Speedster: An Efficient Multi-party State Channel via Enclaves

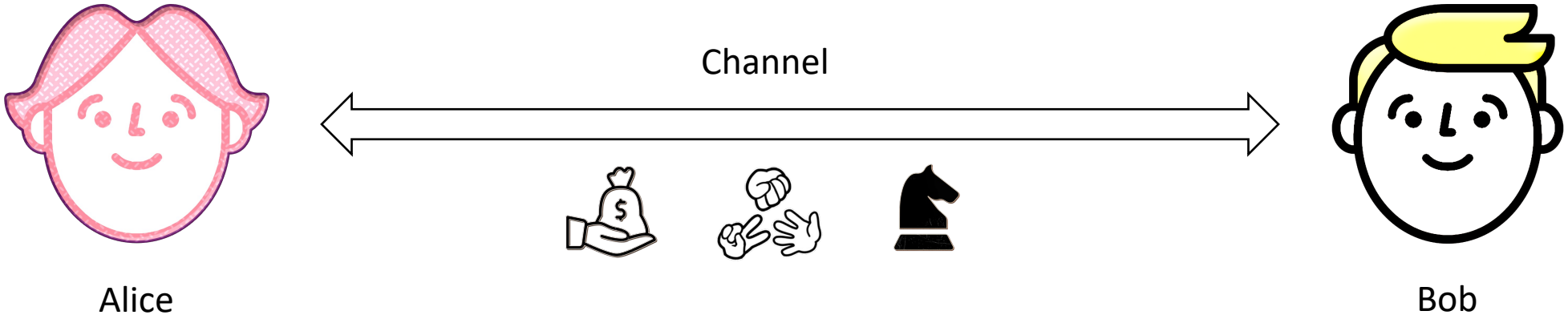
AsiaCCS 2022

Jinghui Liao, Fengwei Zhang, Wenhai Sun, Weisong Shi

Outline

- **Introduction and Background**
- Architecture of Speedster
- Design and Implementation
- Evaluation
- Conclusion

Why Need Payment/State Channel

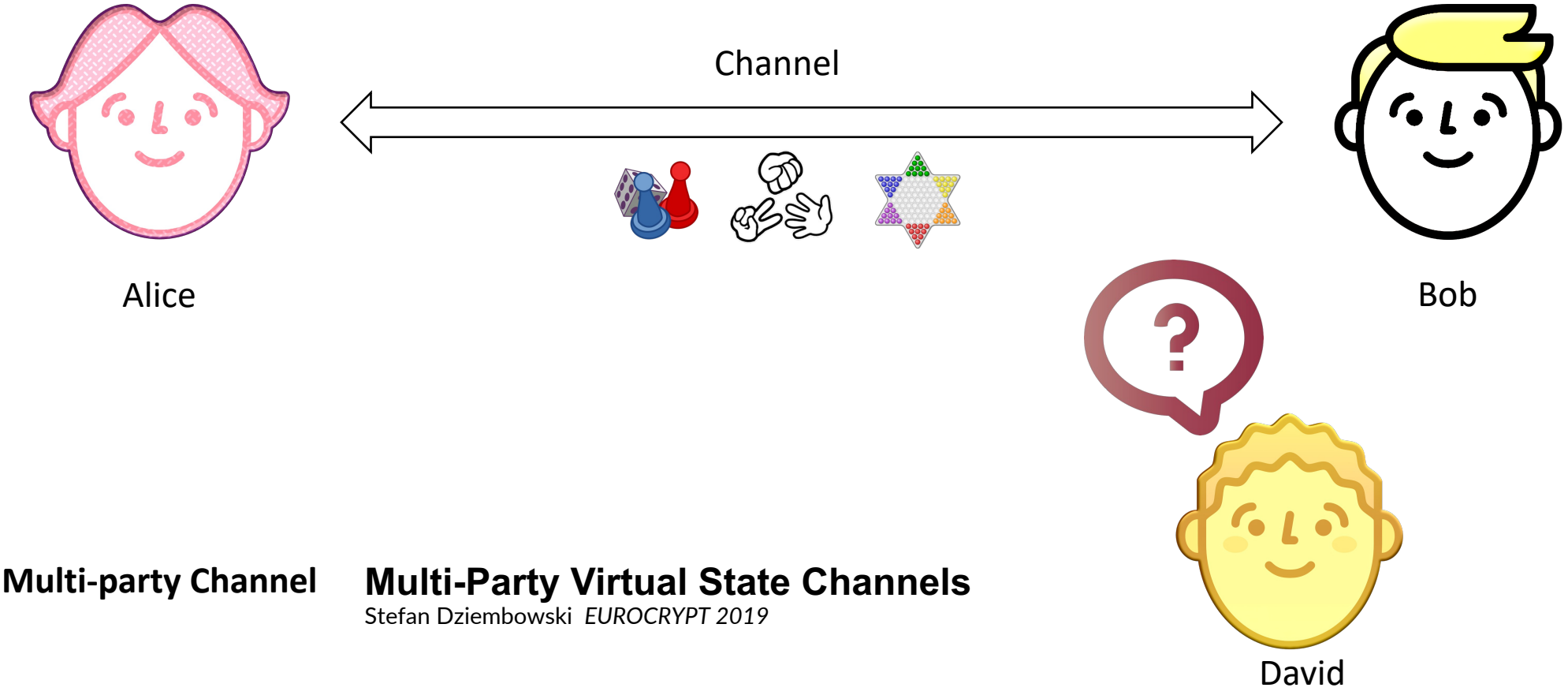


Traditional Channel

Celer

...

Why Need Multi-party State Channel



Multi-party Channel

Multi-Party Virtual State Channels
Stefan Dziembowski *EUROCRYPT 2019*

Challenges: Isolation

1. States in different channels are isolated. Even with hash-time-lock contract (HTLC).

Multi-party state channel needs to synchronize states among channels to prevent double-spending.

Challenges: Efficiency

2. To setup a multi-party state channel, multiple channels need to be created on the blockchain first!

That is expensive and time consuming!

Challenges: Resource Overhead

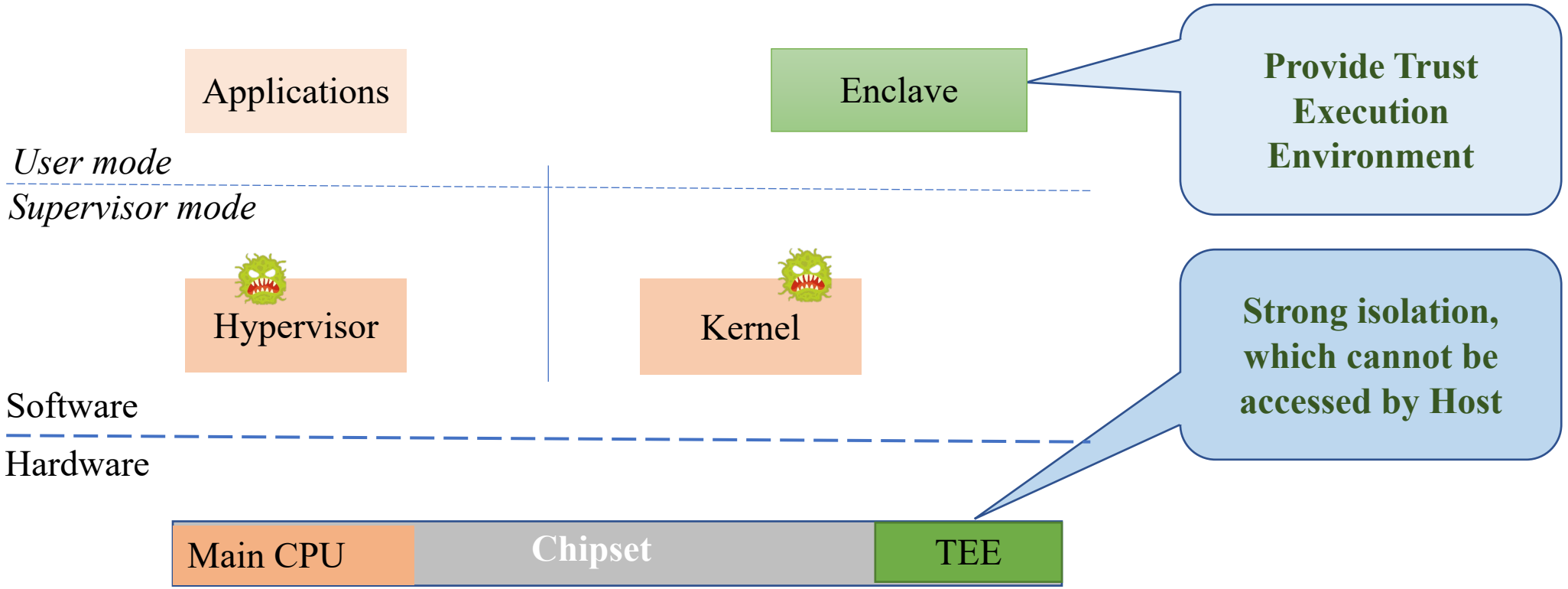
3. Overhead on processing multi-party transactions.

Process multi-party transactions require recursive states update.

Reliable Solution

Using Trusted and Isolated Execution Environment to establish and manage channels without interacting with the main chain!

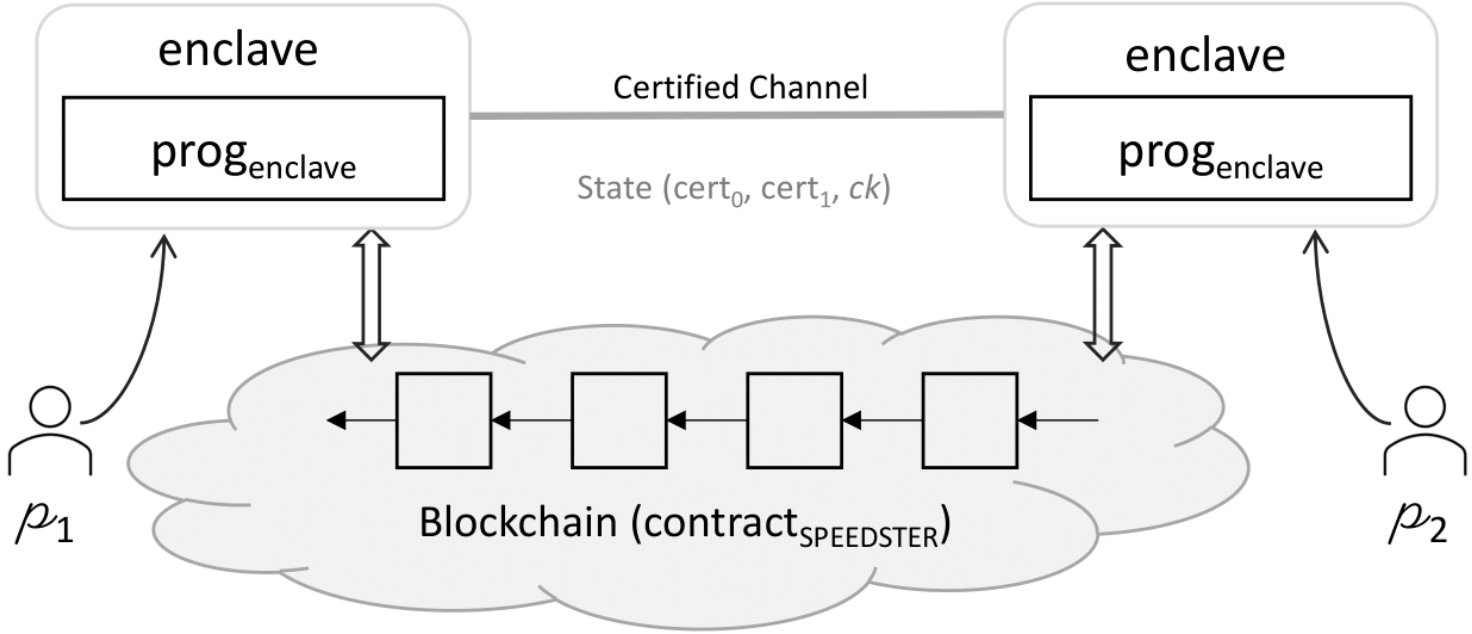
Security System In TEE Architecture



Outline

- Introduction and Background
- **Architecture of Speedster**
- Design and Implementation
- Evaluation
- Conclusion

High-level Architecture of the Speedster



Speedster architecture.

Outline

- Introduction and Background
- Architecture of Speedster
- **Design and Implementation**
- Evaluation
- Conclusion

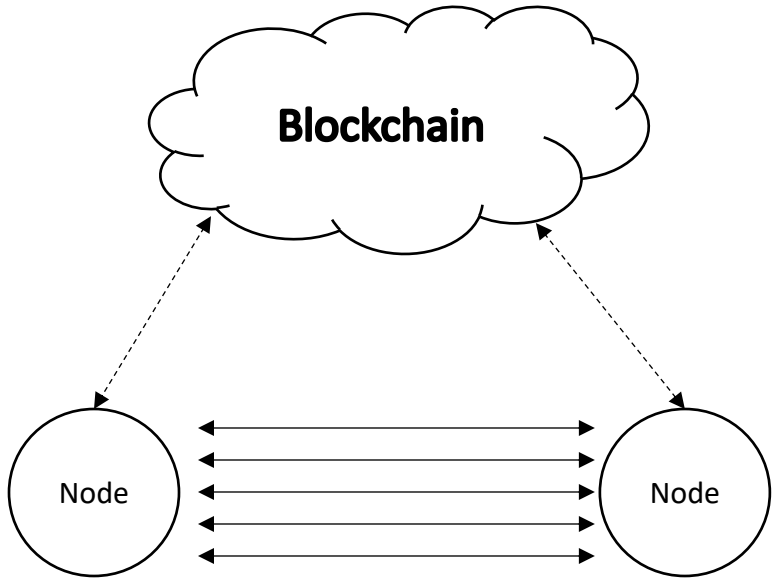
Speedster Design & Implementation

- *Certified Channel*
- Peer-to-Peer Channel Network
- Multi-Party State Channel
- Cross-platform
- TEE Security

Certified Channel

Definition (Certified Channel). A Speedster channel is called a Certified Channel if it is established between two attested enclave accounts and both participants have the channel certificate issued by the other party.

Account Based Channel System



Off-chain Channel Open/Close

1: Node create a TEE account.
2: Node register the account to blockchain,
2: Nodes interact with other nodes off-chain
(attestation, channel creation, transaction)

Transactions in channels are encrypted with AES-GCM instead of ECDSA.

Speedster Design & Implementation

- Certified Channel
- ***Peer-to-Peer Channel Network***
- Multi-Party State Channel
- Cross platform
- TEE Security

Peer-to-Peer Channel Network

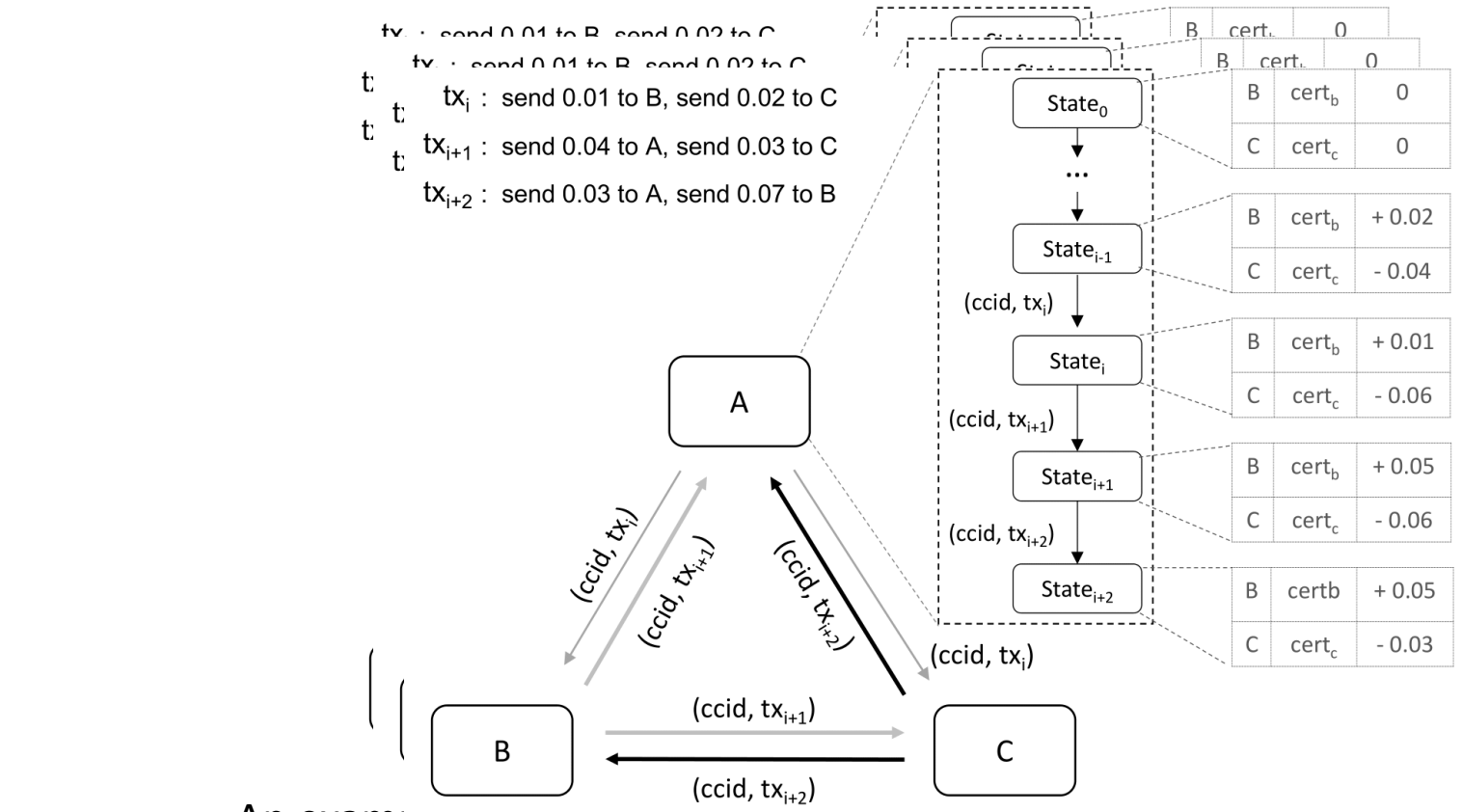
Definition (Peer-to-Peer Channel Network). A payment/state channel network in which a node can establish direct channel connections with other nodes efficiently off-chain and process transactions without relying on intermediaries.

- Direct channel connection.
- Off-chain channel open and close at anytime.
- Minimum fee cost.

Speedster Design & Implementation

- Certified Channel
- Peer-to-Peer Channel Network
- ***Multi-Party State Channel***
- Cross-platform
- TEE Security

Multi-Party State Channel



An example of executing a multi-party transfer contract among A, B and C, assuming SORT(pk_A)>SORT(pk_B)>SORT(pk_C). (+) and (-) in the tables represent the balance change after each respective Certified Channel transaction.

Speedster Design & Implementation

- Certified Channel
- Peer-to-Peer Channel Network
- Multi-Party State Channel
- ***Cross-platform***
- TEE Security

Cross-platform

Prototype of Speedster is cross-platform:

- Intel SGX:
  - Linux-SGX SDK
  - OpenEnclave
- AMD SEV:
  - Qemu
  - Vm:Ubuntu18.04
- ARM TrustZone
  - OPTEE
  - OpenEnclave

Speedster Design & Implementation

- Certified Channel
- Peer-to-Peer Channel Network
- Multi-Party State Channel
- Cross-platform
- ***TEE Security***

TEE Security

TEE Attacks:

- Replay/Rollback attacks.
- Side-channel attacks.
- Denial-of-service attacks.

Solutions:

- A generalized TEE abstraction.
- SEV-SE, Monotonic Counter, RPMB Secure Storage.
- Side-channel-attack resistant cryptographic library.
- Committee enforcement design.

TEE Security

TEE Attacks:

- Replay/Rollback attacks.
- Side-channel attacks.
- Denial-of-service attacks.

❑ TEE Security is another research topic, we can not cover all attacks here!!!

Solutions:

- A generalized TEE abstraction.
- SEV-SE, Monotonic Counter, RPMB Secure Storage.
- Side-channel-attack resistant cryptographic library.
- Committee enforcement design.

Outline

- Introduction and Background
- Architecture of Speedster
- Design and Implementation
- **Evaluation**
- Conclusion

Evaluation

The test environment platform:

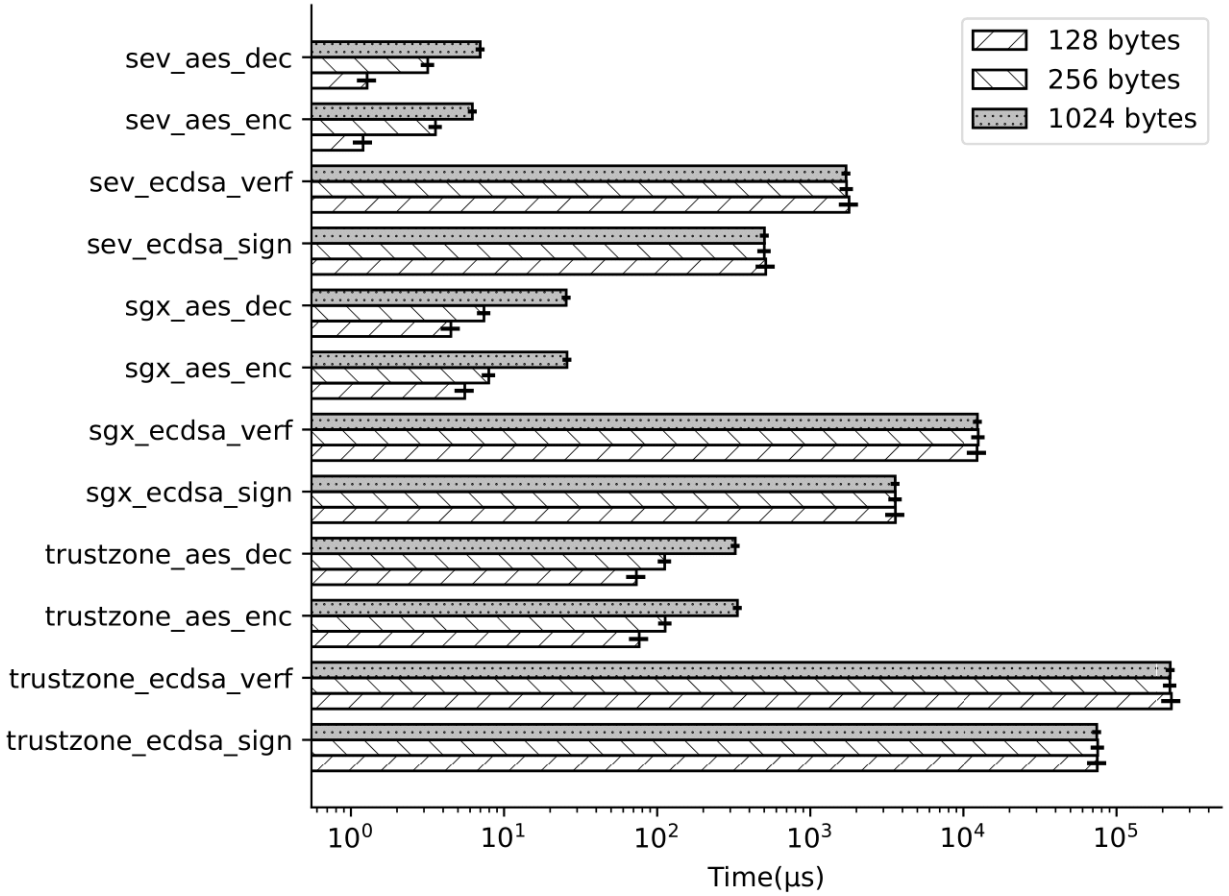
- ✓ Intel SGX: quad-core 3.6 GHz Intel(R) E3-1275 v5 CPU with 32 GB memory.
- ✓ AMD SEV: 64 GB DRAM and an SEV-enabled AMD Epyc 7452 CPU, which has 32 cores and a base frequency of 2.35 GHz.
- ✓ ARM TrustZone: QEMU cortex-a57 virtual machine with 1 GB memory and Linux buildroot 4.14.67-g333dc9e97-dirty as the kernel.
- ✓ Real world: Azure Standard DC1s_v2 (1 vCPUs, 4 GB memory) virtual machines.

Evaluation

Applications:

- Instant State Sharing
- Faster Fund Exchange (ERC20 transaction)
- Sequential Contract Execution (Gomoku)
- Parallel Contract Execution (Rock-Paper-Scissors)
- Multi-party Applications (Monopoly)

Evaluation: Time Cost for Transaction Authentication



- AES-GCM is 3-4 orders faster than ECDSA.

Evaluation: Transaction Performance

- We use the popular layer-2 network, the LN, as a baseline.
- The experiment results are averaged from 10,000 trials.

	Payment	ERC20	Gomuku	RPC
LN	192.630	N/A	N/A	N/A
SEV:AES-GCM	0.1372	0.1382	0.6667	0.1365
SGX:AES-GCM	0.0205	0.3500	0.4500	0.1930
TZ:AES-GCM	20.496	40.148	95.092	37.215

Local time cost for end-to-end transaction (ms)

	LN (lnd)	**Speedster**			
	Payment		ERC20	RPC	Gomoku
Throughput (tps)	14 ±9 %	72,143 ±4 %	30,920 ±10 %	53,355 ±7 %	2,549 ±15 %
Latency (ms)	548.183 ±7 %	80.483 ±1 %	82.490 ±1 %	80.743 ±1 %	82.866 ±1 %

Channel performance in real-world Evaluation

Speedster has better performance than LN in payment processing.

Evaluation: Channel System Comparison

Features	Channel Projects							
	LN [68]	TeeChan [65]	TeeChain [66]	DMC [37]	SFMC [24]	Perun [40]	Celer [38]	Speedster
Direct Off-chain Channel Open	✗	✓	✓	✗	✓	✓	✗	✓
Direct Off-chain Channel Close	✗	✗	✓	✗	✓	✓	✗	✓
Dynamic Deposit	✗	✗	✓	✗	✓	✗	✗	✓
Off-Chain Contract Execution	✗	✗	✗	✗	✗	✗	✓	✓
P2PCN	✗	✗	✗	✗	✗	✗	✗	✓
Multi-Party State Channel	✗	✗	✗	✗	✓	✗	✗	✓
Dispute-Free	✗	✗	✓	✗	✗	✗	✗	✓
Duplex Channel	✗	✗	✓	✓	✓	✗	✗	✓

Feature comparison with other channel projects.

Speedster is the only project that provides all features.

Outline

- Introduction and Background
- Architecture of KShot
- Design and Implementation
- Evaluation: Effectiveness and Performance
- **Conclusion**

Conclusion

- **Speedster** – efficient multi-party state channel system
  - — Leverage TEE.
  - — Use AES-GCM to encrypt transaction.
  - — Off-chain channels can be freely opened/closed.
  - — Dispute free.
  - — Support multi-party state channels.
  - — Cross-platform.

Thank you!

liaojh2021@mail.sustech.edu.cn/jinghui@wayne.edu

https://fengweiz.github.com/