Anonymous Key Agreements for V2X Communication

Gautam Singh

Indian Institute of Technology Hyderabad

May 1, 2024

V2X Related Terminology

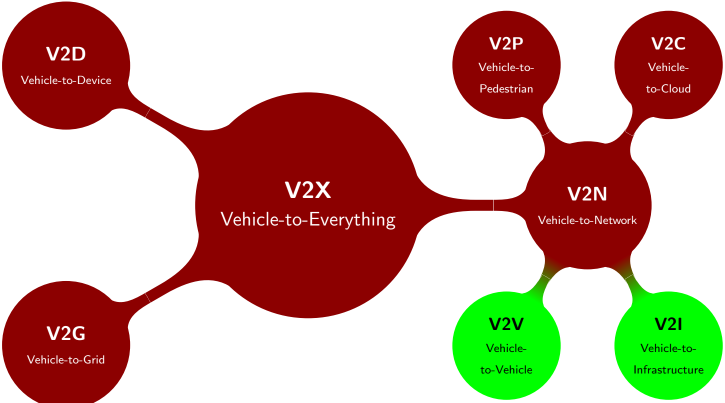

Figure 1: A breakdown of V2X.

Motivation and Goals

1. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2]
    - Include status information such as time, position, speed, active systems, vehicle dimensions, etc.
    - Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).

[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).

Motivation and Goals

1. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2]
   - Include status information such as time, position, speed, active systems, vehicle dimensions, etc.
   - Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
   - **Huge privacy concerns and threats!**
   - Most works focus on protecting/encrypting these.

[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. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2]
   - Include status information such as time, position, speed, active systems, vehicle dimensions, etc.
   - Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
   - **Huge privacy concerns and threats!**
   - Most works focus on protecting/encrypting these.
2. Do we *really* need to encrypt CAMs?
   - Google (Maps) may already be profiling us!
   - Focus on encrypting more sensitive messages.

[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. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2]
    - Include status information such as time, position, speed, active systems, vehicle dimensions, etc.
    - Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    - **Huge privacy concerns and threats!**
    - Most works focus on protecting/encrypting these.
2. Do we *really* need to encrypt CAMs?
    - Google (Maps) may already be profiling us!
    - Focus on encrypting more sensitive messages.
3. Unlimited privacy for vehicles.

[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. **Cooperative Awareness Messages** (CAMs)[1] and **Basic Safety Messages** (BSMs)[2]
    - Include status information such as time, position, speed, active systems, vehicle dimensions, etc.
    - Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    - **Huge privacy concerns and threats!**
    - Most works focus on protecting/encrypting these.
2. Do we *really* need to encrypt CAMs?
    - Google (Maps) may already be profiling us!
    - Focus on encrypting more sensitive messages.
3. Unlimited privacy for vehicles.
4. Better security guarantees (authenticity, confidentiality).

[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*.

Pairings

Definition 1 (Pairing[a])

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

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 $\mathbb{G}_T$.

Pairings

Definition 1 (Pairing[a])

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

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 $\mathbb{G}_T$.

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])

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

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 $\mathbb{G}_T$.

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 involving a private key generator (PKG)[3], which has master keypair (mpk, msk).

[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 involving a private key generator (PKG)[3], which has master keypair (mpk, msk).
3. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a symmetric pairing, where $\mathbb{G} = \langle g \rangle, \mathbb{G}_T$ are cyclic groups of order q. Suppose $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$ is a hash function.

[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 involving a private key generator (PKG)[3], which has master keypair (mpk, msk).
3. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a symmetric pairing, where $\mathbb{G} = \langle g \rangle, \mathbb{G}_T$ are cyclic groups of order q. Suppose $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$ is a hash function.
4. Setup (1^λ)
   1. $s \in_R \mathbb{Z}_q$
   2. Return $msk = s, mpk = g^s$

[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 involving a private key generator (PKG)[3], which has master keypair (mpk, msk).
3. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a symmetric pairing, where $\mathbb{G} = \langle g \rangle, \mathbb{G}_T$ are cyclic groups of order q. Suppose $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$ is a hash function.
4. Setup (1^λ)
    1. $s \in_R \mathbb{Z}_q$
    2. Return $msk = s, mpk = g^s$
5. Issue (id): Issue secret key for user id.
    1. Return $sk_{id} = (\mathcal{H}(id))^{msk}$ to id.

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

Anonymous Key Agreement

1. KeyExchange(id)
    1. Select $r \in_R \mathbb{Z}_q$
    2. Broadcast *psuedonym* $P_{id} \leftarrow (\mathcal{H}(id))^r$.
    3. On receiving $P_{id'}$, return $k \leftarrow e(sk_{id}^r, P_{id'})$.

Anonymous Key Agreement

1. KeyExchange (id)
   1. Select $r \in_R \mathbb{Z}_q$
   2. Broadcast *psuedonym* $P_{id} \leftarrow \left(\mathcal{H}\left(id\right)\right)^r$.
   3. On receiving $P_{id'}$, return $k \leftarrow e\left(sk_{id}^r, P_{id'}\right)$.
2. k is the shared secret key, since

$$e\left(sk_{id}^r, P_{id'}\right) = e\left(\left(\mathcal{H}\left(id\right)\right)^{sr}, \left(\mathcal{H}\left(id'\right)\right)^{r'}\right) = e\left(\mathcal{H}\left(id\right), \mathcal{H}\left(id'\right)\right)^{srr'} \tag{3}$$

Anonymous Key Agreement

1. KeyExchange (id)
    1. Select $r \in_R \mathbb{Z}_q$
    2. Broadcast *psuedonym* $P_{id} \leftarrow (\mathcal{H}(id))^r$.
    3. On receiving $P_{id'}$, return $k \leftarrow e\left(sk_{id}^r, P_{id'}\right)$.
2. k is the shared secret key, since

$$e\left(sk_{id}^r, P_{id'}\right) = e\left((\mathcal{H}(id))^{sr}, \left(\mathcal{H}\left(id'\right)\right)^{r'}\right) = e\left(\mathcal{H}(id), \mathcal{H}\left(id'\right)\right)^{srr'} \tag{3}$$

3. Hardness assumption: *Bilinear Diffie-Hellman Assumption*.
    - Given g^a, g^b, g^c, it is hard to compute $e(g, g)^{abc}$.

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 (Dynamic 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

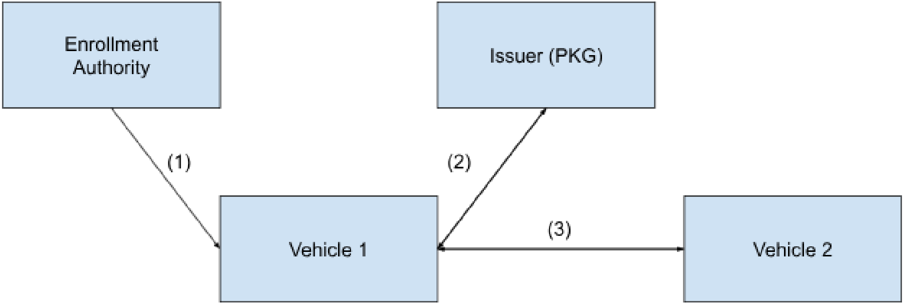

Figure 2: Message flow of the proposed scheme.

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".