Zone Encryption with Anonymous Authentication for V2V Communication

Jan Camenisch, Manu Drijvers, Anja Lehmann, Gregory Neven and Patrick Towa

Gautam Singh

Indian Institute of Technology Hyderabad

April 23, 2024

V2X Related Terminology

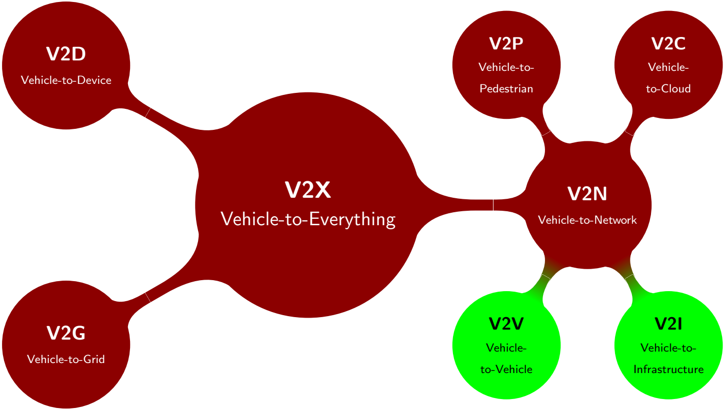

Figure 1: A breakdown of V2X.

Message Types in V2X

1. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)
    1. Exchanged between vehicles to create awareness and support cooperative performance of vehicles in the road network.
    2. Includes status information such as time, position, speed, active systems, vehicle dimensions, etc.

[1] European Telecommunications Standards Institute. "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service". In: ETSI EN 302 637-2 V1.4.1 (2019). URL: https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf.

Message Types in V2X

1. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)
   1. Exchanged between vehicles to create awareness and support cooperative performance of vehicles in the road network.
   2. Includes status information such as time, position, speed, active systems, vehicle dimensions, etc.
2. Other types of messages
   1. **Signal Phase and Timing** (SPaT)
   2. **Roadside Infrastructure Information** (MAP)

[1] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
   1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
   2. Easy to intercept.
   3. Leak sensitive information about the vehicle owners.

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
    2. Easy to intercept.
    3. Leak sensitive information about the vehicle owners.
    4. **Huge privacy concerns and threats!**

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
    2. Easy to intercept.
    3. Leak sensitive information about the vehicle owners.
    4. **Huge privacy concerns and threats!**
2. Encryption impractical, since CAMs *must* be decrypted by nearby vehicles in a highly dynamic environment.
    1. But CAMs *have to* be encrypted because of the data they carry!

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
    2. Easy to intercept.
    3. Leak sensitive information about the vehicle owners.
    4. **Huge privacy concerns and threats!**
2. Encryption impractical, since CAMs *must* be decrypted by nearby vehicles in a highly dynamic environment.
    1. But CAMs *have to* be encrypted because of the data they carry!
3. Instead, focus on *privacy-preserving authentication*.
    1. Ensuring a message is issued by a “genuine” vehicle.
    2. “Genuine” vehicles must be untraceable.

V2X and Cryptology

1. Deployed systems
   1. Use short-term **pseudonym certificates** (100 per week in EU, 20 per week in US), rotate between them.
   2. Trade-off between security (Sybil resistance), privacy and efficiency (storage and bandwidth costs).

V2X and Cryptology

1. Deployed systems
    1. Use short-term **pseudonym certificates** (100 per week in EU, 20 per week in US), rotate between them.
    2. Trade-off between security (Sybil resistance), privacy and efficiency (storage and bandwidth costs).
2. Proposed systems
    1. Stronger privacy and security guarantees.
    2. Do not meet the *stringent bandwidth constraint* of **300 bytes per CAM**, thus impractical.

Motivation and Goals

1. Unlimited privacy.
2. Address problems of authenticity and confidentiality in combination *for the first time*.
3. Meet (bandwidth) requirements.
4. Efficient encryption scheme (symmetric-key crypto).
5. Negligible storage and bandwidth overheads.
6. Better security guarantees (privacy, authenticity, confidentiality).

Preliminaries

1. Pairing-based Cryptography
2. Hardness Assumptions
   1. Symmetric Discrete Logarithm (SDL) assumption
   2. Modified q-Strong Diffie-Hellman (q-MSDH-1) assumption
3. Deterministic Authenticated Encryption (DAE)
4. PS Signatures
5. Dynamic Group Signatures with Attributes (DGS+A)

Overall Flow of Zone Encryption

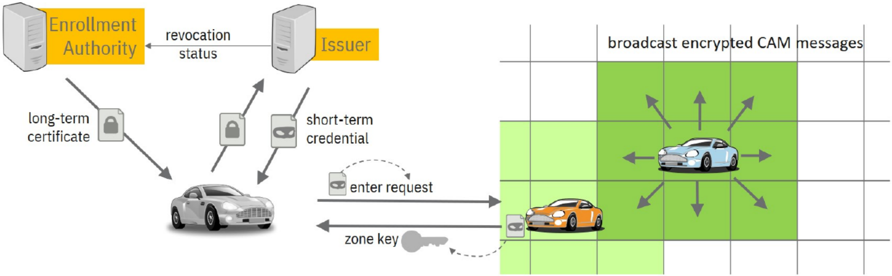

Figure 2: Illustration of Zone Encryption with its Anonymous-Authentication Approach.

Notation

Notation	Meaning
Z	Set of zones covering the road network
$\mathcal{P}$	Payload/message space
$Epoch$	Set of epochs
T	Set of timestamps
$K_{z,t}$	Zone key for zone z at time t
L_K	List of zone keys known to a vehicle, stored as $(z, t, K_{z,t})$
$\mathcal{E}$	Enrollment authority
$\mathcal{I}$	Issuer
$\mathcal{V} \in \{0,1\}^*$	Vehicle identity
$cert_{\mathcal{V}}$	Long-term certificate of $\mathcal{V}$
$cred_{\mathcal{V}}$	Short-term credential of $\mathcal{V}$

Zones, Epochs, Zone Keys

1. A *zone z* is a continuous geographical area covering part of a road network (shown as squares alongside).

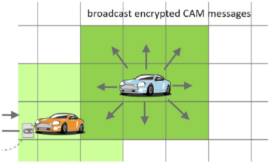

Figure 3: A vehicle must have the zone keys of zones adjacent to it. It can communicate with another vehicle if they share a zone key.

Zones, Epochs, Zone Keys

1. A *zone* z is a continuous geographical area covering part of a road network (shown as squares alongside).
2. Each zone has a *zone key* $K_{z,t}$ periodically refreshed after a time interval called an *epoch*.
   - An epoch is denoted by $[e, e+1)$. Each time instance t satisfies $e \leq t < e+1$ for a unique e. This is denoted as $e(t)$.
   - Vehicles need $K_{z,t}$ for secure communication when they are in zone z at time t.

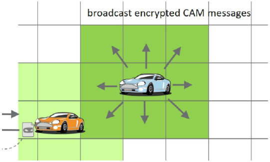

Figure 3: A vehicle must have the zone keys of zones adjacent to it. It can communicate with another vehicle if they share a zone key.

Zones, Epochs, Zone Keys

1. A *zone* z is a continuous geographical area covering part of a road network (shown as squares alongside).
2. Each zone has a *zone key* $K_{z,t}$ periodically refreshed after a time interval called an *epoch*.
   - An epoch is denoted by $[e, e+1)$. Each time instance t satisfies $e \le t < e+1$ for a unique e. This is denoted as $e(t)$.
   - Vehicles need $K_{z,t}$ for secure communication when they are in zone z at time t.
3. Vechicles can communicate securely with other vehicles in surrounding zones also.

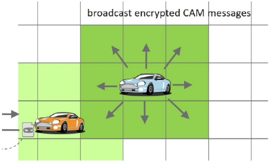

Figure 3: A vehicle must have the zone keys of zones adjacent to it. It can communicate with another vehicle if they share a zone key.

Entities and Credentials

1. An *enrollment authority* $\mathcal{E}$ issues *long-term certificates* to vehicle $\mathcal{V} \in \{0,1\}^*$.
   1. Long-term certificate $cert_{\mathcal{V}}$ obtained.
   2. Can be used to check revocation status.

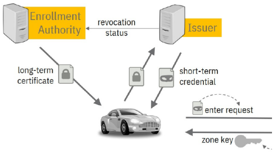

Figure 4: Various entities and exchanged credentials in ZE.

Entities and Credentials

1. An *enrollment authority* $\mathcal{E}$ issues *long-term certificates* to vehicle $\mathcal{V} \in \{0,1\}^*$.
   1. Long-term certificate $cert_{\mathcal{V}}$ obtained.
   2. Can be used to check revocation status.
2. An *issuer* $\mathcal{I}$ issues *short-term credentials* to vehicles every epoch.
   1. Long-term credential $cert_{\mathcal{V}}$ used here.
   2. Short-term credential $cred_{\mathcal{V}}$ obtained.
   3. $cred_{\mathcal{V}}$ is valid only for the epoch e in which it was issued.

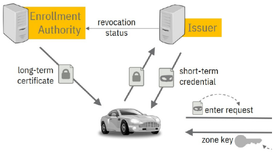

Figure 4: Various entities and exchanged credentials in ZE.

Syntax of ZE

Setup and Key Generation

1. Setup $\left(1^{\lambda}, Z, Epoch, T\right) \rightarrow pp$
2. KG.E $(pp) \rightarrow (pk_{\mathcal{E}}, (sk_{\mathcal{E}}, st_{\mathcal{E}}))$
   - State keeps track of enrolled vehicles.
3. KG.I $(pp) \rightarrow (pk_{\mathcal{I}}, (sk_{\mathcal{I}}, st_{\mathcal{I}}))$
   - State keeps track of open messages sent during key requests.

Syntax of ZE

Setup and Key Generation

1. Setup $(1^\lambda, Z, Epoch, T) \to pp$
2. KG.E $(pp) \to (pk_{\mathcal{E}}, (sk_{\mathcal{E}}, st_{\mathcal{E}}))$
   - State keeps track of enrolled vehicles.
3. KG.I $(pp) \to (pk_{\mathcal{I}}, (sk_{\mathcal{I}}, st_{\mathcal{I}}))$
   - State keeps track of open messages sent during key requests.

Receiving Long-term and Short-term Credentials

1. $\langle$Enroll.V $(pk_{\mathcal{E}}, \mathcal{V}) \leftrightharpoons$ Enroll.E $(sk_{\mathcal{E}}, st_{\mathcal{E}}, \mathcal{V})\rangle \to \langle cert_{\mathcal{V}}, st'_{\mathcal{E}}\rangle$
2. $\langle$Authorize.V $(cert_{\mathcal{V}}, e, pk_{\mathcal{I}}) \leftrightharpoons$ Authorize.I $(sk_{\mathcal{I}}, st_{\mathcal{I}}, \mathcal{V}, e, pk_{\mathcal{E}})\rangle \to \langle cred_{\mathcal{V}}, st'_{\mathcal{I}}\rangle$
   - Vehicle uses certificate to obtain credentials.
   - Issuer checks certificate using public key of issuer.

Syntax of ZE

Entering and Exiting Zones

1. $\langle \text{Enter.V}\,(cred_{\mathcal{V}}, L_K, pk_{\mathcal{I}}, z, t, requester) \leftrightharpoons \text{Enter.W}\,(cred_{\mathcal{W}_i}, L_{K_i}, pk_{\mathcal{I}}, z, t, responder_i)_{i \geq 0}\rangle \rightarrow \langle L_K, \perp\rangle$
   - Why $i \geq 0$?
2. $\text{Exit}\,(L_K, z, t) \rightarrow L'_K$

Sending and Receiving Payloads

1. $\text{Send}\,(L_K, P, Y \subseteq Z, t) \rightarrow \gamma / \perp$
2. $\text{Receive}\,(L_K, \gamma) \rightarrow P / \perp$
3. It's all symmteric key cryptography! (But what is the symmetric key?)

Syntax of ZE

Identity Escrow

1. Open $(sk_{\mathcal{I}}, st_{\mathcal{I}}, m) \rightarrow \mathcal{V}/\perp$
2. m is a message that was sent during an execution of Enter.
3. Only $\mathcal{I}$ can find which vehicle sent m.
4. Use cases
    - To revoke certificates of misbehaving vehicles.
    - To provide concrete court evidence.
5. Assuming identity escrow is rare, Open need not be efficient in terms of time/storage complexity.

Security of ZE

1.

Instantiation of ZE and Efficiency

(Is it worth mentioning section 4.4.1 or can we leave this?)

Summary of ZE

Table 2 of the paper.

DGS+A

Sub-headings

1. Syntax
2. Security properties (no proofs)
3. Instantiation from PS
4. Can be extended to threshold opening (should be a slide or only a mention during talk?)

Challenges in Deploying ZE

Section 4.6

Future Improvements

Section 4.6, brief and top-level idea of mini-project if time permits.