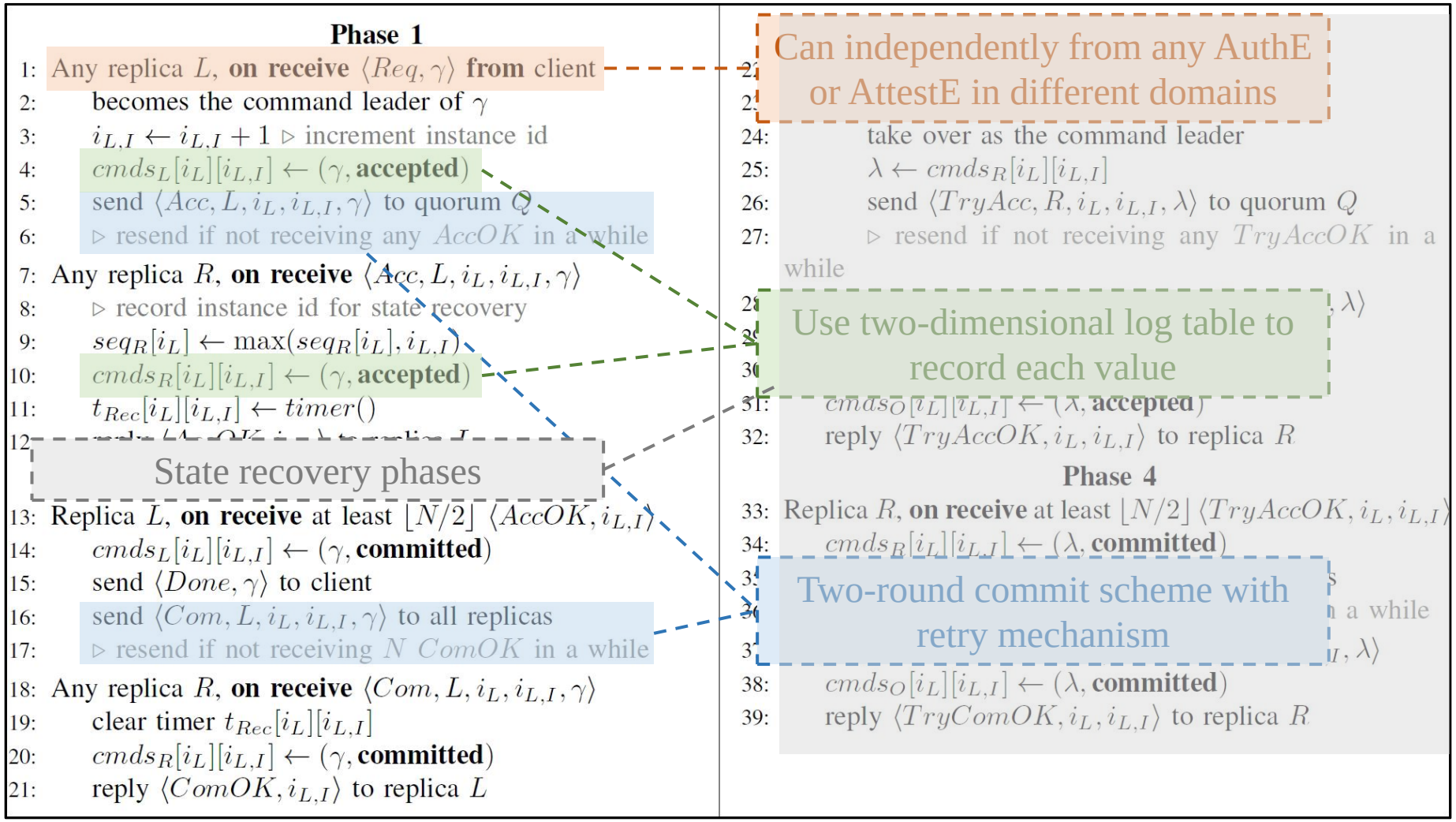
- Lightweight EPaxos to synchronize revoked private keys and signatures

Revocation mechanism

- When a UserE is disconnected
  - The quote used in attestation need to be marked as invalid
  - Prevent quote reuse
  - The UserE counterpart at the opposite end propose a revocation request
  - Signatures of the revoked quotes are stored in SigRL (Distinguished from EPID SigRL)

- When an AttestE is compromised
  - Its EPID member key need to be revoked
  - Can no longer participate in attestation
  - The AuthE within its domain internally initiate a revocation request
  - Revoked EPID member keys are stored in PrivRL

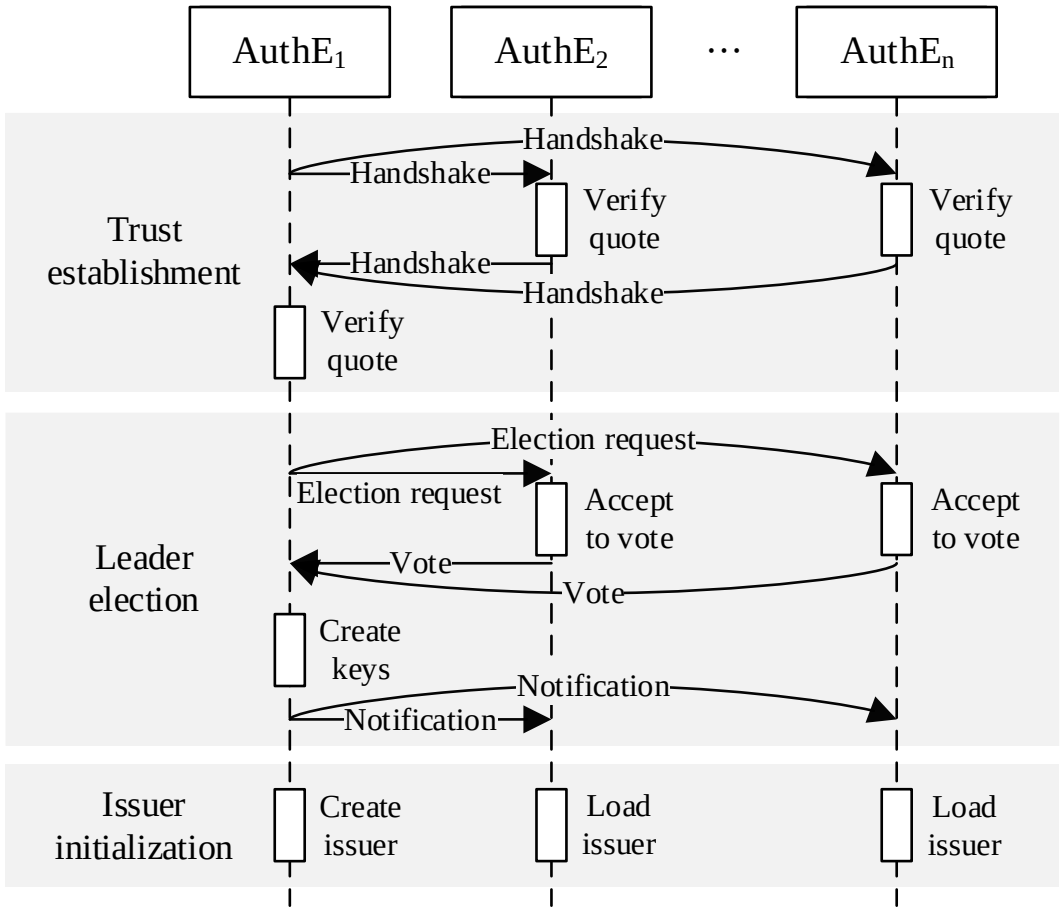
Revocation mechanism



Lightweight EPaxos for synchronizing revoked private keys and signatures

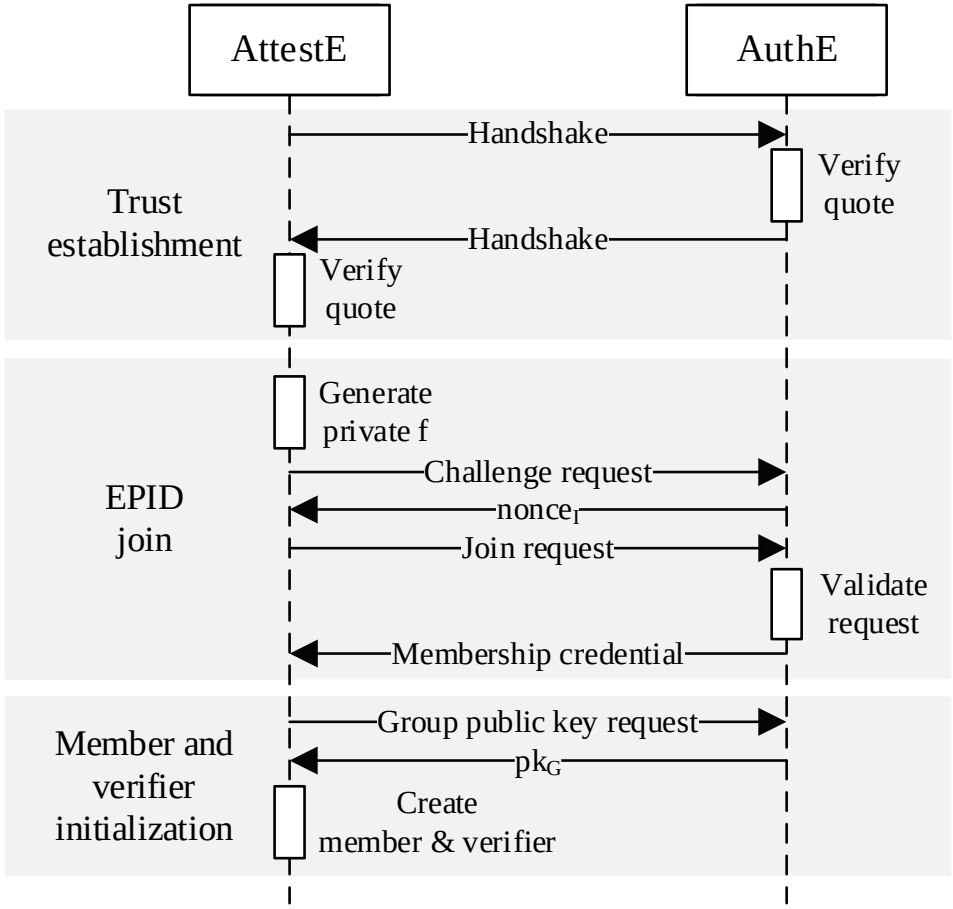
Workflow

- **Preparation phase**
  - Launch AuthE
  - Establish mutual trust among all AuthEs
  - Determine the creator of the unified EPID group
  - Initialize EPID issuer, SigRL and PrivRL



Workflow

- **Provisioning phase**
  - Launch AttestE
  - Establish mutual trust between AttestE and AuthE
  - AttestE run EPID join protocol with AuthE to become a group member
  - AttestE initializes EPID member and EPID verifier



Workflow

- **Attestation phase**
  - Launch UserE
  - Procedure local attestation between UserE and AttestE
  - UserE requests quote signed by AttestE
  - UserE exchanges quote with its peers through TLS handshake
  - UserE verifies the peers’s quote from the AttestE
  - Check enclave attributes and make a trust decision

Security

- **Evidence Freshness and Channel Binding**
  - Channel’s nonce is included in quote and bound to the quote verification process
  - Revocation mechanism ensures that quotes are not reused
- **Security of Data Transmission**
  - Enclave key pair generated at startup and regenerated upon restart
  - TLS channel
- **Security of Trust Transferring**
  - Unforgeability of AuthE’s identity
  - State recovery ensures the state can be restored to crashed nodes
- **Hardware Platform Freshness**
  - Hardware state is cached and embedded in DMA quote to reveal TCB evaluations
- **Privacy**
  - Anonymity guarantees of the EPID group signature algorithm

Evaluation

Latency of some basic operations

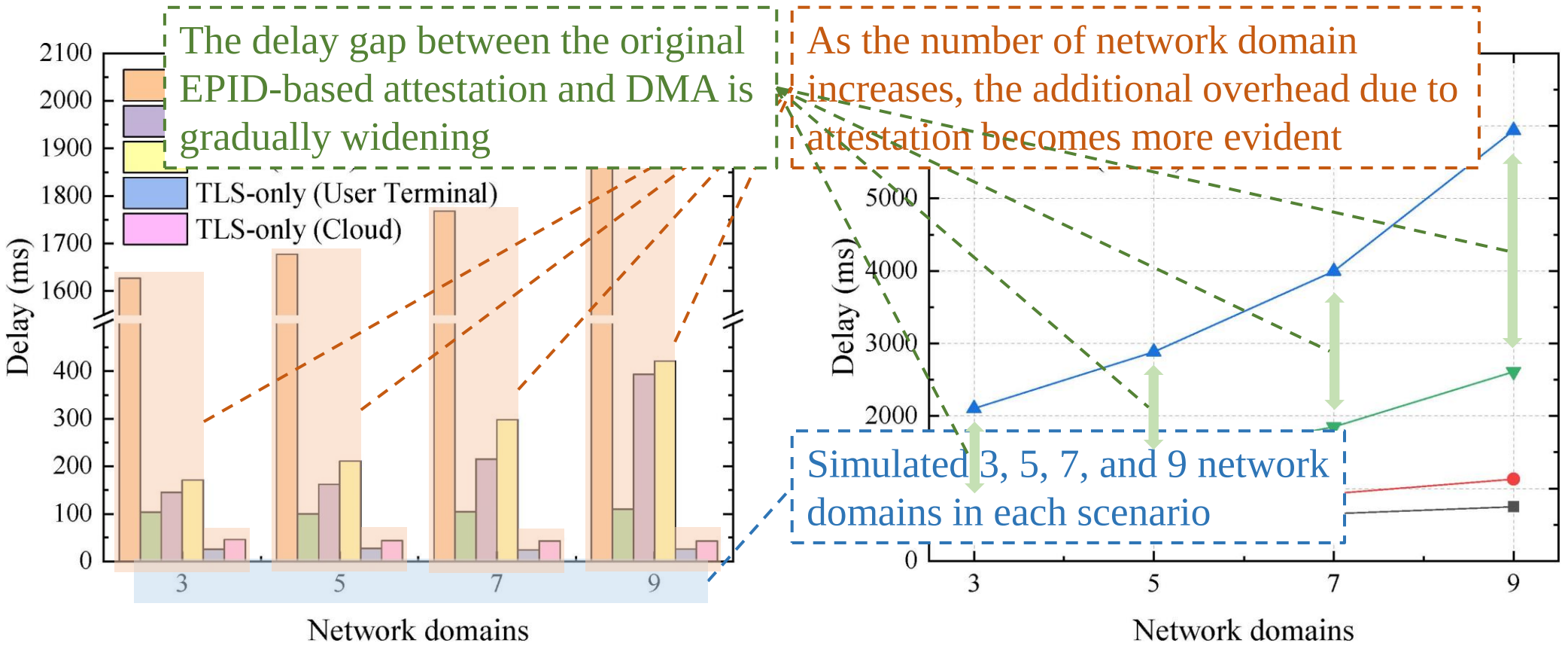
Operation		
EPID	EpidSign	0.005
	EpidVerify	
SigRL	Insert	
	Lookup	

- DCAP-based attestation has smaller computational volume
- More suitable for on-premises network and may raise privacy concerns

Latency of quote generation and verification

Operation	Latency (ms)		
	EPID	DCAP	DMA
Quote generation	298.50	5.66	85.37
Quote verification	1262.01	34.24	47.61

Evaluation



Delay of each individual handshake

Overall delay of all handshakes

Delay of trust establishment through handshakes in user terminal and cloud scenarios

Thank You!

GitHub Repo https://github.com/Seix61/DMA

Email peixi.li@nuaa.edu.cn