Anonymous Key Agreements for V2X Communication

Gautam Singh

Indian Institute of Technology Hyderabad

May 1, 2024

1 Introduction

2 Preliminaries

3 Our Proposition

4 Conclusion

V2X Related Terminology

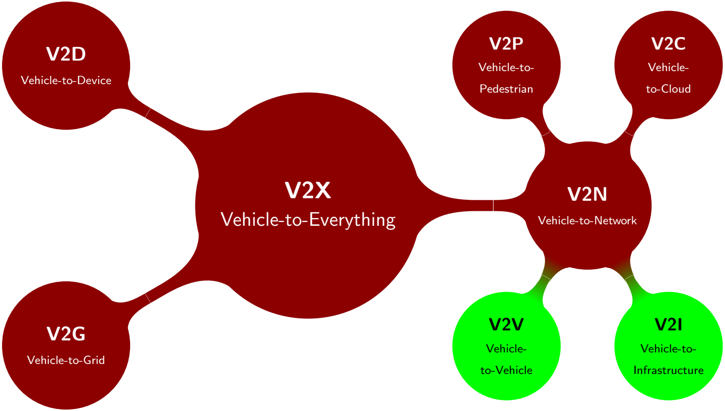

Figure 1: A breakdown of V2X.

Message Types in V2X

1. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2].
    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.
    3. Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    4. **Huge privacy concerns and threats!**

[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.

[2] *J2735_202309: V2X Communications Message Set Dictionary - SAE International*. URL: https://www.sae.org/standards/content/j2735_202309/ (visited on 04/15/2024).

Message Types in V2X

1. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2].
    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.
    3. Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    4. **Huge privacy concerns and threats!**
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".

[2] *J2735_202309*.

Motivation and Goals

1. Do we *really* need to encrypt CAMs?
    - Google (Maps) may already be profiling us!
    - Focus on encrypting more sensitive messages and information sent less frequently.

Motivation and Goals

1. Do we *really* need to encrypt CAMs?
    - Google (Maps) may already be profiling us!
    - Focus on encrypting more sensitive messages and information sent less frequently.
2. Unlimited privacy.

Motivation and Goals

1. Do we *really* need to encrypt CAMs?
    - Google (Maps) may already be profiling us!
    - Focus on encrypting more sensitive messages and information sent less frequently.
2. Unlimited privacy.
3. Better security guarantees (privacy, authenticity, confidentiality).

Pairings

Definition 1

Pairing[a] Let $\mathbb{G}_0 = \langle g_0 \rangle$, $\mathbb{G}_1 = \langle g_1 \rangle$, $\mathbb{G}_T$ be three cyclic groups of prime order q. A *pairing* is an efficiently computable function $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$ satisfying the following properties:

1. *bilinear*: for all $u, u' \in \mathbb{G}_0$ and $v, v' \in \mathbb{G}_1$, we have

$$e\left(uu', v\right) = e\left(u, v\right) e\left(u', v\right) \tag{1}$$

$$e\left(u, vv'\right) = e\left(u, v\right) e\left(u, v'\right) \tag{2}$$

2. *non-degenerate*: $g_T := e\left(g_0, g_1\right)$ is a generator of $\mathbb{G}_T$.

[a] *A Graduate Course in Applied Cryptography*. URL: https://toc.cryptobook.us/ (visited on 04/30/2024).

Pairings

Definition 1

Pairing[a] Let $\mathbb{G}_0 = \langle g_0 \rangle$, $\mathbb{G}_1 = \langle g_1 \rangle$, $\mathbb{G}_T$ be three cyclic groups of prime order q. A *pairing* is an efficiently computable function $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$ satisfying the following properties:

1. *bilinear*: for all $u, u' \in \mathbb{G}_0$ and $v, v' \in \mathbb{G}_1$, we have

$$e\left(uu', v\right) = e\left(u, v\right) e\left(u', v\right) \tag{1}$$

$$e\left(u, vv'\right) = e\left(u, v\right) e\left(u, v'\right) \tag{2}$$

2. *non-degenerate*: $g_T := e\left(g_0, g_1\right)$ is a generator of $\mathbb{G}_T$.

[a] *A Graduate Course in Applied Cryptography*.

1. Here, $\mathbb{G}_0$ and $\mathbb{G}_1$ are called *source groups* and $\mathbb{G}_T$ is called the *target group*.

Pairings

Definition 1

Pairing[a] Let $\mathbb{G}_0 = \langle g_0 \rangle$, $\mathbb{G}_1 = \langle g_1 \rangle$, $\mathbb{G}_T$ be three cyclic groups of prime order q. A *pairing* is an efficiently computable function $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$ satisfying the following properties:

1. *bilinear*: for all $u, u' \in \mathbb{G}_0$ and $v, v' \in \mathbb{G}_1$, we have

$$e\left(uu', v\right) = e\left(u, v\right) e\left(u', v\right) \tag{1}$$

$$e\left(u, vv'\right) = e\left(u, v\right) e\left(u, v'\right) \tag{2}$$

2. *non-degenerate*: $g_T := e\left(g_0, g_1\right)$ is a generator of $\mathbb{G}_T$.

[a] *A Graduate Course in Applied Cryptography*.

1. Here, $\mathbb{G}_0$ and $\mathbb{G}_1$ are called *source groups* and $\mathbb{G}_T$ is called the *target group*.
2. When $\mathbb{G}_0 = \mathbb{G}_1$, the pairing is said to be *symmetric*.

Anonymous Key Agreement

1. A key agreement protocol where two parties agree on a shared secret key, without being able to determine the other party.

[3] Aniket Kate, Greg Zaverucha, and Ian Goldberg. "Pairing-Based Onion Routing". In: *Privacy Enhancing Technologies*. Ed. by Nikita Borisov and Philippe Golle. Vol. 4776. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 95–112. ISBN: 978-3-540-75550-0. DOI: 10.1007/978-3-540-75551-7_7. URL: http://link.springer.com/10.1007/978-3-540-75551-7_7 (visited on 04/04/2024).

Anonymous Key Agreement

1. A key agreement protocol where two parties agree on a shared secret key, without being able to determine the other party.
2. Pairing-based anonymous key agreement for V2X.

[3] Kate, Zaverucha, and Goldberg, "Pairing-Based Onion Routing".

Anonymous Key Agreement

1. A key agreement protocol where two parties agree on a shared secret key, without being able to determine the other party.
2. Pairing-based anonymous key agreement for V2X.
3. We use a pairing-based anonymous key agreement involving a private key generator (PKG)[3].
    1. PKG has its own master private and public key.
    2. PKG uses master secret key to generate secret keys for clients.
    3. Clients use this secret key to establish the shared secret key.

[3] Kate, Zaverucha, and Goldberg, "Pairing-Based Onion Routing".

Anonymous Key Agreement

1. A key agreement protocol where two parties agree on a shared secret key, without being able to determine the other party.
2. Pairing-based anonymous key agreement for V2X.
3. We use a pairing-based anonymous key agreement involving a private key generator (PKG)[3].
    1. PKG has its own master private and public key.
    2. PKG uses master secret key to generate secret keys for clients.
    3. Clients use this secret key to establish the shared secret key.
4. Clients can now create **psuedonyms** or fake identities $id \to (\mathcal{H}(id))^r, \mathcal{H} : \mathcal{ID} \to \mathcal{G}, r \in \mathbb{Z}_q$.

[3] Kate, Zaverucha, and Goldberg, "Pairing-Based Onion Routing".

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.

[4] Jan Camenisch et al. *Zone Encryption with Anonymous Authentication for V2V Communication*. 2020. URL: https://eprint.iacr.org/2020/043 (visited on 02/04/2024). preprint.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.
2. **Credential**: Data possessed by a user that demonstrates their attributes.

[4] Camenisch et al., *Zone Encryption with Anonymous Authentication for V2V Communication*.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.
2. **Credential**: Data possessed by a user that demonstrates their attributes.
3. **Anonymous Credential**: Data possessed by a user that demonstrates their attributes, *without revealing any additional information* about their identity.

[4] Camenisch et al., *Zone Encryption with Anonymous Authentication for V2V Communication*.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.
2. **Credential**: Data possessed by a user that demonstrates their attributes.
3. **Anonymous Credential**: Data possessed by a user that demonstrates their attributes, *without revealing any additional information* about their identity.
4. For V2X
   - Anonymous credentials issued to vehicles regularly.
   - We use DGSA (Digital Group Signatures with Attributes)[4], which gives us a **randomizable** group element as the credential $\sigma \to \sigma^r, r \in \mathbb{Z}_q$.

[4] Camenisch et al., *Zone Encryption with Anonymous Authentication for V2V Communication*.

Proposed Message Flow Diagram

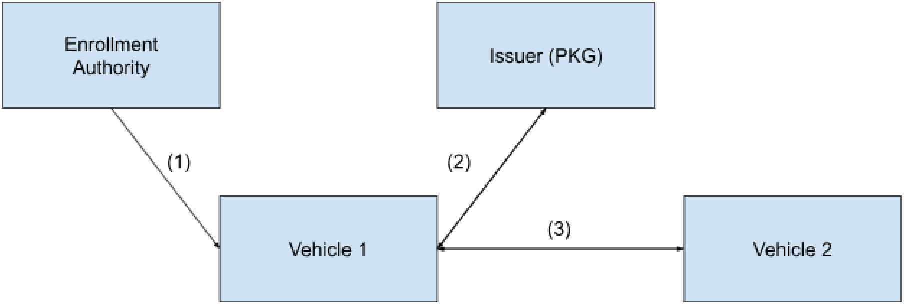

Figure 2: Message flow of the proposed scheme.

Proposed Message Flow

1. Enrollment authority issues certificate to vehicle.
    - Certificate is a long-term credential that can be used to revoke the holder in case of misbehaviour.

Proposed Message Flow

1. Enrollment authority issues certificate to vehicle.
    - Certificate is a long-term credential that can be used to revoke the holder in case of misbehaviour.
2. Issuer issues DGSA credentials and secret key after verifying certificate.
    - This secret key is different from secret key associated with certificate.
    - DGSA credentials guarantee authenticity.
    - Anonymous key agreement ensures that user identities remain anonymous throughout communication.
    - This is done periodically every *epoch*.

Proposed Message Flow

1. Enrollment authority issues certificate to vehicle.
    - Certificate is a long-term credential that can be used to revoke the holder in case of misbehaviour.
2. Issuer issues DGSA credentials and secret key after verifying certificate.
    - This secret key is different from secret key associated with certificate.
    - DGSA credentials guarantee authenticity.
    - Anonymous key agreement ensures that user identities remain anonymous throughout communication.
    - This is done periodically every *epoch*.
3. Vehicles exchange DGSA-signed randomized psuedonyms to generate shared key for futher communicaton.
    - Used in verifying legitimacy of the other party.

Analysis

1. **Advantages**
    - Fully anonymous communication, unlimited privacy between communicating parties.
    - Third parties cannot identify who is communicating.
    - Useful for sending extremely sensitive data.
    - Malicious vehicles can be revoked.

Analysis

1. **Advantages**
    - Fully anonymous communication, unlimited privacy between communicating parties.
    - Third parties cannot identify who is communicating.
    - Useful for sending extremely sensitive data.
    - Malicious vehicles can be revoked.
2. **Disadvantages**
    - Lots of pairing computations, for DGSA and for anonymous key agreement. Incurs computational overheads.
    - Works for single-hop connections only.
    - May not be scalable to communicating with many vehicles simultaneously in terms of storage overhead.

Future Work

1. Encrypt V2X messages like CAMs.

[5] Camenisch et al., *Zone Encryption with Anonymous Authentication for V2V Communication*.

[6] Xiaohan Yue et al. "A Practical Privacy-Preserving Communication Scheme for CAMs in C-ITS". In: *Journal of Information Security and Applications* 65 (Mar. 1, 2022), p. 103103. ISSN: 2214-2126. DOI: 10.1016/j.jisa.2021.103103. URL: https://www.sciencedirect.com/science/article/pii/S2214212621002799 (visited on 04/29/2024).

Future Work

1. Encrypt V2X messages like CAMs.
2. Improve efficiency of the present work.
    - Use one of DGSA or anonymous key agreement, but not both?

[5] Camenisch et al., *Zone Encryption with Anonymous Authentication for V2V Communication*.

[6] Yue et al., "A Practical Privacy-Preserving Communication Scheme for CAMs in C-ITS".

Future Work

1. Encrypt V2X messages like CAMs.
2. Improve efficiency of the present work.
   - Use one of DGSA or anonymous key agreement, but not both?
3. A new workflow for encryption using zones[5] and zone managers[6]

[5] Camenisch et al., *Zone Encryption with Anonymous Authentication for V2V Communication*.

[6] Yue et al., "A Practical Privacy-Preserving Communication Scheme for CAMs in C-ITS".