Lightweight Privacy Preserving Authentication and Encryption Scheme for V2X

No Author Given

No Institute Given

Abstract. Vehicle-to-everything (V2X) has attracted much attention recently as it is a key component in Cooperative Intelligent Transportation Systems (C-ITS). V2X vehicles rely on continuous transmission of on-road traffic information via Cooperative Awareness Messages (CAMs) to provide efficient solutions for traffic management, autonomous driving, road safety, etc. Authentication of vehicles is key here as communication occurs over open insecure networks. At the same time, vehicles do not want to get profiled for it could reveal private details like location, etc and eventually lead to identifying the user. The bandwidth constraint of 300 bytes in C-ITS recommendations for CAMs makes many conventional authentication schemes impractical for V2X. These conflicting requirements between efficiency, privacy, security and authentication makes V2X deployment challenging.
Here we propose a bilinear pairing-based privacy-preserving authentication and encryption mechanism fine-tuned to satisfy V2X constraints. The authentication scheme is based on randomizable signatures and allows the vehicles to get authenticated by the roadside units (RSUs) in their corresponding zones, anonymously. Once a vehicle is authenticated, it derives a symmetric key with the help of the RSU and communicates with its adjacent peers using CAMs encrypted using that key. The anonymous authentication of the vehicle and the encryption of CAMs strengthen the privacy guarantees. As only authenticated vehicles have the valid secret key, we avoid authenticating every outgoing CAM making the scheme efficient. The proposed instantiation provides multi-use credentials with negligible download-and-storage costs, constant-size ciphertexts with a fixed overhead of 40 bytes at a 128-bit security level.

Keywords: Pairing-based cryptography · Randomizable signatures · Privacy preserving authentication· V2X.

1 Introduction

Vehicle-to-everything (V2X) is a new generation of information and communication technology (ICT) that enables vehicles to communicate with adjacent peers and roadside infrastructures and is becoming increasingly important as the world is progressing towards autonomous driving. It not only provides a safer and more efficient transportation environment but also substantially improves traffic efficiency, lowers pollution and accident rates by 80% [30].

In V2X, vehicles communicate through two types of messages : 1) periodic beacon messages referred to as Cooperative Awareness Messages (CAMs) containing information like geographical location, speed, vehicle dimensions, etc., and 2) event-triggered safety messages like emergency braking. Vehicles frequently transmit authenticated CAMs across open wireless networks, making vehicle/user authentication critical in V2X to assure message authenticity. Simultaneously, the vehicles should not be tracked from these messages as this could reveal personal information such as the user's location or travel routines or even their identity. As a result, we require authentication mechanisms that allow us to authenticate users anonymously without revealing any personally identifiable information of the user.

Leading standardization bodies such as the European Telecommunications Standards Institute (ETSI) and the U.S. Department of Transportation (USDOT) use pseudonym certificates for anonymous authentication in V2X [7, 35]. In pseudonym-based mechanisms, every vehicle owns a pool of pseudonyms and it authenticates the messages by signing them with different pseudonyms from the pool [16,18,36]. Pseudonym certificates are short-lived certificates and changing them facilitates the vehicle to avoid getting tracked over an extended period. There are a few hybrid schemes [1, 33] which combine various authentication approaches, such as hash functions, message authentication codes (MACs) and group signatures [6], along with pseudonyms but they do not preserve anonymity completely [3]. Although pseudonym-based mechanisms offer protection against eavesdropping adversaries, they are ineffective against colluding adversaries and malicious infrastructure. They also come with additional storage or download costs. Despite this, pseudonyms still continue to be extensively used because they are relatively lightweight and faster than other complex authentication techniques that provide stronger anonymity guarantees.

Another privacy issue in V2X is the transmission of authenticated messages (CAMs) in plaintext [9]. These are easy to intercept and can potentially leak sensitive information about the users' whereabouts. The frequency by which vehicles broadcast CAMs and static information like vehicle dimensions, etc present in the CAMs makes it easier for an attacker to correlate messages coming from a specific vehicle over an extended period, regardless of how often it changes its pseudonyms [17, 37]. It is also challenging to identify and locate eavesdropping devices in V2X, making it difficult to prevent the misuse of plaintext CAMs [2]. One immediate solution to provide confidentiality is to encrypt CAMs. However, encryption of CAMs in V2X is not straightforward [9] and rather challenging due to the open nature of C-ITSs and the complexity of managing encryption keys among continuously changing groups of vehicles.

Contributions. We propose a privacy-preserving authentication and encryption scheme tailored to V2X with more robust privacy and anonymity guarantees than pseudonym-based mechanisms. The scheme considers three main entities in the V2X environment: enrollment authority as issuer, vehicles as users, and roadside units (RSUs) as verifiers. The scheme also assumes that the V2X environment is geographically partitioned into zones based on the location of roadside units (RSUs). There are two main cryptographic primitives used in the scheme: (1) randomizable signatures [11, 28] and (2) symmetric-key authenticated encryption. The vehicles anonymously prove the possession of valid credentials issued to them by a trusted enrollment authority to a verifier (RSU) using randomizable signatures. The encrypted communication between vehicles provides confidentiality and prevents the misuse of plaintext CAM data. We describe below the two main components of our scheme.

1. **Anonymous Authentication.** A vehicle obtains a single long-term credential when it registers with a trusted issuing/enrollment authority. This long-term credential is a randomizable signature issued by an authority like the department of motor vehicles (DMV). The V2X environment is partitioned into several RSU zones. In order to communicate with other vehicles in a zone, a vehicle on the move must first authenticate itself to the RSU corresponding to that zone. For that the vehicle randomizes its long-term credential to generate a fresh short-term credential. The vehicle does this every time it enters a new zone and sends it to the RSU for authentication. Randomization helps preserve anonymity across different RSU zones. These credentials are unlinkable – no entity can link the randomized credentials across different zones or back to the original long term credential. As the vehicle itself manages its short-term credentials, it is impossible to identify the vehicle even if any entity colludes with the issuing authority. Our scheme is more efficient than other randomizable signatures because the authenticated encryption allows for fewer ZKPs as explained below.
2. **Symmetric key authenticated encryption.** After a vehicle is authenticated, the RSU ties an attribute to the vehicle's credential from which the vehicle derives the secret key for an encrypted communication session in that RSU zone. This key is specific to that zone. The knowledge of the vehicle's secret on which the long term credential is generated is required to derive a valid zone key. This gives us two performance benefits:
   (a) Unlike other randomizable signatures [11, 28], our scheme does not require the user to compute and present the ZKPoK of the secret corresponding to the long term credential explicitly during the authentication process with the RSU. If the vehicle does not have the secret it may still get (wrongfully) authenticated by the RSU but it will not be able to derive the zone key and therefore cannot communicate with any entity in that zone.
   (b) Since only an authenticated vehicle can derive the secret zone key required for communication, the vehicles do not have to authenticate every CAM message.

2 Related work

Pseudonym certificates allow vehicles to transmit messages without disclosing their true identities and are widely preferred for authentication of vehicles in

V2X communication primarily because of their efficiency. For instance, European ETSI [35,36] [39] and USDOT standards [7] for V2X employ ECDSA-based [20] pseudonym certificates as the principal mechanism for vehicle privacy. ECDSA is well suited for V2X due to its short signature sizes and efficient verification. Several pseudonyms management strategies have also been proposed in literature and Petit et al. [27] and ETSI [35] provide a detailed survey. They include those based on asymmetric cryptography and PKIs [21], group signature schemes [25, 34] symmetric cryptography [31], identity-based cryptography [14, 41], and privacy-preserving attribute-based credentials [26]. They differ in the trade-offs between security, privacy and efficiency. For example, a vehicle with a larger pool of pseudonyms offer better privacy but is more expensive to store/download and is less secure against Sybil attacks. An important trade-off w.r.t. privacy is that in most pseudonym-based mechanisms, the vehicle relies on a third party to obtain the pool of pseudonyms which means these mechanisms do not provide privacy from colluding or corrupt authorities [2].

One approach based on group signatures that provides privacy from colluding authorities is direct anonymous attestation (DAA) [8]. It allows vehicles to receive a blind signature on their long-term credential and get authenticated anonymously as a group member during transit. Even if the certificate authority is corrupt, DAA schemes [13, 19, 38] provide stronger privacy guarantees including unforgeability and unlinkability. However, the use of zero-knowledge proofs of knowledge (ZKPoKs) of signatures during the authentication process make such schemes computationally intensive. Chen et al. [13] proposes a DAA scheme that detects vehicles that abuse anonymity and has centralized revocation of credentials. However, it does not use efficient standards-compliant ECDSA signatures on broadcast messages which leads to high communication costs. Another DAA scheme by Hicks et al. [19] substitutes the long-term ECDSA certificates with DAA credentials. However, it still allows vehicles to send unlinkable requests for short-term ECDSA pseudonym certificates. The scheme allows for revocation and has features that prevent Sybil attacks. Although DAA-based techniques have several advantages, they have two major disadvantages: 1. they authenticate every broadcast message using a short-term pseudonym, and 2. the communication is in plaintext.

Camenisch et al. [9] highlights the need to encrypt CAMs in V2X not just for confidentiality but also for privacy. They propose a zone encryption scheme that builds upon dynamic group signatures with attributes. They use modified PS signatures [29] and prove security in the universal composability (UC) framework. They have an enrollment authority that issues long-term credentials to vehicles which is then used to obtain short-term certificates from the short-term credentials issuer. The scheme uses symmetric authenticated encryption with temporary keys shared between vehicles in the same proximity. Only key-exchange messages are signed with short-lived certificates, resulting in a significant efficiency benefit over previous methods that sign every outgoing CAM.

In contrast to these schemes, our scheme does not rely on a pseudonym authority to generate short-term credentials for a vehicle. Vehicle authenticity is linked to the secret zone key derivation enabling vehicles to communicate using encrypted messages rather than signed plaintext messages. The authenticated encryption enables our scheme to avoid the use of ZKPs making it more efficient.

3 Design Goals

The proposed scheme has the following salient features w.r.t. the state-of-the-art pseudonym-based mechanisms.

1. **Anonymous authentication.** We use randomizable signatures to generate credentials for the vehicles during enrollment. The unforgeability and unlinkability property of randomized signatures maintains the vehicle's anonymity.
2. **Collusion resistance.** The individual vehicles manage their short-term credentials, thereby shifting the trust from a pseudonym authority to the user. This protects the user's privacy even if the enrollment authority or the short term credentials issuer colludes with any other entity. The unlinkability of randomized signatures further enables the credential to have collusion resistance.
3. **Confidentiality.** In the proposed scheme, vehicles communicate through encrypted CAMs, thereby preventing the misuse of CAM data for profiling and mass surveillance.
4. **Efficiency.** The authentication of a vehicle is followed by the key derivation process, which requires a vehicle to have knowledge of its secret. This avoids the need for computationally intensive ZKPoKs for verifying the credentials. There is also no need to sign and authenticate every message using temporary certificates ensuring that confidentiality is provided with a minimal overhead of encrypted CAMs.

Our proposed scheme primarily focuses on anonymous authentication and confidentiality in V2X. Though we do not describe a revocation mechanism here, we believe that it can be done by employing a revocation authority and incorporating existing revocation mechanisms for anonymous credentials such as those that utilize dynamic accumulators [10].

4 Preliminaries

We introduce the notations and the cryptographic building blocks used in our scheme.

4.1 Notations

We use $a \overset{R}{\leftarrow} X$ to denote that a is chosen uniformly at random from a set X. We use $\mathbb{Z}_q$ to represent the group of integers modulo q and $\mathbb{Z}_q^*$ for the set $\mathbb{Z}_q \backslash \{0\}$.

4.2 Bilinear pairings

Let $G_1 = \langle g_1 \rangle, G_2 = \langle g_2 \rangle$ be two additive cyclic groups of prime order q and $\boldsymbol{G} = \langle \mathbf{g} \rangle$ be a multiplicative cyclic group of order q. A bilinear pairing is defined as an efficiently computable map $e : (G_1 \times G_2) \to \boldsymbol{G}$ satisfying the following properties:

1. Bilinearity: $\forall\, x, y \in \mathbb{Z}_q^*$, $P \in G_1$, $Q, Q_1, Q_2 \in G_2$, $e(xP, yQ) = e(P,Q)^{xy}$ and $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. Non-degeneracy: $e(g_1, g_2) \neq 1_{\boldsymbol{G}}$ i.e. $e(g_1, g_2)$ is a generator of $\boldsymbol{G}$.

Let $\mathcal{G}en(1^k)$ be a bilinear pairing group generator for the security parameter k and prime $q = \Theta(k)$. Let $(q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}) \overset{R}{\leftarrow} \mathcal{G}en(1^k)$ be the asymmetric bilinear pairing group parameters generated uniformly at random by $\mathcal{G}en(1^k)$. The proposed scheme works with Type-3 pairing groups. These are asymmetric pairing groups for which there is no known efficiently computable homomorphism from G_1 to G_2.

4.3 Hardness assumptions

This section introduces the hardness assumptions underlying our constructions.

Definition 1 (Co-computational Diffie-Hellman (Co-CDH) assumption [6]). *Given* $(q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}) \overset{R}{\leftarrow} \mathcal{G}en(1^k)$, g_1^x, g_2^y, *where* $x, y \overset{R}{\leftarrow} Z_q^*$, *for every PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\epsilon(k)$ *such that*

$$Pr\big[\mathcal{A}\big((q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}), g_1^x, g_2^y\big) \to g_1^{xy}\big] \leq \epsilon(k)$$

Definition 2 (Decisional Bilinear Diffie-Hellman (DBDH) assumption [12]). *Given* $(q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}) \overset{R}{\leftarrow} \mathcal{G}en(1^k)$, g_1^x, g_2^y, g_2^z, *where* $x, y, z \overset{R}{\leftarrow} Z_q^*$, *let* $D_0 = e(g_1, g_2)^{xyz}$ *and* $D_1 = e(g_1, g_2)^c$, *where* $c \overset{R}{\leftarrow} Z_q^*$, *for every PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\epsilon(k)$ *such that*

$$\big|Pr\big[\mathcal{A}\big((q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}), g_1^x, g_2^y, g_2^z, D_0\big) = 1\big] - \\ Pr\big[\mathcal{A}\big((q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}), g_1^x, g_2^y, g_2^z, D_1\big) = 1\big]\big| \leq \epsilon(k)$$

4.4 Randomizable signatures

Camenisch et al. [11] gave the first construction for randomizable signatures based on bilinear pairings. The most intriguing feature of these signatures is that given a randomizable signature σ on a message α, one can create another fresh valid signature σ' for α, indistinguishable from σ by raising σ to a scalar r. They enable the construction of various privacy-preserving constructions such as group signatures, anonymous credentials, aggregate signatures, etc. Generally, in these applications, a user obtains a signature σ on some secret s from an issuer and then prove to a verifier that the secret α is certified by an issuer.

Also, every time the user proves possession of the certificate to a verifier, the proof remains unlinkable from all the previous times. A user can anonymously obtain this signature from the issuer by providing the commitment of the secret instead of the secret itself. In the CL signature scheme proposed by Camenisch et al. [11] user obtain a signature on the commitment of the secret, randomizes the signature and proves the knowledge on the committed secret in zero-knowledge. No adversary can forge the user's credentials due to the unforgeability property of the signature, which follows from the LRSW assumption [24]. PS signatures [28] is another such randomizable signature scheme in type-3 pairing setting.

In our proposed scheme, the long-term credential of the vehicle is randomizable which helps the vehicle in generating the short-term credential for authentication with the RSU. However, our authentication does not require proving knowledge of the signature on the secret using ZKPoK. We argue that the knowledge of the secret is implicit in the proposed authentication mechanism since a vehicle cannot generate a valid secret key required for further communication without it.

5 Proposed Scheme

We present the construction of our privacy-preserving authentication scheme and provide formal proofs of its security. The scheme allows vehicles to get authenticated anonymously by RSUs using randomized credentials. In Section 5.1 we show how the credential of the vehicle is obtained as a randomized signature on the commitment of its secrets. The RSU then ties an attribute to the randomized credential of an authenticated vehicle which helps the vehicle to derive a secret key to communicate with other vehicles that are in the same RSU zone. This key generation mechanism is defined in Section 5.2. The authenticated vehicles within the same RSU zone communicate using a CCA-secure authenticated encryption scheme which is defined in Section 5.3.

5.1 Authentication Mechanism

A vehicle obtains a long-term randomizable signature on the commitments of its secrets $\alpha, \beta \in \mathbb{Z}_q^\star$ while registering itself with an enrollment authority (issuer). The vehicle sends the request as commitments of the secrets, $(a = g_1^\beta, a^\alpha)$ to the authority and obtains the randomizable signature σ as described below. We also define the **Verify** algorithm that verifies the credential.

- **Setup** $\mathcal{S}(1^k)$: Given security parameter k, output the type-3 bilinear pairing parameters $(e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}) \overset{R}{\leftarrow} \mathcal{G}en(1^k)$.
- **Keygen** $\mathcal{K}(1^k)$: The enrollment authority/issuer generates $sk = (x, y) \overset{R}{\leftarrow} Z_q^\star$ as its secret keys and publishes $pk = (X = g_2^x, Y = g_2^y)$ as its public keys.

  The user generates $(\alpha, \beta) \overset{R}{\leftarrow} Z_q^\star$ as its secrets and sends $req = (a = g_1^\beta, b = a^\alpha)$ to the issuer for obtaining the credential.

- **GenCred** $\mathcal{G}(sk, req)$: The issuer verifies the vehicle and uses its secret keys to compute $c = a^x, d = (a^\alpha \cdot c)^y = a^{y(\alpha+x)}$ and outputs the signature $\sigma = (a, b, c, d)$.
- **Verify** $\mathcal{V}(\sigma, pk)$: This algorithm takes the public keys of the issuer and credential of the user as input and verifies whether $e(a, X) \overset{?}{=} e(c, g_2)$ and $e(d, g_2) \overset{?}{=} e(b \cdot c, Y)$ are satisfied. On successful verification it outputs 1 (accept), else 0 (reject).

Correctness. This property ensures that the credentials obtained by the above mechanism are correctly verifiable. If $\sigma = \big(a, b = a^\alpha, c = a^x, d = a^{y(\alpha+x)}\big)$, then substituting the values in the verification equations gives,

$$\begin{aligned} e(a, X) &\overset{?}{=} e(c = a^x, g_2) \\ &= e(a, g_2^x) \\ &= e(a, X), \end{aligned}$$

and

$$\begin{aligned} e(d = a^{y(\alpha+x)}, g_2) &\overset{?}{=} e(b \cdot c, Y) \\ e(a, g_2)^{y(\alpha+x)} &= e(a^\alpha \cdot a^x, g_2^y) \\ &= e(a, g_2)^{y(\alpha+x)}. \end{aligned}$$

Randomizability and Unlinkability. The credential σ can be randomized by selecting $r \overset{R}{\leftarrow} \mathbb{Z}_q^\star$ and computing $\overline{\sigma} = (a^r, b^r, c^r, d^r)$ which is still a valid credential but unlinkable from σ. The verification equations satisfy as follows,

$$\begin{aligned} e(a^r, X) &\overset{?}{=} e(c^r, g_2) \\ e(a, X)^r &\overset{?}{=} e(c, g_2)^r \end{aligned}$$

and

$$\begin{aligned} e(d^r, g_2) &\overset{?}{=} e(b^r \cdot c^r, Y) \\ e(d, g_2)^r &\overset{?}{=} e(b \cdot c, Y)^r. \end{aligned}$$

Unforgeability. This property captures the standard requirement of a secure credential scheme that only the enrollment authority/issuer can issue a valid credential for an input, i.e. no efficient adversary can forge a credential and authenticate itself as a valid user. We say that a credential scheme $(\mathcal{S}, \mathcal{K}, \mathcal{G}, \mathcal{V})$ is unforgeable if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the $\mathbf{Exp}^{\mathbf{unforgeable}}_{\mathcal{O}_{(a,b)}, \mathcal{V}, \mathcal{Q}, k}(\mathcal{A})$ experiment defined as follows.

Experiment $\mathbf{Exp}^{\mathbf{unforgeable}}_{\mathcal{O}_{(a,b)},\mathcal{V},\mathcal{Q},k}(\mathcal{A})$. Let $(q, e, g_1, g_2, G_1, G_2, \mathbf{g}, \mathbf{G})$ be a type 3 bilinear pairing group with $g_1 \in G_1, g_2 \in G_2$, and $\mathbf{g} \in \mathbf{G}$. For the public key parameters $(X = g_2^x, Y = g_2^y)$ where x and y are random scalars in $\mathbb{Z}_q$, consider an oracle $\mathcal{O}(a, b)$ that on input $(a, b = a^\alpha) \in G_1$ where $\alpha \in \mathbb{Z}_q$, outputs the credential $\sigma = (a, b, c = a^x, d = a^{y(\alpha+x)})$. Given (g_1, g_2, X, Y) and unlimited access to this oracle and $\mathcal{Q}$ the set of queries made to $\mathcal{O}$, the goal of the adversary is to efficiently generate a valid credential $\sigma^\star$ for a new input $(\alpha^\star, \beta^\star) \in \mathbb{Z}_q$ such that $(a^\star = g_1^{\beta^\star}, b^\star = (a^\star)^{\alpha^\star}) \notin \mathcal{Q}$. We define the advantage of the adversary $\mathcal{A}$ in attacking the scheme as:

$$\mathrm{Adv}(\mathcal{A}) = |\Pr[\mathcal{V}(pk, \sigma') = 1]| = \epsilon(k).$$

Theorem 1. *The credential scheme $(\mathcal{S}, \mathcal{K}, \mathcal{G}, \mathcal{V})$ is unforgeable, assuming co-CDH is hard for given type-3 pairing parameters. Concretely, suppose there is an adversary $\mathcal{A}$ with $\mathrm{Adv}(\mathcal{A}) = \epsilon(k)$, where $\epsilon(k)$ is non-negligible, then there is an algorithm $\mathcal{B}$ that can solve co-CDH for given type-3 pairing parameters with non-negligible advantage.*

Proof. Algorithm $\mathcal{B}$ generates $(a = g_1^{\overline{r}}, b = a^r)$ where $r, \overline{r} \in \mathbb{Z}_q^*$ to obtain credentials $\sigma = (a, b, c = a^x, d = a^{y(x+r)})$ from $\mathcal{O}$. Algorithm $\mathcal{B}$ is given the co-CDH parameters as input: a type-3 pairing group $(q, e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G})$ and a random instance $(U = g_1^u, V = g_2^v)$ of the co-CDH problem for these parameters. Algorithm $\mathcal{B}$ has to output $g_1^{u \cdot v}$ to solve the co-CDH problem and it does so by interacting with $\mathcal{A}$ as follows:

1. $\mathcal{B}'s$ view of $(U = g_1^u, V = g_2^v)$ is equivalent to $(U^\star = g_1^{x+\alpha^\star}, V^\star = Y = g_2^y)$, where $\alpha^\star \in \mathbb{Z}_q^\star$, i.e. the advantage of $\mathcal{B}$ is same as when generating g_1^{uv} or $g_1^{y(x+\alpha^\star)}$ provided $\mathcal{B}$ does not have access to $\mathcal{O}$ after generating $\alpha^\star$.
2. $\mathcal{B}$ computes the input $(a^\star = g_1, b^\star = g_1^{\alpha^\star})$.
3. $\mathcal{B}$ invokes $\mathcal{A}$ to forge credentials on $(a^\star, b^\star)$.
4. The adversary $\mathcal{A}$ outputs the credential $\sigma^\star = (a, b, c^\star = g_1^x, d^\star = g_1^{y(x+\alpha^\star)})$ with advantage $\epsilon(k)$ and $\mathcal{B}$ outputs $d^\star = g_1^{y(x+\alpha^\star)}$ as the solution of the co-CDH problem.

5.2 Key Generation Mechanism

The mechanism allows the authenticated vehicles to establish a symmetric key k_v with the help of the RSU for encrypted communication.

- **Keygen** $\mathcal{K}(1^k, c = a^x)$: The key issuing authority generates attribute $v \overset{R}{\leftarrow} \mathbb{Z}_q^\star$. The authority adds the attribute v to the credential σ by updating c to $c' = c^v$ and returns it to the user. The commitment $V = g_1^v$ is also published for verification of the derived key.
- **Derive** $\mathcal{D}(c', \beta)$: This algorithm derives the symmetric key g_1^{xv} as follows: $(c')^{\beta^{-1}} (= (a^{xv})^{\beta^{-1}} = (g_1^{\beta xv})^{\beta^{-1}} = g_1^{xv})$.

- **Verify** $\mathcal{V}(V, X, g_1^{xv})$: This algorithm verifies whether $e(V = g_1^v, X = g_2^x) \overset{?}{=} e(g_1^{xv}, g_2)$ is satisfied. It ouputs 1 if successful else 0.

Security Analysis. Only authenticated users can derive the key g_1^{xv}. The parameter of key-generation mechanism, $(V = g_1^v, X = g_2^x)$ can be mapped to a co-CDH instance $(U = g_1^u, V = g_2^v)$ and the problem of forging key g_1^{xv} is then as hard as solving the corresponding co-CDH problem, g_1^{uv}.

5.3 Encryption Scheme

This section explains the proposed symmetric key encryption scheme through which vehicles communicate with each other. First, we propose a CPA-secure encryption scheme and then we convert this scheme into an authenticated encryption scheme that is CCA-secure for a strongly unforgeable MAC.

CPA secure encryption scheme

- **Setup** $\mathcal{S}(1^k)$: Execute the key-generation mechanism $(\mathcal{K}, \mathcal{D}, \mathcal{V})$ to generate the secret key $k_v = g_1^{xv} = g_1^{\gamma}$. The public parameters are $(e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G})$ and $(X = g_2^x, V = g_1^v)$.
- **Encrypt** $\mathcal{E}(M)$: To encrypt the message $M \in \boldsymbol{G}$, we do the following:
  - Select a random $r \in Z_q$ and compute $h = g_2^r$.
  - Compute $w = e(k_v, h)$.
  - Set the ciphertext to be

$$C = (M \cdot e(k_v, h), h).$$

- **Decrypt** $\mathcal{D}(C)$: To decrypt the ciphertext $C = (M \cdot e(k_v, h), h)$, do the following:
  - Compute $w = e(k_v, h)$.
  - Compute $M = \frac{C}{w}$.

The CPA-security of an encryption scheme is formalised by a CPA indistinguishability game (IND-CPA). It is the weakest acceptable notion of security for a symmetric encryption scheme [4]. The CPA security of the above encryption scheme relies on the hardness of the DBDH assumption. We formally define the CPA indistinguishability experiment *IND-CPA* and prove that the hardness of winning the *IND-CPA* game is equivalent to solving a DBDH instance.

Definition 3 (*Chosen plaintext security*). *We say that a symmetric encryption scheme $\pi = (\mathcal{S}, \mathcal{E}, \mathcal{D})$ is semantically secure against an adaptive chosen plaintext attack if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage against the challenger $\mathcal{C}$ in the following game:*

Setup : The challenger takes a security parameter and runs the setup algorithm $\mathcal{S}$ and gives the resulting system parameters $(e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G}, X, V)$ to the adversary. It keeps the secret key k_v to itself.
Query : The adversary issues queries $q_1, \ldots, q_m$, where query q_i is an encryption query of the message M_i. The challenger responds by running algorithm $\mathcal{E}$ to generate the ciphertext C_i using the secret key k_v and the message M_i as inputs. It sends C_i to the adversary. These queries may be asked adaptively, that is, the query q_i may depend on the replies to $q_1, \ldots, q_{i-1}$.
Challenge : The adversary outputs two plaintexts $M_0, M_1 \in \mathbf{G}$. The challenger picks a random bit $b \in \{0, 1\}$ and runs the algorithm $\mathcal{E}$ with the secret key k_v and message M_b as inputs to generate the ciphertext C_b. It sends C_b as the challenge to the adversary. The adversary can again make queries to the challenger after the challenge is issued.
Guess : The adversary $\mathcal{A}$ recieves the challenge ciphertext and outputs a bit b'. $\mathcal{A}$ wins the game if he correctly guesses the bit b i.e. $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-CPA adversary. We define the advantage of the adversary $\mathcal{A}$ in attacking the scheme as:

$$\mathrm{Adv}(\mathcal{A}) = |\Pr[b = b'] - \frac{1}{2}|$$

We now show that the proposed encryption scheme $\mathit{\Pi} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure as long as the DBDH assumption holds for the underlying type-3 bilinear pairing group. Intuitively, DBDH assumption says that $e(g_1, g_2)^{pqt}$ is pseudorandom given g_1^p, g_2^q, g_2^t, so masking the message M with $e(g_1, g_2)^{pqt}$ is as good as masking it with a truly random $e(g_1, g_2)^s$, $s \leftarrow \mathbb{Z}_q$.

Theorem 2. *The symmetric encryption scheme $\mathit{\Pi} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is semantically secure (IND-CPA) assuming DBDH is hard in $\boldsymbol{G}$. Concretely, suppose there is an IND-CPA adversary $\mathcal{A}$ that has an advantage $\mathrm{Adv}(\mathcal{A}) = \epsilon(k)$ where $\epsilon(k)$ is non-negligible, then there is an algorithm $\mathcal{B}$ that can solve DBDH in $\boldsymbol{G}$ with non-negligible probability.*

Proof. Generate a type-3 bilinear pairing group $(e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \mathbf{G})$, select a bit $b'' \in \{0, 1\}$ uniformly at random and give the algorithm $\mathcal{B}$ the following *DBDH* instance as input – $\left(g_1^p, g_2^q, g_2^t, Q_{b''}\right)$, where $p, q, t, s \overset{R}{\leftarrow} \mathbb{Z}_q^*$, $Q_0 = e(g_1, g_2)^{pqt}$ and $Q_1 = e(g_1, g_2)^s$. The goal of the algorithm $\mathcal{B}$ is to solve the DBDH problem with non-negligible probability. The algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in the IND-CPA game as follows ($\mathcal{B}$ simulates the challenger for $\mathcal{A}$):
Setup : The challenger $\mathcal{B}$ takes the security parameter and runs the setup algorithm $\mathcal{S}$. It gives the adversary, the resulting system parameters $(e, g_1, g_2, \boldsymbol{g}, G_1, G_2, \boldsymbol{G})$.
Query : The adversary $\mathcal{A}$ issues queries $q_1, \ldots, q_m$ to the challenger $\mathcal{B}$, where query q_i is the encryption query of message M_i. The algorithm $\mathcal{B}$ responds by running algorithm $\mathcal{E}$ to generate the ciphertext C_i using the secret key $k_i = Q_{b''}$ and message M_i as inputs. It sends $C_i = (M_i \cdot k_i, g_2^t)$ to the adversary. The adversary can make adaptive queries i.e., each query q_i may depend on the replies

to $q_1, \ldots, q_{i-1}$.
Challenge : The adversary $\mathcal{A}$ outputs two plaintexts $M_0, M_1 \in \mathbf{G}$. The algorithm $\mathcal{B}$ picks a random bit $\overline{b} \in \{0,1\}$ to generate the ciphertext $(C_{\overline{b}} = M_{\overline{b}} \cdot Q_{b''}, g_2^t)$. It sends $C_{\overline{b}}$ as the challenge to the adversary. The adversary can make more queries to the challenger after the challenge is issued. The adversary replies with its guess $\overline{b}'$ at the end of the game.
Analysis. If the adversary $\mathcal{A}$ wins the IND-CPA game i.e. $\overline{b}' = \overline{b}$ with non-negligible advantage, then the algorithm $\mathcal{B}$ can also correctly guess the bit b'' with non-negligible advantage using $\mathcal{A}$.

1. If $b'' = 0$, then $\mathcal{B}$'s response in the challenge phase $(M_{\overline{b}} \cdot e(g_1, g_2)^{pqt}, g_2^t)$ has the same distribution as the ciphertexts of $M_{\overline{b}}$ in the proposed encryption scheme, so we perfectly simulate the IND-CPA game with $\mathcal{B}$. Therefore, the advantage of $\mathcal{B}$ to output the correct guess for bit b'' is equivalent to the adversary $\mathcal{A}$'s advantage of winning the IND-CPA game.
2. If $b'' = 1$ then $\mathcal{B}$'s response in the challenge phase $(M_{\overline{b}} \cdot e(g_1, g_2)^s, g_2^t)$ is distributed uniformly at random and is independent of the actual encryption. This implies the probability of $\mathcal{B}$ as well as $\mathcal{A}$ winning their respective games is negligible.

Conclusion. The parameters of the DBDH instance, $(g_1^p, g_2^q, g_2^t, Q_b = e(g_1, g_2)^{pqt})$ or $(g_1^p, g_2^q, g_2^t, Q_{b''} = e(g_1, e(g_1, g_2)^s)$ can be mapped to the encryption scheme parameter, $(V = g_1^v, X = g_2^x, h = g_2^r, k = e(g_1, g_2)^{xvr})$. Any adversary $\mathcal{A}$ that can break the IND-CPA of the encryption scheme $(\mathcal{S}, \mathcal{E}, \mathcal{D})$ with an advantage $\epsilon(k)$ has the same advantage when solving the DBDH problem. Thus, under the assumption that the DBDH problem is hard w.r.t. the type-3 bilinear pairing group, the encryption scheme $\mathit{\Pi} = (\mathcal{S}, \mathcal{E}, \mathcal{D})$ is CPA-secure.

CCA secure encryption scheme The below theorem implies that any encryption scheme that is both IND-CPA secure and INT-CTXT secure is also IND-CCA secure. INT-CTXT requires that it should be computationally infeasible to produce a ciphertext not previously produced by the sender, regardless of whether or not the underlying plaintext is "new".

Theorem 3. *[4, Theorem.3.1] Let $\mathit{\Pi} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $\mathcal{A}$ be an IND-CCA adversary against $\mathit{\Pi}$ running in time t and making q_e* ***Enc*** *queries and q_d* ***Dec*** *queries. Then we can construct an INT-CTXT adversary $\mathcal{A}_c$ and an IND-CPA adversary $\mathcal{A}_p$ such that*

$$\boldsymbol{Adv}_{\mathit{\Pi}}^{\text{IND-CCA}}(\mathcal{A}) \leq 2 \cdot \boldsymbol{Adv}_{\mathit{\Pi}}^{\text{IND-CTXT}}(\mathcal{A}_c) + \boldsymbol{Adv}_{\mathit{\Pi}}^{\text{IND-CPA}}(\mathcal{A}_p)$$

That is, IND-CPA $\wedge$ INT-CTXT $\rightarrow$ IND-CCA. We propose a SUF-CMA secure message authentication scheme to achieve INT-CTXT (integrity of ciphertexts).

- **Setup** $(\mathcal{S})$: Generate system parameters (g_1, G_1). Choose $a, b \in Z_q^\star$ and set $\gamma = ab$ and the secret key $k = g_1^{ab} = g_1^{\gamma}$. Let $H : G_1 \rightarrow \mathbb{Z}_q^\star$ be a hash function.

- **GenMac**($\mathcal{GM}$): To generate the MAC of the message $M \in \mathbb{Z}_q^\star$, do the following:
  1. Select a random $\overline{r} \in \mathbb{Z}_q$ and compute $k^{\overline{r}} = g_1^{\gamma \cdot \overline{r}}$.
  2. Compute the MAC as $\tau = H(M \cdot k^{\overline{r}})$.
  3. Send the output as $(M, \tau, \overline{r})$.
- **VerifyMac**($\mathcal{VM}$): To verify the MAC $(M, \tau, \overline{r})$, do the following:
  1. Compute the key $k^{\overline{r}}$.
  2. Compute $\tau' = H(M \cdot k^{\overline{r}})$.
  3. Verify whether $\tau' \overset{?}{=} \tau$. Return 1 if true, else 0.

The experiment $\mathbf{Exp}^{\text{SUF-CMA}}_{\mathcal{O}_\tau, \mathcal{VM}, \mathcal{Q}}(\mathcal{A})$ given below captures the strong notion of unforgeability under chosen-message attacks where the adversary $\mathcal{A}$ only needs to forge a new message-tag pair which is not in the set of queries $\mathcal{Q}$ made to the oracle $\mathcal{O}_\tau$. For a given input message M, the oracle outputs the unique tag τ using its secret key k.
Experiment $\mathbf{Exp}^{\text{SUF-CMA}}_{\mathcal{O}_\tau, \mathcal{VM}, \mathcal{Q}}(\mathcal{A})$. Let G_1 be an additive group of prime order q with generator g_1 and $H : G_1 \to \mathbb{Z}_q^\star$ be a publicly available hash function. Consider an oracle $\mathcal{O}_\tau(\cdot)$ that generates a symmetric key $k = g_1^{ab}$ where a and b are random scalars in $\mathbb{Z}_q$. Given the input M, the oracle $\mathcal{O}_\tau(\cdot)$ generates the tag $\tau = H(M \cdot k^{\overline{r}})$, where $\overline{r} \xleftarrow{R} \mathbb{Z}_q$ and outputs $(M, \tau, \overline{r})$. Also, $\mathcal{O}_\tau$ stores the pair (M, τ) in its query set $\mathcal{Q}$. Given unlimited access to this oracle, the goal of the adversary is to efficiently generate a new message tag pair $(M', \tau') \notin \mathcal{Q}$ such that the **VerifyMac** algorithm, $\mathcal{VM}$ outputs 1 for the pair $(M', \tau', \overline{r}')$. We define the advantage of the adversary $\mathcal{A}$ in attacking the scheme as

$$\text{Adv}(\mathcal{A}) = |\Pr[\mathcal{VM}(M', \tau', \overline{r}') = 1]| = \epsilon(k).$$

Theorem 4. *The MAC scheme $\mathcal{M} = (\mathcal{S}, \mathcal{GM}, \mathcal{VM})$ is SUF-CMA secure assuming co-CDH is hard in G_1 and $H : G_1 \to \mathbb{Z}_q^\star$ is a collision-resistant and pre-image resistant hash function. Concretely, suppose there is an adversary $\mathcal{A}$ that has an advantage* $\text{Adv}(\mathcal{A}) = \epsilon(k)$ *against the MAC scheme $\mathcal{M} = (\mathcal{S}, \mathcal{GM}, \mathcal{VM})$ and $\epsilon(k)$ is non-negligible, then there is an algorithm $\mathcal{B}$ that can either break the security of the hash function or solve the co-CDH problem with non-negligible probability.*

Proof. Suppose that we have an adversary $\mathcal{A}$ who creates a valid forged tag with probability $\epsilon(k)$. Then we consider the following three scenarios.

1. With probability at least $\epsilon_1(k)$, the adversary $\mathcal{A}$ creates a new valid forged tag (M, τ', r') on some message M which was previously queried and the oracle had returned the output (M, τ, r) where $\tau \neq \tau'$. We refer to this type of forgery as "Type 1" and the corresponding adversary as "Type-1 adversary".
2. With probability at least $\epsilon_2(k)$, the adversary $\mathcal{A}$ is able to forge a valid tag (M', τ, r) for a new message M' where (M, τ, r) was a previous reply of the oracle as a valid tag for a message M. We refer to this type of forgery as "Type 2" and the corresponding adversary as "Type-2 adversary".

3. With probability at least $\epsilon_3(k)$, the adversary $\mathcal{A}$ is able to forge a new message M with a valid tag (M, τ, r) where neither M has been queried nor (τ, r) has been generated as the tag for any message by the oracle. We refer to this type of forgery as "Type 3" and the corresponding adversary as "Type-3 adversary".

One of the above three must hold when we upper bound the sum of probabilities of different types of forgery to $\epsilon(k)$, i.e., $\epsilon_1(k) + \epsilon_2(k) + \epsilon_3(k) \leq \epsilon(k)$. Next we show that these type of forgeries either violate the security of the hash function H or contradicts the co-CDH assumption.

1. For type-1 forgery, the adversary needs to compute a tag $(\tau' = H(M \cdot k^{r'}), r')$ where it already has access to $(\tau = H(M \cdot k^r), r)$. If the adversary $\mathcal{A}$ can compute such a tag τ' with non-negligible probability, then there exists an algorithm $\mathcal{B}$ that can break the non-malleability of the hash function with non-negligible probability as well. Note that a hash function H is called non-malleable if for any PPT adversary $\mathcal{A}$, when provided with the input $y = H(x)$, the probability of computing $y^\star = H(x^\star)$, where there exist a non-trivial relation between x and $x^\star$, is negligible [5].
2. For type-2 forgery, the adversary needs to compute a message M' which when given to the oracle $\mathcal{O}_\tau$ returns (M', τ, r) such that previously, for some query message M the output of the oracle was (M, τ, r). If the adversary $\mathcal{A}$ can compute such a message M' with non-negligible probability, then clearly we can construct an algorithm $\mathcal{B}$ that can break the collision-resistance of the hash function with non-negligible probability as well.
3. For type-3 forgery, the adversary needs to come up with a new message M, not previously queried to the oracle, and its corresponding tag (M, τ, r). Given that type-1 and type-2 forgeries can be done only with negligible probability, type-3 forgery can only be done when the adversary $\mathcal{A}$ can forge the key k. We have shown in Section 5.2 that any adversary who can forge the key can break the co-CDH hardness assumption.

6 Experimental results

In this section, we describe the results of the secure instantiation of our scheme that satisfy the V2X environment constraints. We further compare our instantiation with pseudonyms, the current mechanism for privacy-preserving authentication as per ETSI and USDOT standards. The most critical operation in V2X is the signing and verification of broadcast messages for which ECDSA signature algorithm is mostly used. We propose an authenticated encryption scheme to replace this signature algorithm. This allows for encrypted communication between vehicles, increasing the cost of eavesdropping. This privacy guarantee comes at the cost of performance overhead of key distribution and encryption of messages. Table 1 shows the computational cost of deriving the key. We argue that the optimized handover algorithms [22, 23, 40], which are widely used in cellular communication to switch base stations with minimal disturbance, can minimize the key-derivation overhead. The computational cost of performing authenticated encryption is undoubtedly higher than a digital signature. However, in V2X, the more critical constraint is bandwidth, and our scheme generates an overhead of 40 bytes when SHA-256 is used, compared to ECDSA, which has a signature size of 64 bytes.

Curve Name	Sec. Lvl. (bits)	Latency (ms)
BN254	100	1.6454
BLS12-381	128	1.9129
BLS48-556	256	2.7268

Table 1. Latency of key derivation with various curves and their associated security levels

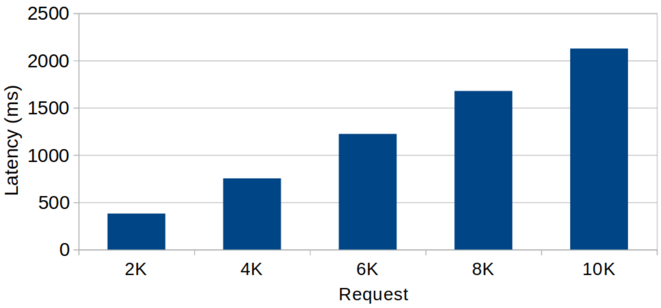

Fig. 1. Latency at the RSU for verifying authentication requests of the vehicles

Our scheme introduces an additional overhead compared to the current standards when the vehicle enters the RSU zone. This is because our protocol requires that the vehicle authenticate itself to the RSU using randomized credentials. Fig. 1 shows the throughput of a single RSU that verifies the vehicle's credential and also adds the required attributes to the credential for deriving the zone key. A single RSU can handle 10K requests with a latency of 2 seconds, which is a fair upper bound on the number of vehicles entering a zone. Fig. 1 shows that the increase in latency w.r.t the number of requests is almost linear and this means an RSU with a multi-core system can still handle a large number of requests with minimum delay. We acknowledge that an adversary can launch a DoS attack on the RSU, which can become a bottleneck in our scheme. The techniques for protection against DoS attacks are out-of-scope of this work. In Fig. 2, we compare pseudonyms and our scheme w.r.t. bandwidth overhead of a vehicle entering different RSU zones. To simulate the scenario, we use veins framework [32], which is a widely used simulator for V2X research, running over a single core of an Intel i7 processor. We used the realistic 24-hour scenario of Luxembourg city [15] for simulation.

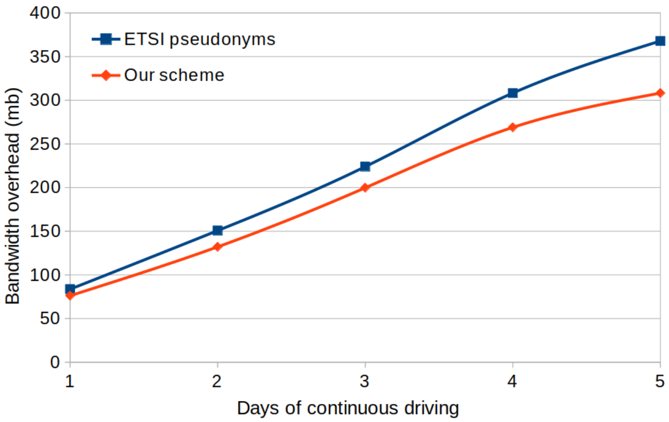

Fig. 2. Bandwidth overhead of vehicles when driving in Luxembourg

	PS	CL	Proposed
Signing Efficiency (Issuer)	2e	5e	2e
Signing Efficiency (User)	2e	2e	2e
Verification Efficiency (Verifier)	1p	5e+6p	2p
Verification Efficiency (User)	2e	4e	4e

Table 2. Comparison of randomizable signature schemes in terms of exponent and pairing-based operations where 'e' represents the former and 'p' the latter.

Table 2 represents a theoretical comparison between the randomized signatures of our scheme and other existing lightweight signatures. Though the proposed signature scheme has only almost the same efficiency as other randomizable signatures like PS signatures [28], it additionally facilitates secure key distribution, which PS signatures or even CL signatures [11], do not do. This is because in PS and CL signatures, the attribute 'a' of the credentials is selected by the issuer, whereas in our scheme '$a = g^{\beta}$' is the commitment of the secret chosen by each vehicle. This allows the vehicles to derive the zone key $k_v = g^{xv}$, where g is a public parameter. The Table 3 provides a cursory comparison between the proposed scheme, ETSI standards [35] and the zone encryption scheme by Camenisch et al. [9]

	Zone Encryption [9]	C-ITS Standards [35]	Proposed Scheme
Encrypted CAM	✓	✗	✓
Anonymity	✓	✗	✓
Pseudonyms Limit	Unlimited	20-100/Week	Unlimited
CAM Authentication	Authenticated Encryption	ECDSA	Authenticated Encryption
Overhead per CAM	224 bytes	64 bytes	40 bytes
Overhead per entered Zone	284 bytes	NA	32 bytes

Table 3. Comparison of proposed scheme with C-ITS standards and zone encryption at a 128-bit security level.

7 Conclusion

We present a privacy-preserving authentication scheme to enable anonymous authentication and resolve confidentiality issues in V2X. Firstly, the proposed authentication mechanism enables the vehicle to generate short-term unlinkable credentials with the help of a single long-term credential obtained from the issuer. It has a significant advantage over schemes with limited pseudonym pool sizes and expensive download and storage costs. Secondly, our encryption scheme allows for encrypted communication of CAM messages with a fixed overhead of 40 bytes, which is less than the current C-ITS proposals.

Despite these improvements, our scheme has the disadvantage that to communicate with other vehicles, a vehicle has to rely on an RSU for authentication and key derivation. The scheme also does not have a revocation mechanism to revoke the credentials of a misbehaving vehicle and stop it from getting authenticated. However, we believe that it can be integrated into our scheme by incorporating existing revocation mechanisms for anonymous credentials and this will be our future work.

References

1. Adrian, P., Ran, C., Tygar, J., Dawn, S.: The TESLA broadcast authentication protocol. RSA CryptoBytes **5**, 2002 (2002)
2. Article 29 Data Protection Working Party: Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS). Tech. Rep. (2017), ec.europa.eu/newsroom/article29/redirection/document/51025
3. Baee, M.A.R., Simpson, L., Boyen, X., Foo, E., Pieprzyk, J.: ALI: Anonymous Lightweight Inter-Vehicle Broadcast Authentication with Encryption. IEEE Transactions on Dependable and Secure Computing (2022)
4. Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Journal of cryptology **21**(4), 469–491 (2008)

5. Boldyreva, A., Cash, D., Fischlin, M., Warinschi, B.: Foundations of non-malleable hash and one-way functions. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 524–541. Springer (2009)
6. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. Journal of cryptology **17**(4), 297–319 (2004)
7. Brecht, B., Hehn, T.: A security credential management system for V2X communications. In: Connected Vehicles, pp. 83–115. Springer (2019)
8. Brickell, E., Camenisch, J., Chen, L.: Direct anonymous attestation. In: Proceedings of the 11th ACM conference on Computer and communications security. pp. 132–145 (2004)
9. Camenisch, J., Drijvers, M., Lehmann, A., Neven, G., Towa, P.: Zone encryption with anonymous authentication for V2V communication. In: 2020 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 405–424. IEEE (2020)
10. Camenisch, J., Lysyanskaya, A.: Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Annual international cryptology conference. pp. 61–76. Springer (2002)
11. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Annual international cryptology conference. pp. 56–72. Springer (2004)
12. Chatterjee, S., Menezes, A.: On cryptographic protocols employing asymmetric pairings—The role of Ψ revisited. Discrete Applied Mathematics **159**(13), 1311–1322 (2011)
13. Chen, L., Ng, S.L., Wang, G.: Threshold anonymous announcement in VANETs. IEEE Journal on selected areas in communications **29**(3), 605–615 (2011)
14. Chim, T.W., Yiu, S.M., Hui, L.C., Li, V.O.: SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks **9**(2), 189–203 (2011)
15. Codeca, L., Frank, R., Engel, T.: LuST: a 24-hour Scenario of Luxembourg City for SUMO Traffic simulations (2015)
16. ETSI: Security. ITS communications security architecture and security management, Technical Report ETSI TS 102 940 v1.3.1, ETSI (2018), www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf
17. Förster, D., Löhr, H., Grätz, A., Petit, J., Kargl, F.: An evaluation of pseudonym changes for vehicular networks in large-scale, realistic traffic scenarios. IEEE Transactions on Intelligent Transportation Systems **19**(10), 3400–3405 (2017)
18. Henry, K.: Pseudonym issuing strategies for privacy-preserving V2X communication. SAE International Journal of Transportation Cybersecurity and Privacy **2**(11-02-02-0012), 131–139 (2020)
19. Hicks, C., Garcia, F.D.: A vehicular DAA scheme for unlinkable ECDSA pseudonyms in V2X. In: 2020 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 460–473. IEEE (2020)
20. Johnson, D., Menezes, A., Vanstone, S.: International journal of information security **1**(1), 36–63 (2001)
21. Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Schoch, E., Wiedersheim, B., Thong, T.V., Calandriello, G., Held, A., Kung, A., et al.: Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Communications magazine **46**(11), 110–118 (2008)
22. Luo, W., Fang, X., Cheng, M., Zhou, X.: An optimized handover trigger scheme in LTE systems for high-speed railway. In: Proceedings of the Fifth International Workshop on Signal Design and Its Applications in Communications. pp. 193–196. IEEE (2011)

23. Luo, W., Zhang, R., Fang, X.: A CoMP soft handover scheme for LTE systems in high speed railway. EURASIP Journal on wireless Communications and Networking **2012**(1), 1–9 (2012)
24. Lysyanskaya, A., Rivest, R.L., Sahai, A., Wolf, S.: Pseudonym systems. In: International Workshop on Selected Areas in Cryptography. pp. 184–199. Springer (1999)
25. Malina, L., Castella-Roca, J., Vives-Guasch, A., Hajny, J.: Short-term linkable group signatures with categorized batch verification. In: International Symposium on Foundations and Practice of Security. pp. 244–260. Springer (2012)
26. Neven, G., Baldini, G., Camenisch, J., Neisse, R.: Privacy-preserving attribute-based credentials in cooperative intelligent transport systems. In: 2017 IEEE Vehicular Networking Conference (VNC). pp. 131–138. IEEE (2017)
27. Petit, J., Schaub, F., Feiri, M., Kargl, F.: Pseudonym schemes in vehicular networks: A survey. IEEE Communications Surveys Tutorials **17**(1), 228–255 (2015). https://doi.org/10.1109/COMST.2014.2345420
28. Pointcheval, D., Sanders, O.: Short randomizable signatures. In: Cryptographers' Track at the RSA Conference. pp. 111–126. Springer (2016)
29. Pointcheval, D., Sanders, O.: Reassessing security of randomizable signatures. In: Cryptographers' Track at the RSA Conference. pp. 319–338. Springer (2018)
30. Praveen, K.: V2X driving towards connected cars - Tata Elxsi. Tataelxsi (2020), tataelxsi.com/storage/insights/December2020/blyrAO1FibrFEV7IKfhp.pdf
31. Schweppe, H., Roudier, Y., Weyl, B., Apvrille, L., Scheuermann, D.: Car2x communication: securing the last meter-a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography. In: 2011 IEEE Vehicular Technology Conference (VTC Fall). pp. 1–5. IEEE (2011)
32. Sommer, C., Eckhoff, D., Brummer, A., Buse, D.S., Hagenauer, F., Joerer, S., Segata, M.: Veins: The open source vehicular network simulation framework. In: Recent advances in network simulation, pp. 215–252. Springer (2019)
33. Studer, A., Bai, F., Bellur, B., Perrig, A.: Flexible, extensible, and efficient VANET authentication. Journal of Communications and Networks **11**(6), 574–588 (2009)
34. Sun, Y., Feng, Z., Hu, Q., Su, J.: An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. Security and Communication Networks **5**(1), 79–86 (2012)
35. transport systems, I.: (ITS); Vehicular communications; basic set of applications; Specification of cooperative awareness basic service, Technical Report ETSI EN 302 637-2 V1.3.1, ETSI (2014)
36. USDOT: National Highway Traffic Safety Administration Notice of proposed rulemaking for federal motor vehicle safety standards. V2V communications, Federal Register p. 82(8) (2017)
37. Wernke, M., Skvortsov, P., Dürr, F., Rothermel, K.: A classification of location privacy attacks and approaches. Personal and ubiquitous computing **18**(1), 163–175 (2014)
38. Whitefield, J., Chen, L., Giannetsos, T., Schneider, S., Treharne, H.: Privacy-enhanced capabilities for vanets using direct anonymous attestation. In: 2017 IEEE Vehicular Networking Conference (VNC). pp. 123–130. IEEE (2017)
39. Whyte, W., Weimerskirch, A., Kumar, V., Hehn, T.: A security credential management system for V2V communications. In: 2013 IEEE Vehicular Networking Conference. pp. 1–8. IEEE (2013)
40. Yu, X., Luo, Y., Chen, X.: An optimized seamless dual-link handover scheme for high-speed rail. IEEE transactions on vehicular technology **65**(10), 8658–8668 (2015)

41. Zhang, J., Xu, Y.: Breaking and repairing of an anonymous and traceable communication protocol for vehicular ad hoc networks. In: 2012 IEEE 12th International Conference on Computer and Information Technology. pp. 88–93. IEEE (2012)