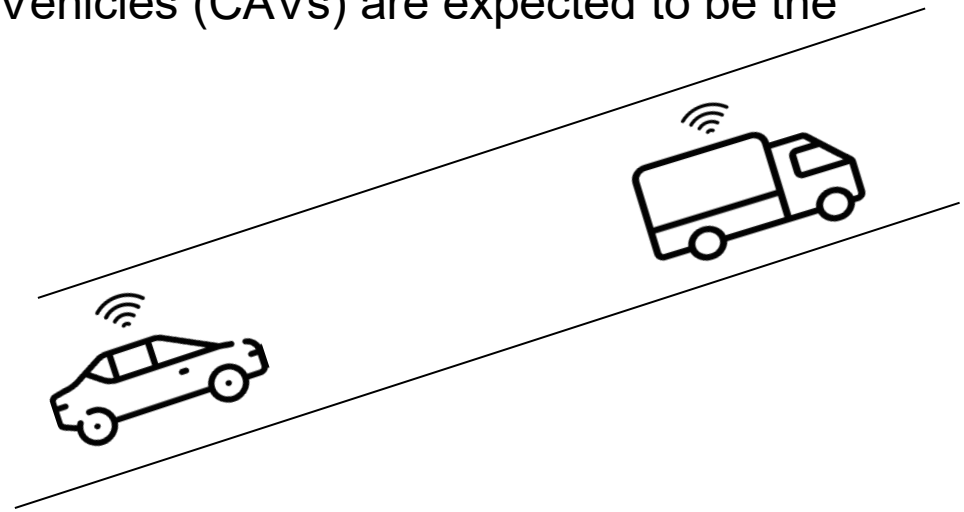
Towards a TEE-based V2V Protocol for Connected and Autonomous Vehicles

Zhiqiang Lin
zlin@cse.ohio-state.edu

7/27/2022

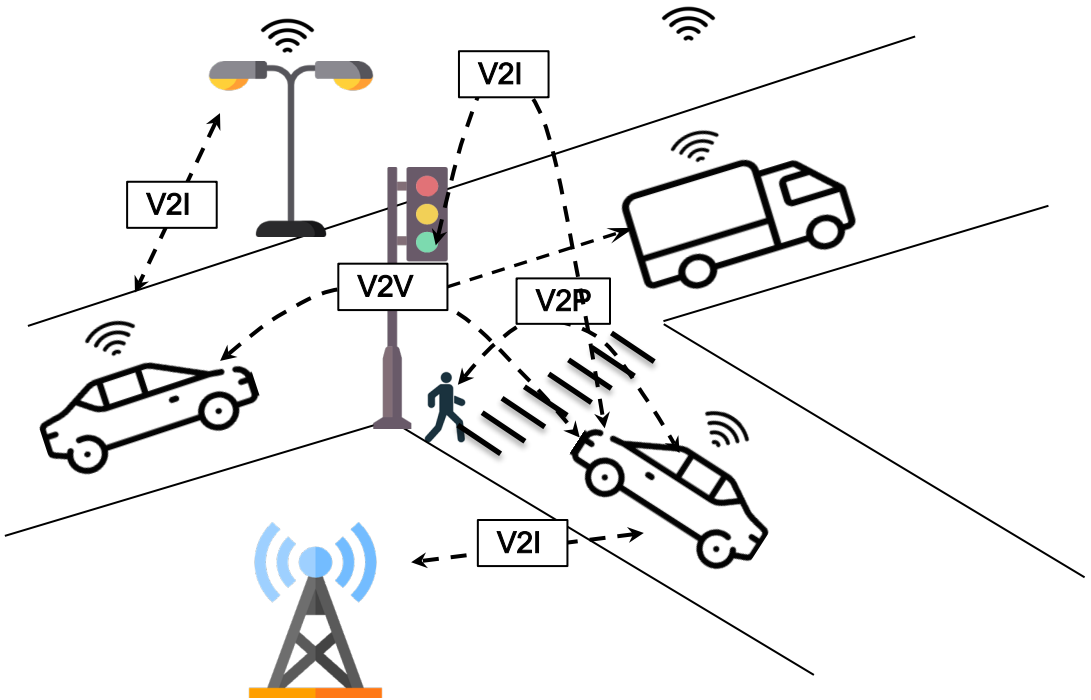
Background

- Connected and Autonomous Vehicles (CAVs) are expected to be the dominant vehicles
  - Increased safety
  - Reduced driver stress
  - Reduced energy consumption
  - Reduced traffic congestion
  - Reduced pollution



The need for communication in CAVs

- Vehicle to Vehicle (V2V)
  - 360-degree “awareness”
    - Speed
    - Location
    - Position
    - Heading
- Vehicle to Infrastructure (V2I)
  - Traffic lights
  - Lane markers
  - Parking meters
- Vehicle to Pedestrian (V2P)
  - People walking
  - Children in strollers
  - People using wheelchairs
  - People riding bicycles

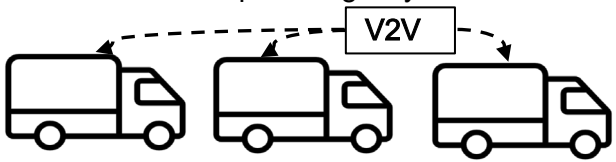


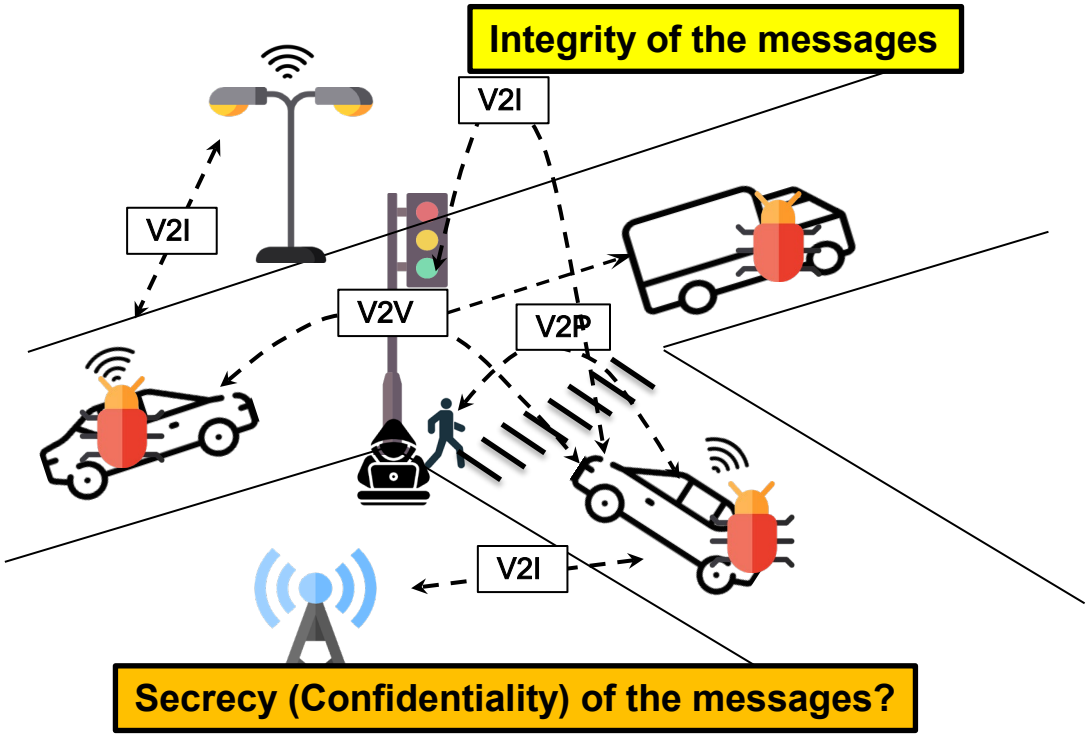
The need for ***secure*** communication in CAVs

- Vehicle to Vehicle (V2V)
  - 360-degree “awareness”
    - Speed
    - Location
    - Position
    - Heading

- Vehicle to Infrastructure (V2I)
  - Traffic lights
  - Lane markers
  - Parking meters

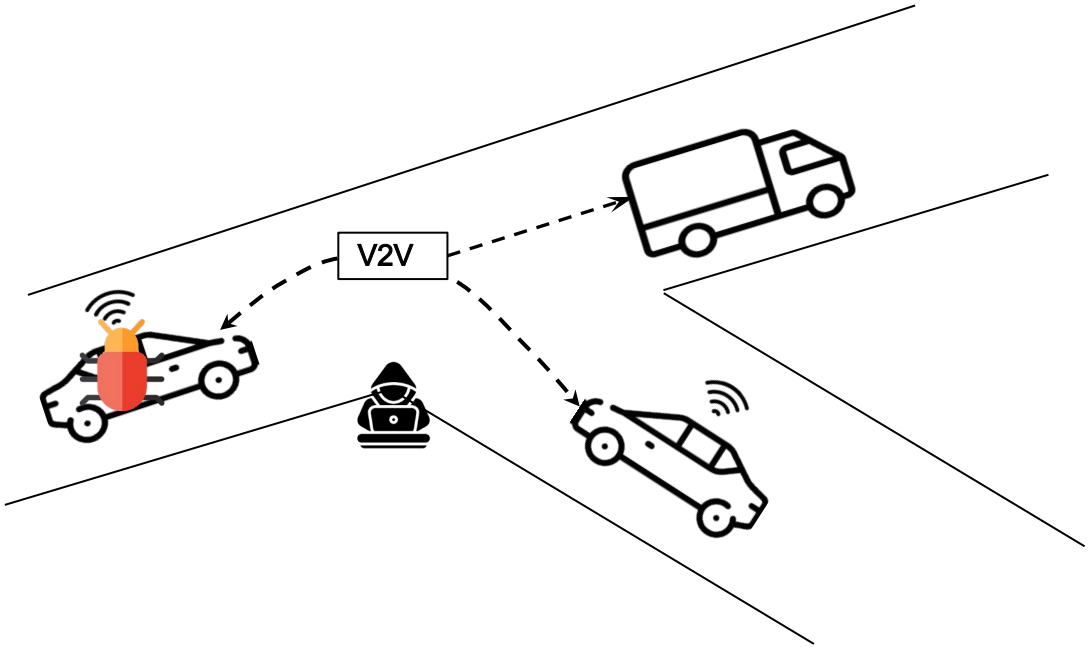
- Vehicle to Pedestrian (V2P)
  - People walking
  - Children in strollers
  - People using wheelchairs
  - People riding bicycles





The need for ***secure*** and ***efficient*** communication in CAVs

- **Security and Privacy**
  - **Integrity**
    - Replay prevention
    - Message forgery
  - **Privacy (Secrecy)**
    - Identity of the vehicle
    - Location of the vehicle
  - Two-way authentication
  - Non-repudiation
  - Accountability
  - Dynamic revocation



- **Efficient and Performant**
  - < 100 *ms* latency

Prior Solutions

- Using **Certificates** (Public Key Cryptography) and PKI
  - IEEE 1609.x: standards for Applications and Security
- **Message Integrity** (not confidentiality)
  - Signed by the private key of the vehicle
- No broadcast encryption
  - Hard to exchange crypto-keys efficiently among encountered Vehicles

Our Proposed Solution

- Using **TEEs** to protect the secrets (integrity and confidentiality)
  - ***Private Key*** for signing
  - ***Symmetric Key*** for broadcast encryption

- Achieving
  - Integrity
    - Replay prevention
    - Message forgery
  - Privacy (Secrecy)
    - Identity of the vehicle
    - Location of the vehicle
  - Two-way authentication
  - Non-repudiation
  - Accountability
  - Dynamic revocation

"**Towards A TEE-based V2V Protocol For Connected And Autonomous Vehicles**". Mohit Jangid, and Zhiqiang Lin. In *Proceedings of the Automotive and Autonomous Vehicle Security (AutoSec) Workshop 2022*, San Diego, CA, April 2022.

Threat Model

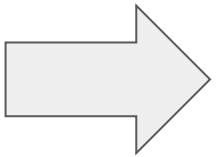
- Malware 
- MitM adversary 
  - Access, modify, and replay the wireless traffic to any vehicles

- Physical access
  - Vehicle can be under complete physical control of an adversary

Side channel attacks against TEEs out of scope

Overview of Our Approach

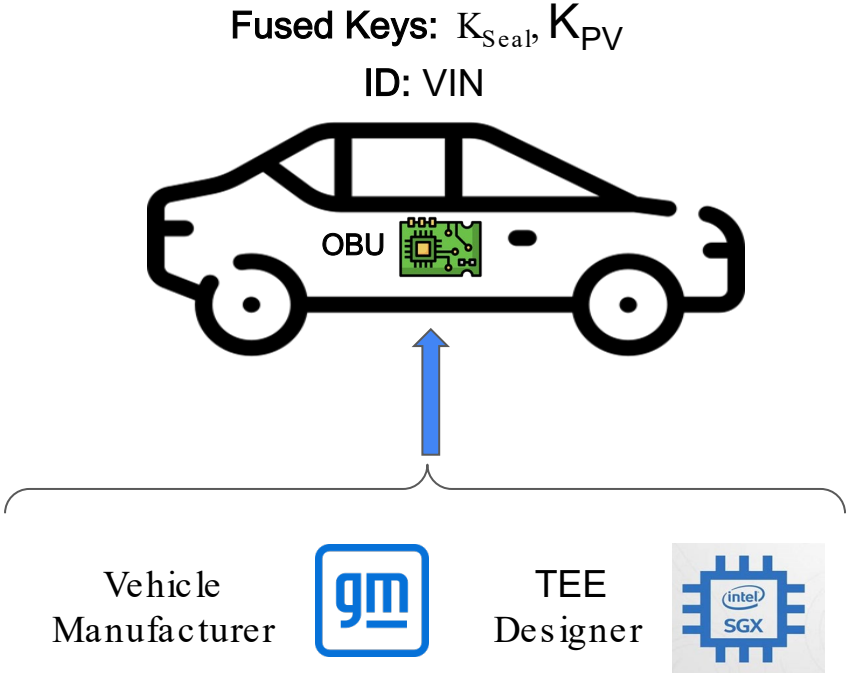
- Using **broadcast encryption**
  - Symmetric key distribution using remote attestation
- **Leveraging TEEs** for
  - Run-time data protection
  - Instant peer-peer authentication
  - Secure symmetric key provision
- Using **temporal IDs** for privacy



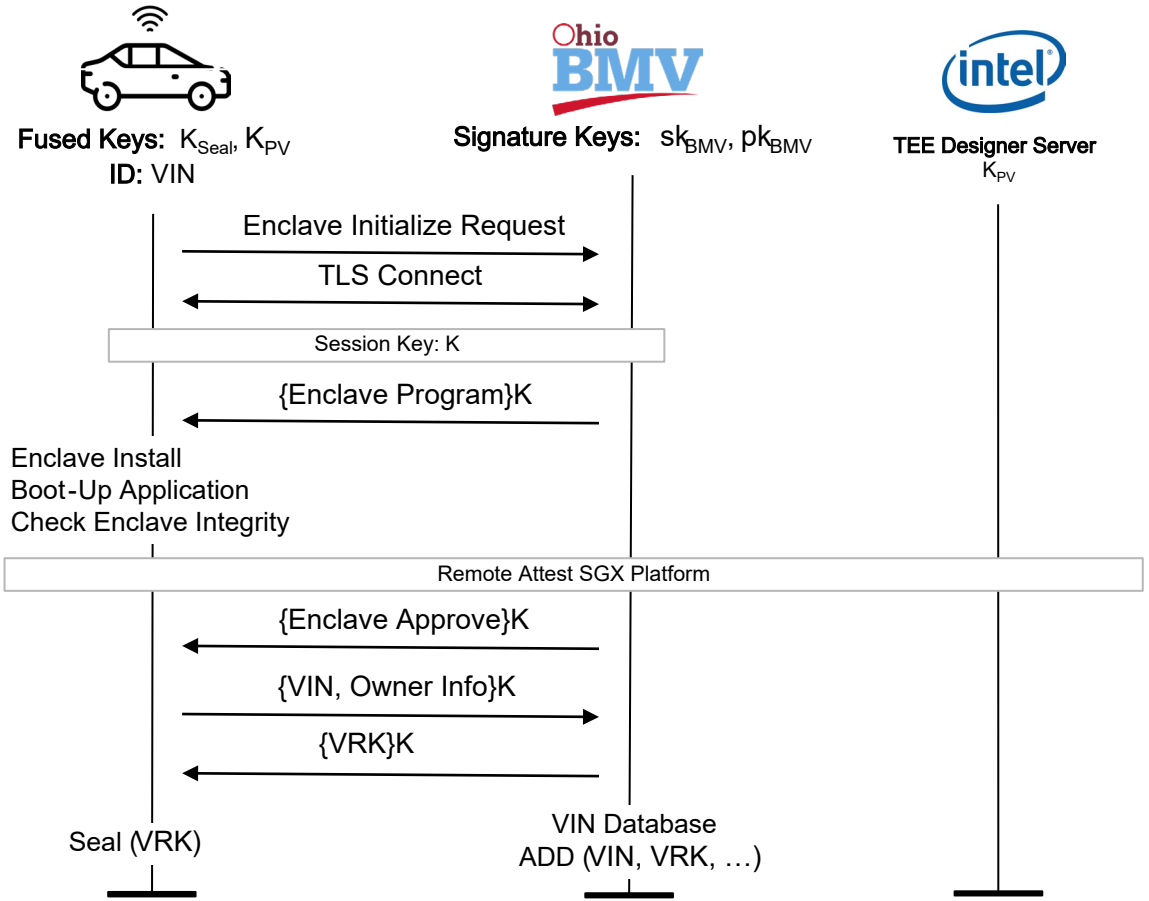
- Fast (Performant)
- Secure
- Privacy Preserving
- Accountability

Detailed Design: A Four Stage Protocol

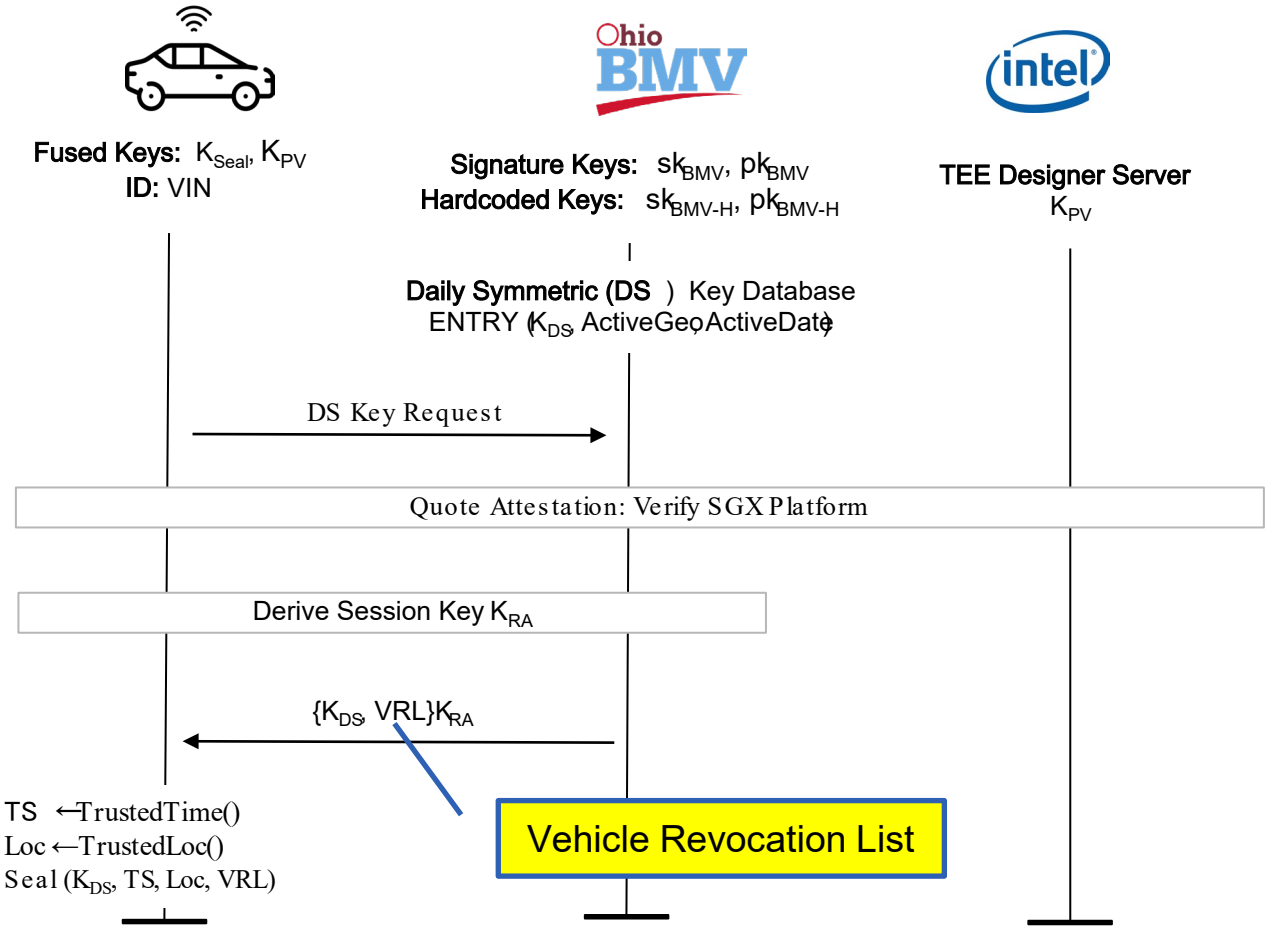
Stage 1 -- Manufacture Phase (One time)



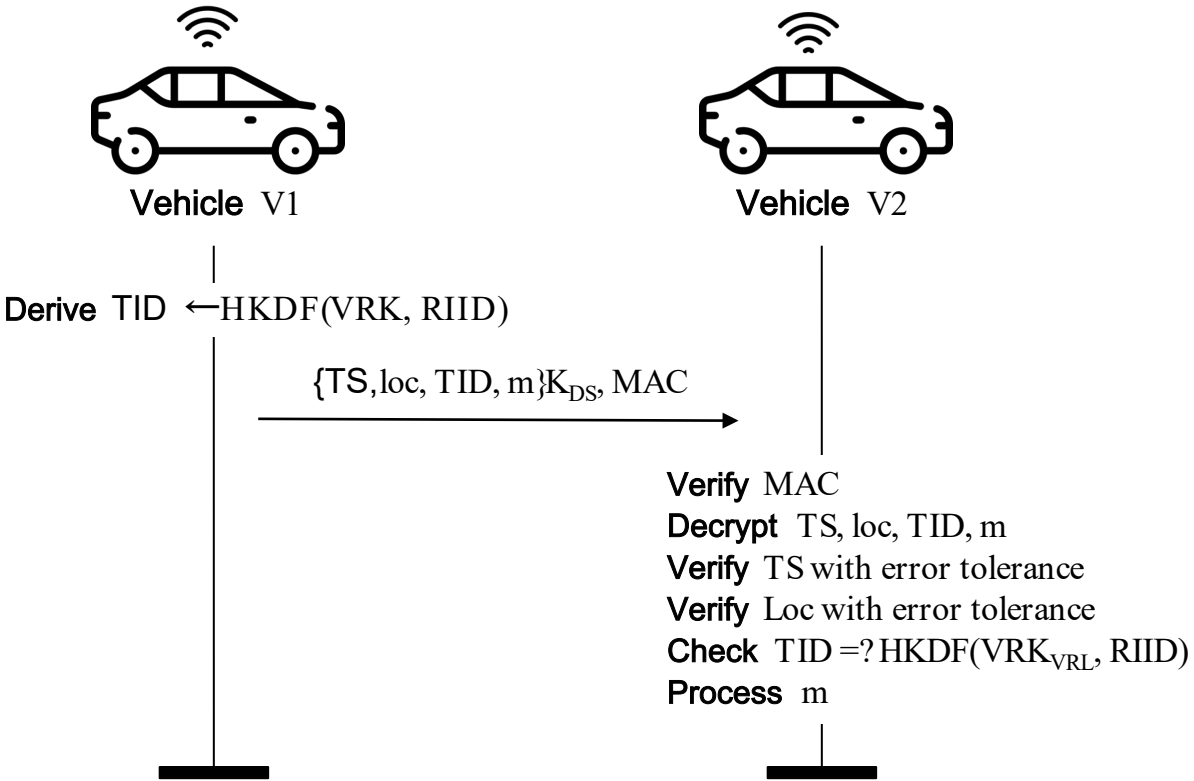
Stage 2 -- Registration Phase (One time)



Stage 3 -- Symmetric Key Provision



Stage 4 -- On-Road Instant Broadcast



Other Design Details

Privacy and Accountability Computations

Privacy

Vehicle Root Key: Random seed

$$\text{VRootKey} = CRNG(128)$$

Rolling Temporal ID : one TempID for each time slice

$$\text{TempID} = HKDF(\text{VRootKey}, \text{RollingID})$$

Accountability

Misbehaving incident broadcast: TempID_M

$$\text{RollingID}_M = \frac{\text{TimeStamp}_M - \text{EpochTime}}{\text{Rolling Interval}}$$

Probe, all Seed_i entries in the database to match TempID_M

$$\text{TempID}_M \stackrel{?}{=} \text{HKDF}(\text{VRootKey}_i, \text{RollingID}_M)$$

Experiment Result

Prototype Setup

- **TEE:** Intel SGX Enclave based encryption/decryption, TID generation, revocation

VS

- **PKI:** 3 Way Certificate-PKI based authentication and revocation

Setup

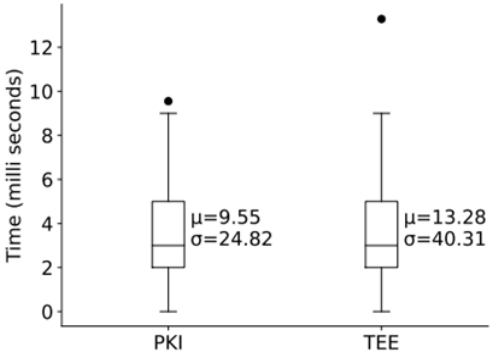
- Two Intel processors with Intel wireless adaptors
- Socket programming for payload preparation
- 100 revoked vehicles
- Constant size payload for 39 bytes of a safety message

Prototype Assumption

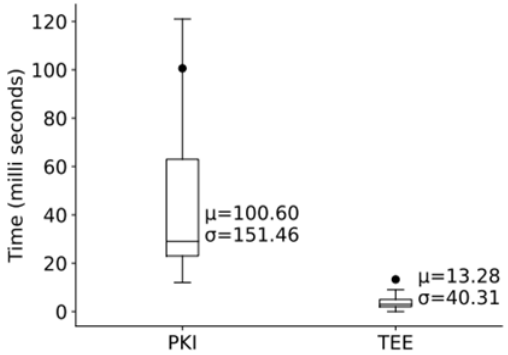
- **Trusted Time**, **Trusted Location** and **Monotonic Counters** are not implemented for TEE-V2V yet

- Tested on two stationary laptops, communicating with Wi-Fi channels

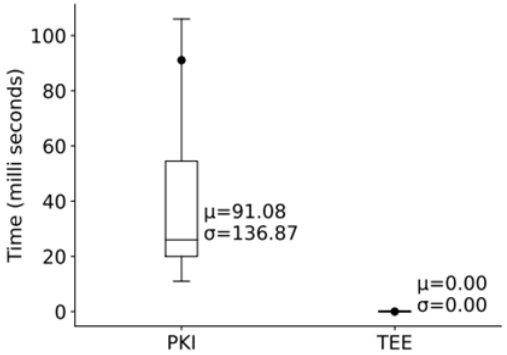
Preliminary Results



(a) BSM Broadcast Latency



(b) End To End Latency



(c) Key Exchange Latency

Future Work

Using Group Signatures?

Privacy

Vehicle Root Key: Random seed

$$\text{VRootKey} \leftarrow CRNG(128)$$

Rolling Temporal ID : one TempID for each time slice

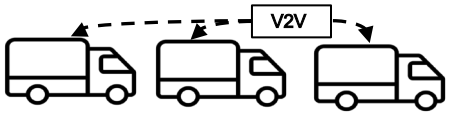
$$\text{TempID} = HKDF(\text{VRootKey}, \text{RollingID})$$

Group Signatures [Chaum and Heyst 1991]

- Unforgeability
- Anonymity
- Traceability
- Unlinkability

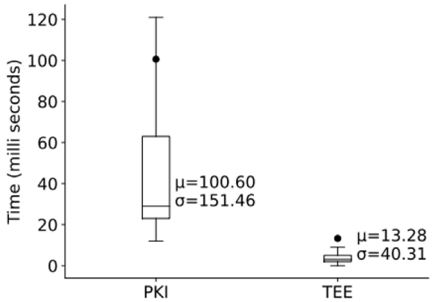
Takeaway

- Using TEEs to protect the secrets (integrity and confidentiality)
  - Private Key
  - Symmetric Key for broadcast encryption



- Achieving
  - Integrity
    - Replay prevention
    - Message forgery
  - Privacy
    - Identity of the vehicle
    - Location of the vehicle
  - Two-way authentication
  - Non-repudiation
  - Accountability
  - Dynamic revocation

- Our preliminary results demonstrates that TEE-based approach is faster compared with a certificate-based approach



http://web.cse.ohio-state.edu/~lin.3021/file/AutoSec2022.pdf