Location Privacy in VANETs: Provably Secure Anonymous Key Exchange Protocol Based on Self-Blindable Signatures

Mishri Saleh AlMarshoud*, Ali H. Al-Bayatti and Mehmet Sabir Kiraz

[a] Cyber Technology Institute, De Montfort University, Leicester, UK

ARTICLE INFO

Keywords:
VANETs, Security, Privacy, Location Privacy, Pseudonym Change, Vehicle-to-Vehicle

Abstract

Security and privacy in vehicular ad hoc networks (VANETs) are challenging in terms of Intelligent Transportation Systems (ITS) features. The distribution and decentralisation of vehicles could threaten location privacy and confidentiality in the absence of trusted third parties (TTP)s or if they are otherwise compromised. If the same digital signatures (or the same certificates) are used for different communications, then adversaries could easily apply linking attacks. Unfortunately, most of the existing schemes for VANETs in the literature do not satisfy the required levels of security, location privacy, and efficiency simultaneously. This paper presents a new and efficient end-to-end anonymous key exchange protocol based on Yang *et al.* 's self-blindable signatures. In our protocol, vehicles first privately blind their own private certificates for each communication outside the mix-zone and then compute an anonymous shared key based on zero-knowledge proof of knowledge (PoK). The efficiency comes from the fact that once the signatures are verified, the ephemeral values in PoK are also used to compute a shared key through an authenticated Diffie-Hellman key exchange protocol. Therefore, the protocol does not require any further external information to generate a shared key. Our protocol also does not require an interference with the Roadside Units or Certificate Authorities, and hence can be securely run outside the mixed-zones. We demonstrate the security of our protocol in an ideal/real simulation paradigm. Hence, our protocol achieves secure authentication, forward unlinkability, and accountability. Furthermore, the performance analysis shows that our protocol is more efficient in terms of computational and communication overheads compared to existing schemes.

1. Introduction

There has been continuous advancement in Intelligent Transportation Systems (ITS), particularly in Vehicular Ad Hoc Networks (VANETs). Safety and efficiency in VANETs are mainly achieved via safety and non-safety applications. Beaconing services are essential to safety applications as they are crucial for ITS efficiency; otherwise, accidents may occur. A VANET is considered an open network that is accessible by any node. In general, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) are two forms of communication performed by VANETs; communication occurs via the recent Radio Access Technology (RAD) IEEE 802.11bd for Dedicated Short-Range Communications (DSRC) and NR-V2X for Cellular-V2X (C-V2X). These are applicable in different circumstances, such as tunnels and confined areas [1] and increase the packet delivery ratio while decreasing packet collisions [2]. As demonstrated in [3], DSRC performance is sufficient for nearly all vehicular safety applications that need an end-to-end latency of around 100 ms. Due to their high mobility, vehicles' On-Board Units (OBUs) have to broadcast Cooperative Awareness Messages (CAMs), which include real-time information about speed, position, and trajectory [4]. According to the global standards (i.e., IEEE 1609.2 WG [5] and the European Telecommunications Standards Institute ETSI-ITS [6]), there is a need to guarantee authenticity, message integrity, and entities' non-repudiation on the road.

In the technical report by ETSI ITS, the infrastructure was built on Vehicular Public-key Infrastructure (VPKI), which includes several Certificate Authorities (CAs) managing entities' certificates [7, 8]. During registration, the CA authorises certificates for vehicles and Roadside Unit RSUs. After that, the CA issues certificates based on pseudonyms to prevent any linking attacks on the road. However, the standard body ETSI [9] recommends frequently changing the whole communication stack layers' identifiers with pseudonyms, i.e., the MAC and IP addresses [10]. Nevertheless, an adversary can collect CAMs offline and then can track vehicles' locations smoothly via either *syntactic linking* or *semantic linking* attacks by linking pseudonyms. Moreover, pseudonyms can be linked through the content of the signed messages, whereby an adversary can easily predict the vehicle's next position, also known as a semantic linking attack. It should be noted that a semantic linking attack is superior to a syntactic linking attack because the adversary focuses on the data contained in the safety messages used to link the pseudonyms [11].

Extensive research has developed numerous strategies for pseudonym changing to overcome these linking attacks, as mentioned in the technical report by ETSI ITS [9, 11, 12, 13, 14]. For instance, some strategies propose that vehicles initiate a silent period, which means they are not sending messages but do receive and process them. Tracking is quite difficult during this period, but it is hazardous in terms of safety [15, 16, 17, 18]. The use of such strategies thus clearly increases the possibility of accidents. On the other

*Corresponding author
Email addresses: mishri.almarshoud@dmu.ac.uk (M.S. AlMarshoud); alihmohd@dmu.ac.uk (A.H. Al-Bayatti); mehmet.kiraz@dmu.ac.uk (M.S. Kiraz)
ORCID(s): 0000-0002-8062-1258 (A.H. Al-Bayatti); 0000-0002-7262-562X (M.S. Kiraz)

hand, the concept of a mix-zone has been proposed to enhance the privacy technique for pseudonym-change strategies in Cooperative-ITS (C-ITS).

The mix-zone proposed by Beresford *et al.* [19] is a prespecified geographical area (bound to an RSU's coverage) wherein vehicles can exchange messages and change pseudonyms. The cryptographic mix-zone (CMIX) method depends on a secret key distributed among vehicles to exchange encrypted messages inside the RSU's communication range. This method is constructed to prevent tracking inside the mix-zone [20]. As revealed in ETSI ITS [9], pseudonym changes, silent periods, randomness, fixed parameters, mix-zones, and CMIX all have their particular vulnerabilities.

The self-blindable certificates scheme proposed by Verheul [21] are efficient and effective credential-pseudonymous certificate systems that provide anonymity without the requirement for a trusted third party. The system includes cryptographic protection against forging and unlinkability. The certificates are constructed by Weil pairing in supersingular elliptic curves. The certificate owner blinds the certificate for anonymous vehicle authentication on the road. A self-blindable certificate is a version of the regular public key certificate that preserves privacy. While the CA signature remains valid, the certificate holder can blind the certificate's public key, preventing successive uses of the same certificate from being linked via modification of the digital signature with specific homomorphic properties. The self-blindable certificates work in a similar manner to anonymous certificates for vehicle authentication on the road, but with less computation. Nonetheless, despite its superior performance for intelligent devices, it lacks an efficient credential revocation mechanism. We follow the notion of self-blindable credentials and the associated security structure of [22], involving a credential revocation system towards the need of vehicle communication for a privacy-preserving to a lightweight anonymous entity authentication scheme.

(a). Our Contributions

This paper presents a novel anonymous key exchange protocol for V2V communications to accomplish forward unlinkability without the need for a trusted third party. At a high level, the contributions of the paper can be outlined as follows:

- We first address generic security and privacy issues in the existing schemes wherein an adversary could apply linkability attacks. Some of these schemes are subject to linking attacks due to the misuse of the VANETs' Certificate Revocation Lists (CRLs) and the use of the same certificates outside the mix-zone where RSUs are not available. We next propose the first novel anonymous key exchange protocol that ensures complete location privacy and accountability among the vehicles outside the mix-zone (without communicating to the RSUs). Our scheme uses Yang *et al.* 's self-blindable signatures so that once the signatures are verified, the signature values (i.e., the ephemeral values of the zero-knowledge proofs) will be used to generate a shared key between the participants, in a similar manner to the authenticated Diffie-Hellman key exchange protocol. Since the signature blinding values are fresh and random, the shared key becomes fully secure. On a high level, vehicles first privately blind their own private certificates for each communication outside the mix-zone by hiding their certificates and then compute an anonymous shared key based on zero- knowledge proof of knowledge (PoK). Due to the underlying discrete logarithm problem, the verifier (or a third party) cannot link the newly blinded certificates from the previously used certificates. Hence, to the best of our knowledge, this paper is the first to provide an end-to-end cryptographically secure mechanism against linkability attacks for the communication of vehicles outside the mix-zone without the help of any other participant. We demonstrate the security of our protocol under the ideal/real simulation paradigm.

- We would like to highlight that accountability can still be achieved because if a vehicle is corrupted and sends wrong or misused information to vehicles, then the CAs can still identify the dishonest vehicle. Suppose the corrupted vehicle starts the communication with an honest vehicle outside the range of the trusted third party (e.g., RSU) and receives the blinded certificate of that actual vehicle but does send wrong or invalid information. The honest vehicle would then stop the communication immediately and send the communication record once the CAs becomes available again. Once the CAs obtain their real identity and are sure that this was indeed dishonest behaviour, they can immediately issue revocation through the vehicle's present dynamic accumulator. We would like to highlight that our scheme can be applicable outside the mix-zone in the absence of the TTP since it is important to achieve both accountability and revocability without using conventional PKI. Hence, our scheme accomplishes forward unlinkability, revocability, and accountability simultaneously.

- We conduct a performance analysis of our anonymous key exchange protocol and compare it with other schemes. This comparison illustrates that our scheme is better than other protocols in terms of security. To reduce the online computations associated with our protocol, the vehicles can generate blinded signatures offline (or in parallel). Our scheme is efficient since Yang *et al.* 's scheme allows us to use group operations in only $\mathbf{G}_1$ instead of expensive pairing computations. Performance improvements in our scheme show the ostensibly VANET-based prover to operate entirely on $\mathbf{G}_1$ for faster pairing operations. The anonymous key generation reduces the communication overhead. Furthermore, the revocation in our scheme has a dynamic accumulator Λ that prevents the growth in the number of revoked vehicles by updating that number. Moreover, the efficiency of our protocol comes from the fact that the key exchange protocol does not have any external data or any other expensive computation like pairings or additional signatures; instead, it just uses the existing PoK data to generate the key.

(b). Roadmap

The remainder of this paper is structured as follows: Section 2 reviews the related work on location privacy via unlinkability schemes. Section 3 outlines the security and privacy model of our architecture, which utilises self-blindable signatures. In Section 4, we demonstrate our improved scheme using self-blindable signatures; this is followed by the security analysis of this scheme in Section 5. Section 6 includes the performance and the comparison between our scheme with similar existing security mechanism schemes in the literature. Finally, Section 7 concludes the paper.

2. Related Work

This section first describes three common categories in VANET safety message authentication, namely PKI-based protocols, identity-based protocols, and group-signature-based protocols. We then present the most recent self-blindable certificate method, which forms the basis of our scheme.

(a). PKI-Based VANETs.

PKI-based protocols use public-key certificates, loading numerous pseudonym certificates for vehicles via the Trust Authority (TA) [23]. Vehicles attach a relevant certificate to a safety message. The TA can revoke malicious vehicles' certificates by submitting them to the CRL and updating the CRL across the network. To manage certificates and perform CRL checks, this system requires significant storage, computational, and communication resources [24]. However, the suggested system largely depends on RSUs, and if it is hacked, the system will be destroyed, which means it is inefficient.

Wasef and Shen [25] used a Hash Message Authentication Code (HMAC) check to increase authentication efficiency. However, because the corresponding key used to acquire the HMAC is a global key, updating the key's time and resource costs are quite large. Simplicio *et al.* [26] presented a new design, called Activation Codes for Pseudonym Certificates (ACPC), to address the problem of huge CRLs. To decrease the total size of the CRL, specific short-bit activation codes can be assigned to vehicles. However, because of the decentralised structure and the massive scope of vehicle networks, the distribution of revocation information through the CRL represents a significant challenge in terms of operative pseudonym and node revocation. Lu. *et al.* [27] employed RSUs to give short-lifetime pseudonyms and certificates to vehicles to avoid the limitations of centralised management, but they did not consider a revocation system. Despite the anonymity features given, the ECPP system has several flaws. First, ECPP is inefficient since it has a relatively high latency for RSUs to generate pseudonym keys and requires RSUs to be present to help cars generate their pseudonyms at any given road position. Second, the ECPP requires the issuing authority to know the issued pseudonyms (i.e., RSUs). RSUs are vulnerable to physical assaults since they are distributed in open locations along highways. As a result, unless they are fitted with tamper-resistant hardware, they should not be entirely trusted. Third, there is no specific ECPP revocation method. Malicious vehicles cannot be revoked since they can obtain their pseudonyms from any RSU, even a hacked one. When many RSUs are compromised, ECPP does not provide unlinkability or untraceability. Because each RSU retains unchanged pseudonyms for OBUs in ECPP, an attacker can monitor the vehicle movement trajectory using the information contained in the compromised RSUs.

(b). Identity-Based VANETs.

The public key of a vehicle user can be deduced from its IDs in identity-based protocols. Zhang *et al.* [28] suggested a batch authentication approach for RSUs based on identity in which cars generate pseudonyms and private keys on their own. Their scheme relied on the RSU and suffered from apparent enlargement in the CRL.

Chim *et al.* [29] suggested a scheme in which vehicles occasionally receive pseudonyms and private keys from the TA, which holds the master secret key. The proposed scheme in Chim *et al.* [29] was vulnerable to impersonation attacks because bilinear pairing has a high computational cost.

Some researchers use anonymous certificates in a primitive cryptographic manner that allows entity authentication to occur anonymously in order to achieve unlinkability [30, 31, 32, 33, 34]. A certificate can only be used once in some of the schemes in [30, 33] since any reuse would lead to unlinkability attacks. Although these one-use anonymous certificates operate well [35, 36], k-TAA (k-Times Anonymous Authentication) extends the life of a one-time anonymous certificate by allowing it to be used k times without being linked, such that certificate holders must regularly obtain fresh certificates from the certificate issuer. Certificates require an online connection with a CA, leading to a security vulnerability if the CA has been corrupted. In general, CAs are kept online. If CAs were kept offline, then many certificates would have to be generated offline, which would require significant overhead from the users. Zhou *et al.* [37] proposed a system based on mutual authentication using Elliptic Curve Cryptography (ECC). Nonetheless, this approach is vulnerable to identity guessing and impersonation attacks and has lower levels of user anonymity. In 2017, Li *et al.* [38] suggested a strategy that utilises IDB for the authentication and PKI for the pseudonym generation, although it lacks traceability if a malicious vehicle is involved in malicious activities. Furthermore, several potential attacks, such as modification, replay, DoS, and bogus information, weaken their system. In 2019, Wang *et al.* [39] proposed that an RSU can be fully trusted while being vulnerable to being compromised, which may break the whole scheme. Also, they did not explain the communication between V2V outside the range of the RSU.

(c). Group Signature-Based VANETs.

In group signature protocols, the common group public key can authenticate signatures generated by any group member. Group signatures are a primitive method that works in a similar manner to anonymous certificates in that they allow signatures to be constructed in an unlinkable manner. The distinction is that a CA can undermine the signatures' anonymity and track down the actual signers in group signatures [40, 41, 42, 43, 44, 45]. The ring signature is also primitive, generating unlinkable signatures, and unlinkability is preserved among a collection of dynamically specified vehicles [46]. Lin *et al.* [47] built a privacy-preserving conditional V2V communication system based on group signatures. They assigned private keys to vehicles using a single membership manager, making it hard for the manager to successfully revoke malicious vehicles in large-scale VANETs. In Zhang *et al.* 's scheme [24], RSUs are responsible for revoking malicious vehicles by updating private/public keys according to the communication range. In this case, however, if the vehicle is outside the range, the system will crash. Zhu *et al.* [48] proposed an HMAC as an alternative for the time-consuming CRL check. A hacked RSU, on the other hand, could launch an impersonation attack under such a scheme. Shao *et al.* [49] integrated the decentralised group model and threshold authentication approach to accomplish efficient message authentication and message dependability at the same time. Unfortunately, this does not meet the requirements for traceability [50]. In general, progress has been made in the current study on anonymous message authentication for VANETs. More research is needed, however, to increase message authentication efficiency while still maintaining security and privacy.

Recently, [51] proposed a two-party key agreement based on a lightweight ECC that extends to a Dynamic Group Key Agreement. A fixed RSU runs as Group Controller (GC) with a higher processing ability than the vehicles' OBU. Only two lightweight operations, XOR and hashing, are used to create identity-based authentication and privacy-preserving systems. XOR and hashing are used for lightweight encryption and decryption. To improve performance and security in VANETs, Wu *et al.* [52] presented a mutual authentication password-based approach for V2V in 2019, although an attack can occur from offline password guessing [53].

(d). Self-Blindable Certificates

Structure-preserving anonymous certificates have been presented (e.g., [54, 35, 41, 55, 30, 42, 56, 57, 58]) that make use of non-interactive zero-knowledge proofs [59]. If all the public keys, messages, certificates, and authentication data (produced when revealing a certificate) in an anonymous certificate scheme are $\mathbf{G}_1$ and $\mathbf{G}_2$ group elements, the system is structure-preserving. The goal of their structure-preserving anonymous certificates was to display certificates in a non-interactive manner while avoiding the Fiat–Shamir heuristics [60].

Self-blindable certificates are a cryptographic primitive technique that is similar to conventional certificates, except it also ensures the privacy of the entities [21]. The certificate owner blinds his/her certificate (hence the Public-key) so that no one can link the newly generated certificates, while the signature can still be validated successfully. The authentication data created by displaying a self-blindable certificate that only contains $\mathbf{G}_1$ group elements is more efficient compared to their protocol. As a result, we use Fiat–Shamir heuristics to achieve non-interactive self-blindable certificates. However, the certificate revocation usually has two options. 1) The first method is verifier-local revocation, where the revoked certificates are collected on a list managed by the verifier. Then, the verifier must check the certificate against all the revoked certificates during the validation check (for anonymous entity authentication) [61, 31, 44, 32, 33]. 2) The second method uses a dynamic accumulator, a revocation approach extensively used in anonymous credentials and group signatures, to avoid linear computation on the verifier side. It is a group of values that are collected into a single value called the accumulator, with a witness confirming that the accumulated value is genuinely present in the accumulator for each accumulated value [34, 45, 62]. Prominently, the revocation of the certificates based on the dynamic accumulator solves the linear computation problem in the verifier-local approach. However, there is an issue here: all remaining legitimate users must update their witnesses based on the updated accumulator whenever a certificate is removed. While a user can choose to make witness updates in batch mode and thus avoid being online 24 hours a day, a significant computational overhead is incurred [22].

[63] proposed a privacy-preserving authentication mechanism called the multiple trusted authority one-time identity-based aggregate signature method. In this scheme, credentials are generated by a root trusted authority (TA) for RSUs and vehicles. This scheme assumes RSUs to be semi-honest (honest but curious), which they named lower-level TA. The TA generates the certificate and Public-keys for RSUs and provides a vehicle's internal pseudo-identity and authentication key. Also, it has a member list in its database containing information about the vehicles. After receiving the member secrets and the approved period, the vehicle stores them in a tamper-proof device. The vehicle then broadcasts the message along with its signature across the network.

The receiver validates the signature pairs using bilinear pairing to guarantee correctness and non-repudiation. The TAs can accomplish traceability by utilising the vehicle information recorded in the member list. Each time a vehicle switches networks, it must go through a new authentication process, and RSUs manage all the vehicles' private keys. The scheme is attractive because it aggregates multiple signatures into one, allowing efficient verification and minimising storage requirements. This construction has multiple issues. First, vehicles have to seek shares from neighbouring RSUs, leading to high bandwidth requirements. Also, using a private key with an ID-based signature might create delays and severely weaken communication efficiency in their

VANET system. Furthermore, we would like to highlight that their construction requires RSU for any communication, and therefore if a vehicle is outside the range or the RSU is not available, their system will not work at all.

3. The Use of Self-Blindable Signatures in VANETs

We will now present self-blindable signatures, which are used to ensure anonymous communication without a trusted third party. More specifically, this allows intelligent vehicles to anonymously authenticate themselves to a device reader so that a corrupted reader cannot correlate multiple certificate use. The infrastructure of the scheme is presented in Figure 1, while Figure 2 illustrates the communication between vehicles without the trusted third party or the RSUs. In our scheme, we follow the ETSI standards of PKI as the types of CAs [9]:

- The Root CA (RCA) is a governance organization in charge of all subordinate CAs.
- Long Term CA ($LTCA$) for entity registration and certificate issuance.
- Resolution Authority (RA) works to retrieve the certificates of misbehaving vehicles.
- Pseudonym CA (PCA) is in charge of issuing pseudonyms.

Furthermore, security policies have been widely analysed in several works. Access control through the administration of authorization systems in VANETs is also very crucial in terms of security and privacy. The value of the subject and object characteristics determines the permission decision for usage control. As a result of attribute mutability, three types of activities can influence usage decisions: preupdate, onupdate, and postupdate. These activities can be carried out by the system or the subject before, during, or after access, resulting in system state changes [84], [83]. The SPIN model checker was used by the authors in [83] to verify a policy implementation of a usage control system. The implementation was built for a web-based conference management application that supports several applications via a single communication channel. However, the usage scenario does not enable ongoing rules. The poster was introduced by Rajkumar and Sandhu to improve administrative role-based access control. By establishing three necessary key actions, it has incorporated obligations via an administrative model. The model was limited to administrative actions inside the system [65]. Apart from traditional access control, usage control is a unified authorization system that supports a wide variety of security policies. Safety decidability is a necessary condition for decentralizing and automating authorization system administration like that in VANETs. It is a fundamental requirement for the development of policy analysis tools for system administrators, as they must determine whether the given set of policies and initial configuration can grant unintended access correctly in any future state. This is referred to as safety analysis, and it is well established that it is undecidable in general for the pre-authorization usage control model, referred to as $PreUCON_{A}^{finite}$. As a result, $PreUCON_{A}$'s safety checking cannot be automated in its entirety, and its safety decidable sub-models must impose constraints on their attributes and update functions. Recently, it was demonstrated that even with unbounded object creation, the safety problem for the pre-authorization usage control sub-model with finite attribute domains, called $PreUCON_{A}^{finite}$, is decidable. A significant limitation of finite attributes is their inability to connect objects via their attribute values when unbounded object creation occurs (since attributes that reference other objects must be infinite in this case). It would be desirable to have models with safety-decidable attributes that incorporate both finite and infinite attributes (though necessarily with some restrictions) [82].

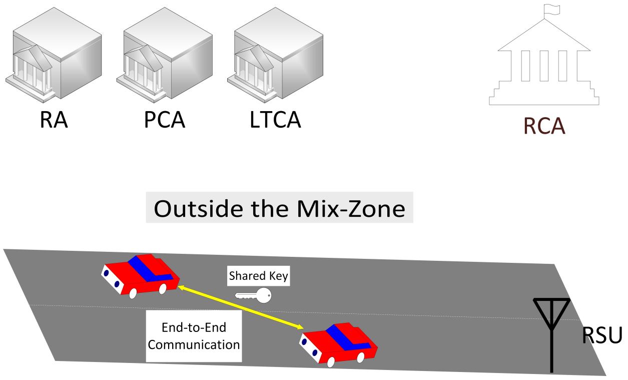


Figure 1: Our C-ITS PKI High-Level Architecture

Rajkumar *et al.* [64] proposes a pre-authorization usage control sub-model, called $PreUCON_{A}$, where attribute domains are entirely composed of infinite object identifiers with significant constraints on how these attributes can be updated. The safety decidability of $PreUCON_{A}$ is established by defining the concept of equivalent usage configurations and demonstrating that the reachable set of these configurations is computable and can be used to answer safety questions. An example demonstrates the utility of such models in practice. In addition, the paper demonstrates that even a single finite domain attribute added to $PreUCON_{A}^{id}$ results in undecidable safety. These findings suggest that combining finite and infinite attributes in a safety decidable model is a difficult task that will almost certainly require carefully crafted constraints on attribute updates.

(a). Privacy Requirements of VANETs

In general, VANETs should ensure the following security and privacy properties:

Apart from the general confidentiality, authentication, integrity, and non-repudiation security requirements, a VANET system must also specifically ensure privacy protection. In our protocol, we achieve this through the following requirements:

- **Unlinkability:** Unlinkability in vehicular networks is generally considered to constitute identity and location privacy. The unlinkability feature basically prevents any types of adversaries from linking multiple messages by means of different interactions to compromise their privacy. Also, any compromise of a vehicle's identity should not affect any other vehicles' privacy at all. In general, identities are generated by means of digital certificates. The user certificate for every vehicular communication must be unlinkable, i.e., an adversary (or the verifier) should not be able to link a vehicle's certificate with previous communications. In this paper, this will be achieved through blinded-certificates.

- **Unforgeability:** For any certificate-based system, the certificates might be unforgeable as this is a core requirement. Hence, the adversary should be incapable of forging the certificate.

- **Revocability:** In the ETSI ITS design, CAs can revoke misbehaving vehicles' certificates [9], and this is essential for practical certificate systems.

(b). Types of adversaries :

In this section, we explore some of the distinctions in attackers' attributes and list the different types of adversaries, as follows:

1. **Global and Local:** The scope of an attacker is used to evaluate whether the adversary is global or local. Global attackers are assumed to have complete network access. Local adversaries, on the other hand, are constrained to a certain segment of the network; eavesdroppers, for instance, may have access to a restricted number of RSUs stationed at traffic junctions [66].

2. **Active and Passive:** An active attacker might compromise the security or privacy on the network by injecting new messages or modifying existing communication messages. Passive attackers, on the other hand, are incapable of altering communication messages. They can only read and monitor data transmitted by the network nodes [12].

3. **Static and Adaptive:** Regardless of how the attack proceeds, static adversaries are assumed to select an attacking technique or plan before initiating the attack. Adversaries that are adaptive monitor the network by obtaining knowledge of the system's configuration and parameters. The majority of threat models in location privacy are adaptive adversaries, referred to as inference attacks in the context of location privacy [67, 68, 69, 70].

4. **Internal and External:** The internal attacker is an authenticated member or network who can send and receive messages as part of the communication range. An external adversary can eavesdrop on messages using sniffing stations [71, 72, 73, 74, 75].

In our paper, we consider active and static adversaries, who can be internal or external.

(c). Self-Blindable Certificate Management

Our anonymous key exchange protocol uses Yang *et al.* 's Self-Blindable Signature scheme [22] as the basis of our scheme, which is described as follows:

Let $e : \mathbf{G}_1 \times \mathbf{G}_2 \rightarrow \mathbf{G}_T$ be a bilinear map for a multiplicative cyclic group of prime order q, and g be generator of $\mathbf{G}_1$, and h be a generator of $\mathbf{G}_2$, $e(g, h) \neq 1$.

(c).1. Setup(1^k)*:*

The following algorithm will be executed by the long-term CA (denoted as $LTCA$):

1. Choose $a, b, d, t_1, t_2 \in_R \mathbf{G}_1$.

2. Compute $Z = h^z$ and compute $T_1 = t_1^z, T_2 = t_2^z$, where $z \in_R \mathbf{Z}_q^*$. Note that z is the master secret key of $LTCA$, i.e., $sk_{LTCA} = z$.

3. Create an accumulator with the value $\Lambda \in_R \mathbf{G}_1$.

4. Set the public parameters

$$pp = (e, a, b, d, h, t_1, t_2, Z, T_1, T_2, \Lambda, CRL = \emptyset).$$

(c).2. CertIssue (sk_{LTCA}, sk_{OBU})*.*

We now generate certificates for OBUs. Let $m = sk_{OBU}$ be the private key of an OBU. We use the key pair of an ElGamal type as $(m, y = g^m)$ where the public key denoted by y is certified by the $LTCA$. The $LTCA$ issues the OBU's certificate as follows.

1. Compute a self-blindable certificate (M, k, s), where $M = (a^m b^s d)^{\frac{1}{k+z}}$, and $k, s \in_R \mathbf{Z}_q$.

2. Compute the witness $W = \Lambda^{\frac{1}{k+z}}$, where Λ is the most recent accumulator.

3. Set the certificate to $Cert = (M, k, s, m, W)$. Note that this real certificate will not be shared with anyone; instead, it will be first blinded, and the blinded ones will be used to ensure privacy during the communication.

The accumulator is used to prevent the certificate holder from sharing the real certificate. In the following, we describe blinded certificate generation for OBUs:

(c).3. CertBlind$(Cert)$*.*

Given $pp, Cert = (M, k, s, m, W)$, we generate a blinded certificate, $BCert$, with the most recent accumulator, Λ.

1. Choose $f, r_1, r_2 \in_R \mathbf{Z}_q$.

2. $M' = (M \cdot W)^f \cdot t_1^{r_1}$.

3. $M'' = (M \cdot W)^{f \cdot k} \cdot T_2^{r_2}$.

4. $A' = (a^m b^s d \cdot \Lambda)^f$.

5. $T_1' = T_1^{r_1}$.

6. $T_2' = t_2^{r_2}$.

7. $PoK\{(k, \mu, \varsigma, f, \gamma, r_1, r_2) : M'' = M'^k t_1^{-\gamma} T_2^{r_2} \bigwedge A' = a^\mu b^\varsigma d^f \Lambda^f \bigwedge T_1' = T_1^{r_1} \bigwedge T_2' = t_2^{r_2}\}$, where $\gamma = k \cdot r_1, \mu = m \cdot f, \varsigma = s \cdot f$. Set the blinded certificate $BCert = (M', M'', A', T_1', T_2', PoK)$.

(c).4. *CertVerify*$(BCert, CRL)$:

For a given blinded certificate $BCert = (M',\ M'',\ A',\ T_1',\ T_2',\ PoK)$, the verifier retrieves the most recent accumulator from the CRL (which includes the most up-to-date accumulator) and verifies all of the following verifier output as follows:

$$\begin{cases} A' \neq 1 \in \mathbf{G}_1 \\ \text{PoK is valid} \\ e(M', Z)e(M'', h) \overset{?}{=} e(A', h)e(T_1', h)e(T_2', Z) \end{cases}$$

The PoK assures the validity of the blinded certificates and the correctness can easily be shown as follows:

$$\begin{aligned} & e\left(M', Z\right) e\left(M'', h\right) = \\ & = e\big((M \cdot W)^f t_1^{r_1}, h^z\big) e\big((M \cdot W)^{fk} t_2^{r_2}, h\big) \\ & = e\big((M \cdot W)^{fz} t_1^{r_1 z}, h\big) e\big((M \cdot W)^{fk} t_2^{r_2}, h\big) \\ & = e\big((M \cdot W)^{fz} t_1^{r_1 z} (M \cdot W)^{fk} t_2^{r_2}, h\big) \\ & = e\big((M \cdot W)^{f(z+k)}, h\big) e\big(t_1^{r_1 z} t_2^{r_2 z}, h\big) \\ & = e\big((M \cdot W)^{f(z+k)}, h\big) e\big(t_1^{r_1 z}, h\big) e\big(t_2^{r_2 z}, h\big) \\ & = e\big((M \cdot W)^{f(z+k)}, h\big) e\big(T_1', h\big) e\big(T_2'^{z}, h\big) \\ & = e\big((M \cdot W)^{f(z+k)}, h\big) e\big(T_1', h\big) e\big(T_2', Z\big) \\ & = e\left(\left((a^m b^s d)^{\frac{1}{k+z}} \Lambda^{\frac{1}{k+z}}\right)^{f(z+k)}, h\right) e\left(T_1', h\right) e\left(T_2', Z\right) \\ & = e\left(\left((a^m b^s d\Lambda)^{\frac{1}{k+z}}\right)^{f(z+k)}, h\right) e\left(T_1', h\right) e\left(T_2', Z\right) \\ & = e\Big((a^m b^s d\Lambda)^f, h\Big) e\big(T_1', h\big) e\big(T_2', Z\big) \\ & = e\big(A', h\big) e\big(T_1', h\big) e\big(T_2', Z\big) \end{aligned} \tag{3.1}$$

(c).5. *CertRevoke*$(z, Cert, \Lambda_{old})$.

A dynamic accumulator method combines a large number of values in one single value, which is known as the *accumulator*. We use the dynamic accumulator in [62], which is a revocation approach to avoid linear computation on the verifier side. There is a witness for each accumulated value, as well as evidence that the collected value is genuinely held in the accumulator, and its correctness can be verified through zero-knowledge proofs (which do not require any relevant data about the witness to be revealed).

1. The RA revokes the value k_j of the OBU_j in the current accumulator Λ_{old} and computes a new accumulator as $\Lambda_{new} = \Lambda_{old}^{\frac{1}{k_j+z}}$. Then, it publishes a new item on a public board as $\langle \Lambda_{new}, k_j \rangle$.

2. The witness can be updated for the holder by a witness as W_i (related to k_i) by computing $W_i^{new} = W_i^{\frac{1}{k_j+z}} = (\Lambda_{old}^{\frac{1}{k_i+z}})^{\frac{1}{k_j+z}} = \Lambda_{old}^{(\frac{1}{k_i+z} - \frac{1}{k_j+z}) \cdot \frac{1}{k_j-k_i}} = (\frac{W_i}{\Lambda_{new}})^{\frac{1}{k_j-k_i}}$. Note that the witness holder updates the W without z's knowledge using the proof of knowledge, whereby the accumulator Λ is $PoK\{(W, k) : e(W, Z \cdot h^k) = e(\Lambda, h)\}$ [35, 62].

3. Adds a new entry (k, Λ_{new}) to the CRL, so that $CRL := CRL \bigcup (k, \Lambda_{new})$.

(d). Efficient Construction of Privacy-Preserving Authentication through Self-Blindable Signatures

As shown in Section 2, it is hard to preserve both privacy and accountability simultaneously outside the mix-zone, the reason for which is that both vehicles must verify the credentials before generating a secure shared key. However, this generally requires a public key scheme and, in particular, digital signatures. However, if the vehicles keep using the same certificates (e.g., RSA, ECDSA), then an adversary (including one of the communicating corrupted parties) can eavesdrop the channel and can link with previous communication as the vehicles keep using the same certificates (unless a bunch of different certificates were generated offline, which would bring additional significant storage, communication, and computational overhead). Therefore, the unlinkability feature would be broken, as addressed in Section 2 for several previous constructions.

Self-blind certificates could be an alternative solution by eliminating conventional signatures due to their randomised blinding structure and accountability feature. Also, we would like to highlight that VANETs generally should not use a fully anonymous key exchange protocol since the identity of the malicious participants must be obtained by the help of RA if there is a safety issue. In this paper, we have used the self-blindable signatures to ensure privacy outside the mix-zone as well as providing accountability, and used in an ingenious way where the private values of the zero-knowledge proofs are used to construct a fresh shared key (i.e., the private values of the proofs of knowledge $T_1''^{r_1}$ and $T_1'^{r_1'}$ in PoK_{OBU_j} and PoK_{OBU_j}, respectively in the blind signature algorithm). More specifically, once the certificates are blinded, shared, and verified by both parties, the parties do not have to send extra values like signed fresh values to perform an authenticated Diffie-Hellman key exchange protocol. Instead, since the zero-knowledge proofs are already used as part of the verification of the underlying signatures, they are fully random and are also using private values in the exponent. We could directly use those public and private

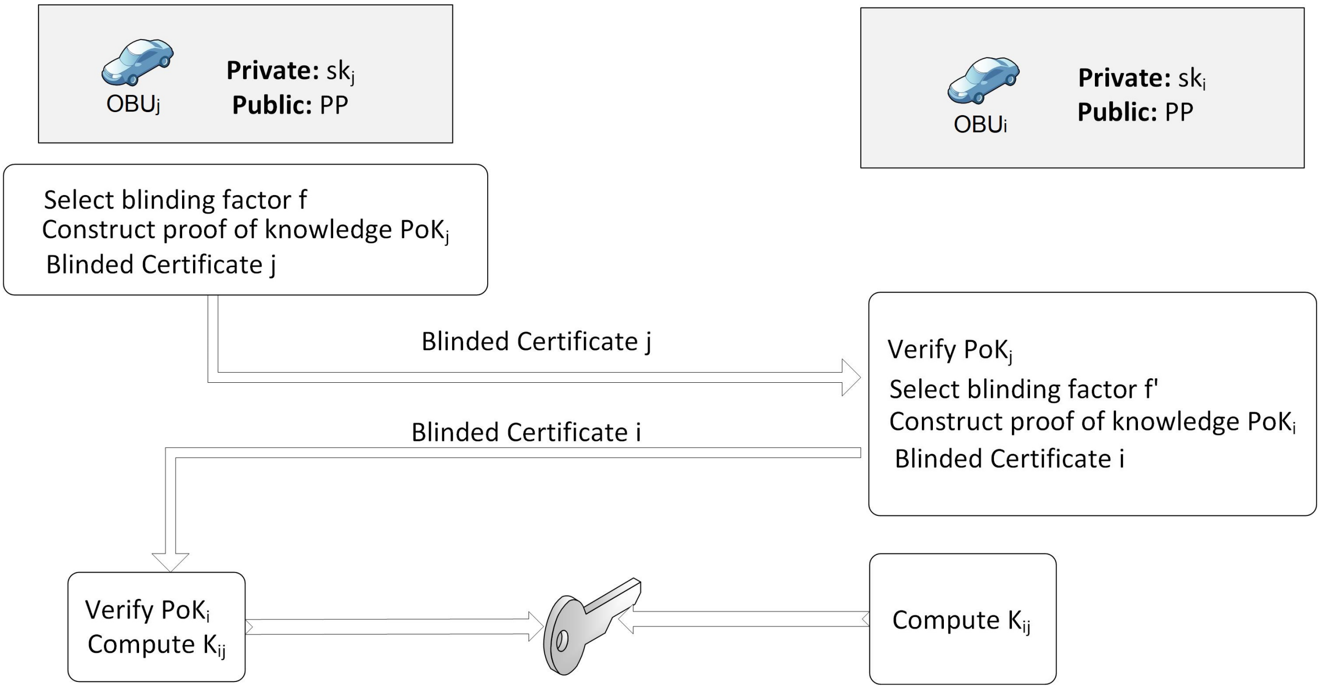


Figure 2: Anonymous and Authenticated Key Exchange Protocol using Self-Blindable Certificates

values to perform an authenticated DH protocol to generate the shared key $K_{ij} = T_1''^{r_1} = T_1'^{r_1'}$. Therefore, this ensures that both parties can compute the symmetric key, eliminating any type of eavesdropping attack. Thus, the vehicles can efficiently and securely transmit their shared secret data during communication outside the mix-zone.

Hence, this proposed work extends Yang *et al.* 's [22] scheme by generating a privacy-preserving key exchange protocol providing accountability without the need for a trusted intermediary. Surely, both parties can use this key continuously until the session is terminated. In Section 5, we give the security proof of our protocol, and in Section 6 we demonstrate that ours is faster than the current state-of-the-art.

4. Our Anonymous Key Exchange Protocol using Self-Blindable Certificates.

We are now ready to present our anonymous key exchange scheme employing Yang *et al.* 's Self-Blindable Signature scheme [22]. As described in Section (c), after running CertIssue(), vehicles can blind their certificates. In case of revocation, they get the latest dynamic accumulator, Λ, and the witness, W, from the CRL, and run CertRevoke(). We would like to highlight that our new protocol generates an indistinguishable shared key for every communication between vehicles.

Suppose that there are two vehicles, OBU_i and OBU_j, outside the range of the RSUs and they are willing to communicate. On a high level, our anonymous key exchange protocol is as follows. At the first stage, OBU_i blinds its certificate by generating proof of knowledge (PoK_{OBU_i}), and sends it to OBU_j. Similarly, OBU_j also blinds its certificate by generating PoK_{OBU_j} and sends it to the OBU_i. Both vehicles utilize the proofs to securely compute a shared and fresh key (see Figure 3 for an illustration of the protocol).

1. OBU_j picks a blinding factor $f, r_1, r_2 \in_R \mathbf{Z}_q$ and computes $M' = (M.W)^f.t_1^{r_1}$. Next, it computes $T_1' = T_1^{r_1}$ and $T_2' = t_2^{r_2}$. Then, it constructs a proof of knowledge PoK_{OBU_j} $\{(k, \mu, \varsigma, f, \gamma, r_1, r_2)$: $M'' = M'^k t_1^{-\gamma} T_2^{r_2} \bigwedge A' = a^{\mu} b^{\varsigma} d^f \Lambda^f \bigwedge T_1' = T_1^{r_1} \bigwedge T_2' = t_2^{r_2}\}$ [76, 77]. After that, it sets its new blinded certificate $BCert_{OBU_j}$ $= (M', M'', A', T_1', T_2', PoK_{OBU_j})$ and sends it to OBU_i.

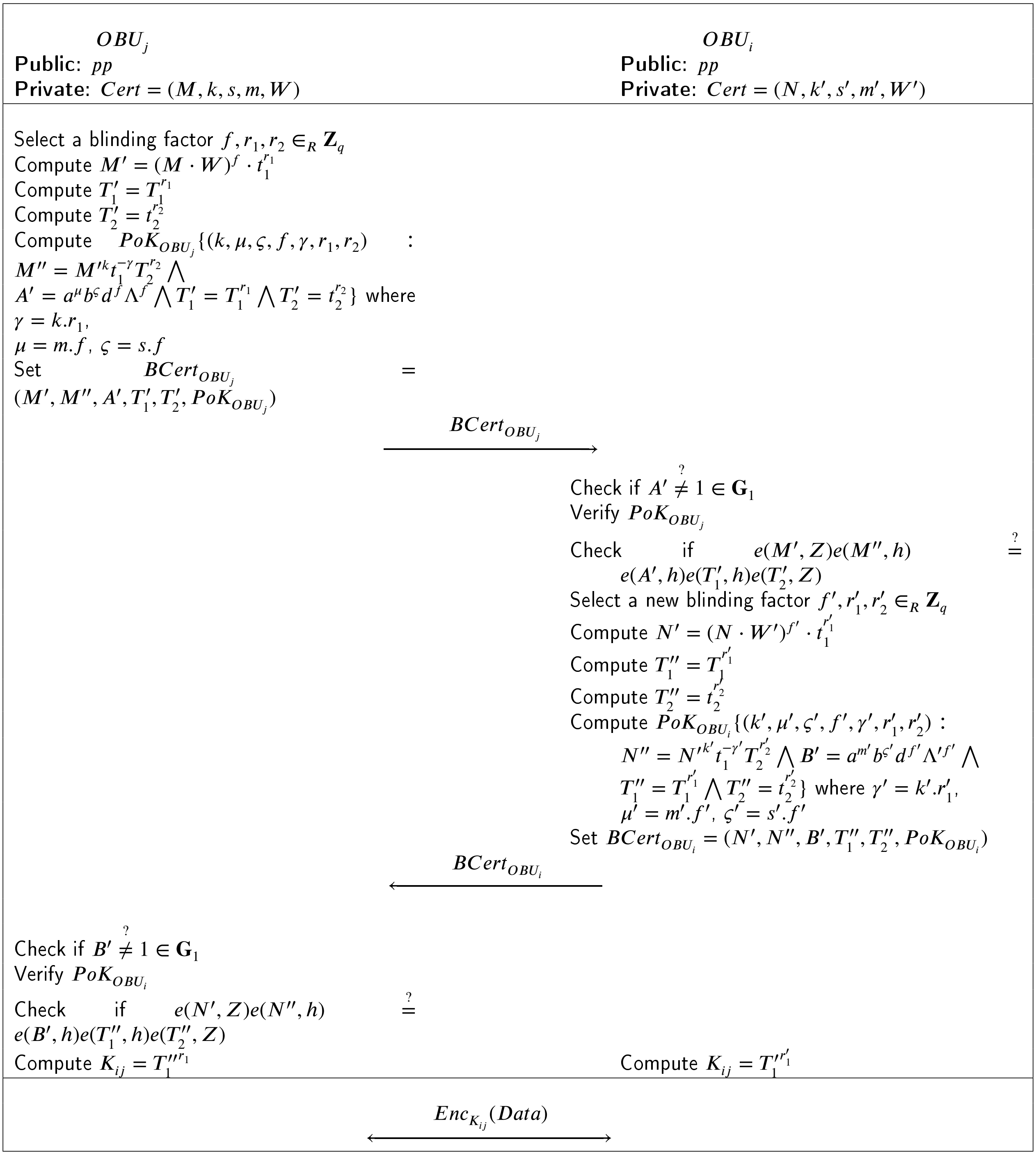
2. OBU_i checks if $A' \overset{?}{\neq} 1 \in \mathbf{G}_1$.

3. Verify PoK_{OBU_j}, check if $e(M', Z)e(M'', h) \overset{?}{=} e(A', h)$ $e(T_1', h)\, e(T_2', Z)$ to ensure that the new blinded certificate is valid.

4. If the proof is valid, it next picks a random blinding factor $f', r_1', r_2' \in_R \mathbf{Z}_q$, computes $N' = (N.W)^{f'}.t_1^{r_1'}$, and computes $T_1'' = T_1^{r_1'}$ and $T_2'' = t_2^{r_2'}$.

5. Then, it constructs a proof of knowledge as PoK_{OBU_i} $\{(k', \mu', \varsigma', f', \gamma', r_1, r_2)$: $N'' = N'^{k'} t_1^{-\gamma'} T_2^{r_2} \bigwedge B' = a^{\mu'} b^{\varsigma'} d^{f'} \Lambda'^{f'} \bigwedge T_1'' = T_1^{r_1'} \bigwedge T_2'' = t_2^{r_2'}$. It also sets its new blinded certificate $BCert_{OBU_i} = (N', N'', B',$ $T_1'', T_2'', PoK_{OBU_i})$ and sends it to OBU_j.

6. OBU_j checks if $B' \overset{?}{\neq} 1 \in \mathbf{G}_1$.



OBU_j
Public: pp
Private: $Cert = (M, k, s, m, W)$

OBU_i
Public: pp
Private: $Cert = (N, k', s', m', W')$

Select a blinding factor $f, r_1, r_2 \in_R \mathbf{Z}_q$
Compute $M' = (M \cdot W)^f \cdot t_1^{r_1}$
Compute $T_1' = T_1^{r_1}$
Compute $T_2' = t_2^{r_2}$
Compute $PoK_{OBU_j}\{(k, \mu, \varsigma, f, \gamma, r_1, r_2)$: $M'' = M'^k t_1^{-\gamma} T_2^{r_2} \bigwedge$ $A' = a^\mu b^\varsigma d^f \Lambda^f \bigwedge T_1' = T_1^{r_1} \bigwedge T_2' = t_2^{r_2}\}$ where $\gamma = k.r_1$, $\mu = m.f$, $\varsigma = s.f$
Set $BCert_{OBU_j}$ = $(M', M'', A', T_1', T_2', PoK_{OBU_j})$

$\xrightarrow{BCert_{OBU_j}}$

Check if $A' \overset{?}{\neq} 1 \in \mathbf{G}_1$
Verify PoK_{OBU_j}
Check if $e(M', Z)e(M'', h) \overset{?}{=} e(A', h)e(T_1', h)e(T_2', Z)$
Select a new blinding factor $f', r_1', r_2' \in_R \mathbf{Z}_q$
Compute $N' = (N \cdot W')^{f'} \cdot t_1^{r'_1}$
Compute $T_1'' = T_1^{r'_1}$
Compute $T_2'' = t_2^{r'_2}$
Compute $PoK_{OBU_i}\{(k', \mu', \varsigma', f', \gamma', r_1', r_2')$: $N'' = N'^{k'} t_1^{-\gamma'} T_2^{r'_2} \bigwedge B' = a^{m'} b^{\varsigma'} d^{f'} \Lambda'^{f'} \bigwedge$ $T_1'' = T_1^{r'_1} \bigwedge T_2'' = t_2^{r'_2}\}$ where $\gamma' = k'.r_1'$, $\mu' = m'.f'$, $\varsigma' = s'.f'$
Set $BCert_{OBU_i} = (N', N'', B', T_1'', T_2'', PoK_{OBU_i})$

$\xleftarrow{BCert_{OBU_i}}$

Check if $B' \overset{?}{\neq} 1 \in \mathbf{G}_1$
Verify PoK_{OBU_i}
Check if $e(N', Z)e(N'', h) \overset{?}{=} e(B', h)e(T_1'', h)e(T_2'', Z)$
Compute $K_{ij} = T_1''^{r_1}$

Compute $K_{ij} = T_1'^{r'_1}$

$\xleftrightarrow{Enc_{K_{ij}}(Data)}$

Figure 3: Anonymous Key Exchange Protocol using Self-Blindable Signatures

7. Checks if $e(N', Z)e(N'', h) \overset{?}{=} e(B', h)\, e(T_1'', h)\, e(T_2'', Z)$.
8. Verifies PoK_{OBU_i}. If the proof is valid, then OBU_j computes the shared key as $K_{ij} = T_1''^{r_1}$.
9. Similarly, OBU_i computes the same shared key as $K_{ij} = T_1'^{r'_1}$.
10. Finally, they securely communicate with each other through the shared secret key K_{ij}.

In the next section, we show that our protocol achieves forward unlinkability, unforgeability, and revocability (see Figure 2 for a high-level illustration of the protocol). With the above construction, three fundamental requirements for location privacy in VANETs have been addressed. First, we achieve unlinkability by end-to-end anonymous communication. It is essential to clarify that the RSUs and the CAs are not involved in this communication, it does not rely on security assumptions, and it solves these requirements cryptographically following the DDH assumption. The communication between any two vehicles starts with blinding the certificates and exchanging proofs of knowledge PoKs to ensure the validity of their credentials among each other. The underlying signature scheme will achieve the second requirement, i.e., unforgeability. Finally, forward unlinkability is accomplished by hiding k in the CRL through the accumulator Λ and the witness W (which ensures security against linkability attacks from the revoked vehicles' information).

5. Security Analysis

We now present the security analysis of our protocol. We start with the correctness of our protocol and then the soundness, which covers the forward unlinkable self-blindable certificates, communication integrity, signature unforgeability, and revocability.

(a). Correctness

If OBU_i and OBU_j are honest, then they generate a shared key, K_{ij}, outside the range of the RSUs correctly from the proofs of knowledge in the blinded certificates as follows:

$$\begin{aligned} K_{ij} &= T_1''^{r_1} \\ &= (T_1^{r'_1})^{r_1} \\ &= T_1^{r'_1 r_1} \\ &= (T_1^{r_1})^{r'_1} \\ &= T_1'^{r'_1} \end{aligned} \tag{5.2}$$

Note that $T_1'^{r'_1}$ is computed by OBU_i while $T_1''^{r_1}$ is computed by OBU_j, as given in Figure 3.

(b). Soundness

Our scheme constructs an anonymous key exchange between the prover and the verifier in end-to-end communication using the XDH assumption based on zero- proof of knowledge from non-interactive self-blindable certificates. Also, we assume the vehicles are authentic, and any corrupt ones will not be able to compute proof of knowledge PoK and blind the certificate (Check the correctness 5.2). If the XDH assumption is accurate, the anonymous shared key is resistant to impersonation attacks [1]. The theorem is as follows:

Theorem 1. *Assume that Yang* et al. *'s self-blindable certificate scheme is secure as the XDH assumption is accurate, and the blinded certificate described above is indistinguishable and achieves forward unlinkability. If either OBU_i or OBU_j is corrupted, then the corrupted vehicle will not obtain any information about the honest vehicle.*

Proof. **Case 1: Assume that OBU$_i$ is corrupted.**
The simulator already has the public parameters and can extract the corrupted party's witness from $BCert_{OBU_i}$, as described in the anonymous key exchange protocol (i.e., (N, k', s', m', W')). From this information, the simulator constructs the view for the OBU_i, which is statistically close to the one when the vehicle interacts with the honest verifier. Since the simulator already knows the private values of OBU_i, it can blind this certificate in exactly the same manner as in the protocol, and outputs $BCert^*_{OBU_i}$. More specifically,

1. It first selects a random blinding factor $f'^*, r_1'^*, r_2'^* \in_R \mathbf{Z}_q$ and computes $N^* = (N.W')^{f'^*}.t_1^{r_1'^*}$ and computes $T_1''^* = T_1^{r_1'^*}$ and $T_2''^* = t_2^{r_2'^*}$.
2. Then, it constructs a proof of knowledge as $PoK_{OBU_i}\{(k'^*, \mu'^*, \varsigma'^*, f'^*, \gamma', r_1'^*, r_2'^*) : N^{**} = N^{*k'^*} t_1^{-\gamma'^*} T_2^{r_2'^*} \bigwedge B^* = a^{\mu'^*} b^{\varsigma'^*} d^{f'^*} \Lambda'^{f'^*} \bigwedge T_1''^* = T_1^{r_1'^*} \bigwedge T_2''^* = t_2^{r_2'^*}$.
3. It finally outputs $BCert^*_{OBU_i} = (N^*, N^{**}, B *, T_1''^*, T_2''^*, PoK^*_{OBU_i})$.

$BCert^*_{OBU_i}$ is computationally indistinguishable from the actual blinded certificate $BCert_{OBU_j} = (M', M'', A', T_1', T_2', PoK_{OBU_j})$ due to the XDH assumption.

Case 2: Assume that OBU$_j$ is corrupted.
The simulator already has the public parameters and can extract the corrupted party's witness from $BCert_{OBU_j}$, as described in the anonymous key exchange protocol (i.e., (M, k, s, m, W)). From this information, the simulator constructs the view for the OBU_j, which is statistically close to the one when the vehicle interacts with the honest verifier. Since the simulator knows the private values of OBU_j, which is $Cert = (M, k, s, m, W)$, it blinds this certificate in exactly the same manner as in the protocol, and outputs $BCert^*_{OBU_j}$. More specifically,

1. It first selects a random blinding factor $f^*, r_1^*, r_2^* \in_R \mathbf{Z}_q$ and computes $M^* = (M.W)^{f^*}.t_1^{r_1^*}$ and computes $T_1'^* = T_1^{r_1^*}$ and $T_2'^* = t_2^{r_2^*}$.
2. Then, it constructs a proof of knowledge as $PoK_{OBU_i}\{(k^*, \mu^*, \varsigma^*, f^*, \gamma, r_1^*, r_2^*) : M^{**} = M^{*k^*} t_1^{-\gamma^*} T_2^{r_2^*} \bigwedge A^* = a^{\mu^*} b^{\varsigma^*} d^{f^*} \Lambda^{f^*} \bigwedge T_1'^* = T_1^{r_1^*} \bigwedge T_2'^* = t_2^{r_2^*}$.
3. It finally outputs $BCert^*_{OBU_j} = (M^*, M^{**}, A *, T_1'^*, T_2'^*, PoK^*_{OBU_j})$ and sends it to OBU_i .

Hence, the blinded certificate $BCert^*_{OBU_j}$ is computationally indistinguishable from the actual blinded certificate, $BCert_{OBU_i} = (N', N'', B', T_1'', T_2'', PoK_{OBU_i})$, due to the XDH assumption.

□

[1] Let the CDH (Computational Diffie-Hellman) be intractable in both $\mathbf{G}_1$ and $\mathbf{G}_2$. The external Diffie-Hellman (XDH) assumption states that the DDH (Decisional Diffie-Hellman) is also intractable in $\mathbf{G}_1$ [78, 79, 80].

	Our Scheme	[39]	[38]	[51]	[52]	[63]
Mutual Authentication	✓	✓	✓	✓	✓	✓
Unforgeability	✓	×	×	✓	✓	✓
Revocability	✓	×	×	✓	✓	✓
Traceability	✓	✓	×	✓	✓	✓
Attack resistance	✓	×	×	✓	×	×
Forward unlinkability	✓	×	×	×	×	×

Table 1
Comparison in terms of security and privacy.

As a result, each step of the proposed authentication protocol for the simulator is simulated, and the simulation for the malicious party is completed. When engaging with the honest user, the transcript is consistent and statistically indistinguishable from the corrupted party's point of view. Hence, the proof ensures that the proposed is unlinkable and unforgeable.

(c). Unlinkability:

Our scheme achieves unlinkability as the attacker cannot obtain any data from the blinded certificates through the communication outside the mix-zone as the vehicles can interact with each other once the verification through proof of knowledge proofs are validated. Hence, a newly generated fresh key will ensure the unlinkability feature. The newly generated symmetric key will be used for the end-to-end confidential communication between the authenticated vehicles. Hence, any eavesdroppers, including CAs and service providers, would not be able to obtain any private data from this secure communication. Thus, our scheme guarantees the unlinkability, which was proven in the Theorem 1 and (b).

(d). Unforgeability:

Theorem 1 and Proof (b) basically cover the following two possible scenarios: 1) OBU_i corruption, 2) OBU_j corruption. If either vehicle is corrupted, then they will not be able to authenticate to the honest participant and hence they will not be able to generate a shared key. Because the malicious entity cannot gain any data from the proof of knowledge proof, the blinded certificate will be computationally indistinguishable. The corrupted parties would also be unable forge the certificate of an honest participant, hence unforgeability has been achieved in the presence of internal (active) attackers.

(e). Revocability:

The revocation process has two main goals: the vehicle can change the pseudonym certificate, or it can be revoked due to malicious activities. The RA can revoke the vehicle certificate due to either malicious activities of a vehicle or the certificate key of the owner or the issuer being compromised. Also, honest vehicles are expected to report malicious vehicles to the RA when it becomes available again. The RA will receive the communication record from the vehicle, and after the investigation it will revoke the vehicle by deleting k_j from Λ_{old} and updating the accumulator Λ_{new}. The accumulation number Λ_{new} is basically a unique number accumulating the revocation numbers of corrupted vehicles so that anyone can efficiently check whether a particular device has been corrupted or otherwise. Furthermore, the witness holder updates the W without z's knowledge using the proof of knowledge, whereby the accumulator Λ is $PoK\{(W,k) : e(W, Z\cdot h^k) = e(\Lambda, h)\}$. Then, the CRL for both sides is updated. This approach ensures forward unlinkability as the accumulator updates via zero-knowledge proof PoK, which do not reveal any extra data about the witness.

In general, our scheme does not need additional certificates because the vehicles will not change the pseudonym certificate until the TTPs are available. The vehicles will keep blinding their certificates in a fresh manner for each communication. Thus, the number of certificates on the system will be significantly reduced compared to the current works. Hence, the revocation execution will not be complex or of high intensity.

6. Comparison

In this section, we first analyse the performance of our protocol and compare it with existing schemes in terms of performance, and security and privacy. The metrics of performance include signature size, multiplication, exponentiation, and pairing operations. The metrics of security and privacy include mutual authentication, forward unlinkability, unforgeability, revocability, traceability, and attack resistance.

(a). Performance Comparison

The V2V communication in our scheme has four main performance stages: 1) The vehicle offline computation reduces the real-time execution addressing the VANETs requirements. In particular, both vehicles must compute blinded signatures to generate a shared key once the proof is validated. Computation of blinded certificates can be computed offline as this does not require any data from the other party. 2) We can also reduce the overall time complexity by allowing the parties to simultaneously blind their certificates in parallel. 3) The computation of the shared key does not require any additional data since the ephemeral data in the PoK will be used to generate an anonymous and authenticated Diffie-Hellman key exchange. This significantly improves the performance compared to others. 4) The com-

Protocol	Signature Generation	Verification
[63]	$17T_h$	$12T_h + 10T_{mult} + 6T_{add}$
[52]	$8T_{mult} + 2T_{add}$	$4T_h + 5T_{exp}$
[51]	$12T_h$	$4T_{mult}$
[38]	$2T_{pair} + 6T_{mpair} + T_{apair}$	$3T_h + 5T_{exp}$
[39]	$8T_{mult} + 5T_{add}$	$8T_{mul} + 2T_{add}$
Our scheme	$8T_{exp}$	$8T_{exp}$

Table 2
Performance comparison.

munication will be conducted using only one symmetric key (i.e., K_{ij}) to ensure confidential communication.

Let $mult(G)$ denote a scalar point multiplication operation in $\mathbf{G}_1$ and $\mathbf{G}_2$, and the exponentiation operation is $\exp(G)$ in $\mathbf{G}_T$. Let also $|\mathbf{G}|$ signify the bit length of an element in group $\mathbf{G}$. In our architectures, the vehicle computes exclusively on $\mathbf{G}_1$, and the verifier performs the group computation and bilinear pairings on $\mathbf{G}_T$ like [22]. This feature distinguishes our method from practically all existing anonymous certificates' bilinear map-based and group signatures, such as those described in Section 2. Note that $|\mathbf{G}_1|$ is substantially shorter than $|\mathbf{G}_2|$ and $|\mathbf{G}_T|$ in the context of bilinear maps, and $exp(\mathbf{G}_1)$ is significantly quicker than $exp(\mathbf{G}_2)$, $exp(\mathbf{G}_T)$ and the pairing operation. While we claim that our technique is more efficient than existing anonymous certificate and group signature protocols, we recognize that different protocols rely on varying cryptographic assumptions.

The comparison in terms of signature generation and the verification is given in Table 2. Furthermore, Table 3 illustrates the execution time of each basic operation by considering the computation costs. Note that in our calculations, the proof of knowledge PoK in the blinded certificate incurs $8exp(\mathbf{G}_1)$ in total computation [77, 76]. We would like to highlight that in our scheme, OBU_i can blind its signature in parallel with OBU_j to reduce communications, instead of waiting for the blinded signature of OBU_j. Our main goal is to provide an accountable and privacy-preserving key exchange protocol without utilizing any external parties such as RSUs (due to outside the mixed-zone), and this is achieved by blinding their own signatures in an ingenious way where the data within the PoK is used to generate a shared key. Furthermore, the results show that our scheme is fast and has a low overhead compared to others because the entities OBU_i and OBU_j only share one single blinded signature together with a proof of knowledge. Our calculations demonstrate that our scheme is practical since the execution time is less than 100 ms.

In our certificate anonymous credential system, we use a lightweight signing method (a short signature length of 154 bits only, based on the Weil pairing that is obtained from certain subgroups of low dimensional abelian varieties over finite fields [42, 80]), which ensures privacy and trust outside the mix-zone without interference from any third parties. The signature method is based on Boneh–Lynn–Shacham (BLS), which fulfils our essential goals. Hence, the schemes in Table 2 failed to guarantee simultaneous accountability, privacy, and trust, while we provide them in our scheme.

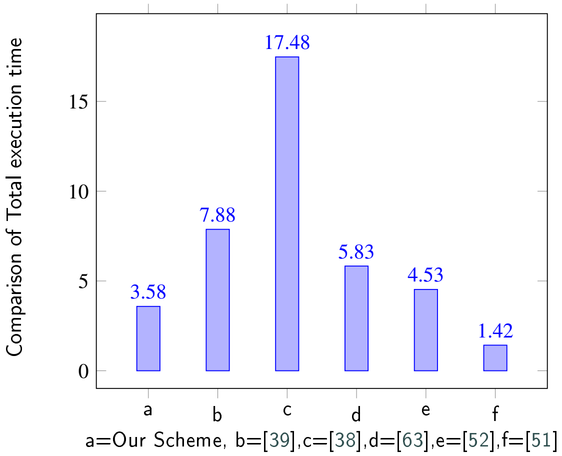


Figure 4: Total execution comparison.

On the other hand, our signature generation and verification computations are in range. More precisely, the DSRC performance is sufficient for nearly all vehicular safety applications that need an end-to-end latency of around 100 ms [3]. We compare our scheme computation with the existing schemes in Figure 4. The results show that our scheme is second-fastest, at 3.58 ms. If we consider that our scheme is generating the signature offline and it is only one round verification, then our scheme can be considered sufficiently fast for vehicular communication.

(b). Security and Privacy Comparison

In Table 1, we compare the existing schemes with our own in terms of forward unlinkability, revocability, unforgeability, traceability, attack resistance, and mutual authentication; more precisely, those concepts in V2V communication with the absence of the TTPs. Some of these schemes rely on TTP, which would not work for the cases outside the mix-zone. The scheme proposed in [52] has various drawbacks in terms of security and privacy. Their scheme lacks forward unlinkability and uses a password-based authentication protocol that is not resistant to offline password guessing attacks [53]. The scheme in [39] has mutual authentication and traceability, but their protocol does not consider RSU corruption. In the scheme proposed by [63], the

Symbol	Description	Execution time (ms)
T_h	**Hash function Execution**	**0.010**
T_{add}	**Scalar Point Addition Execution**	**0.38**
T_{mult}	**Scalar Point Multiplication Execution**	**0.326**
T_{exp}	**Exponentiation Execution**	**0.224**
T_{pair}	**Bilinear Pairing Execution**	**4.28**
T_{mpair}	**Multiplication with Pairings Execution**	**1.27**
T_{apair}	**Addition with Pairings Execution**	**0.148**

Table 3
Execution time of basic operations.

RSU is responsible for managing the vehicle's private key, which is objectionable [81]. Li *et al.* 's scheme [38] has no traceability if a malicious vehicle shows malicious activities. Moreover, some possible attacks threaten these systems, such as modification, replay, DoS, and bogus info [13]. The recent proposal in [51] has a mutual authentication and attack resistance and achieves unforgeability and revocability. However, their proposal relies entirely on the RSU. If the RSU has been corrupted, this will break the whole system. Also, their scheme does not accomplish forward unlinkability because attackers could execute linking attacks through the CRL.

Our approach has forward unlinkability, which means that our scheme is secure and has privacy against linkability attacks from the CRL. Also, our scheme allows mutual authentication in the communication through PoKs verification. Furthermore, freshness and unforgeability are guaranteed through generating a K_{ij} shared key based on the PoK that has been computed through the communication. Moreover, the anonymous key K_{ij} uses the XDH assumption, which means that giving the PoKs to attackers is not sufficient to generate that key. Our scheme is secure and overcomes the vulnerabilities of existing works.

7. Conclusion

In this paper, we focused on the security protocols of existing works without a trusted third party and pointed out that they are vulnerable to linkability attacks. This generally occurs because they share certain deterministic values (e.g., the same digital certificates) in each communication. We also address the security and privacy issues in the existing works concerning pseudonym change management, which degrades privacy and obstructs unlinkability. In this respect, we proposed an (end-to-end) anonymous key exchange protocol based on self-blindable certificates, which achieves forward unlinkability in vehicles' communications. Hence, our end-to-end protocol prevents eavesdroppers, including the CAs and service providers, in terms of addressing location privacy. Furthermore, in our system, the vehicles generate signatures offline and, in real-time, they blind their certificates in parallel to lessen the communication time. Similarly, our shared key requires a one-time certificate blind, decreasing the number of the more computationally intensive bilinear pairing operations. To the best of our knowledge, this is the first paper to present a complete unlinkability solution for location privacy in VANETs that is cryptographically secure. The access control of the VANETs entities and architecture's policies is also an essential aspect for the future. However, a full examination of such expansions is outside the scope of this article. Furthermore, as potential future work, implementation of this scheme could be given as a proof-of-concept for benchmarking and tracking of outcomes.

Acknowledgement

We would like to thank the anonymous referees and Muhammed Ali Bingol for their insightful comments and suggestions.

References

[1] A. Chehri, H. Chehri, N. Hakim, R. Saadane, Realistic 5.9 ghz dsrc vehicle-to-vehicle wireless communication protocols for cooperative collision warning in underground mining, in: Smart Transportation Systems 2020, Springer, 2020, pp. 133–141.

[2] G. Naik, B. Choudhury, J.-M. Park, IEEE 802.11 bd & 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications, IEEE Access 7 (2019) 70169–70184.

[3] M. I. Hassan, H. L. Vu, T. Sakurai, Performance analysis of the ieee 802.11 mac protocol for dsrc safety applications, IEEE Transactions on vehicular technology 60 (8) (2011) 3882–3896.

[4] Z. Doukha, S. Moussaoui, An SDMA-Based Mechanism for Accurate and Efficient Neighborhood-Discovery Link-Layer Service, IEEE Transactions on Vehicular Technology 65 (2) (2015) 603–613.

[5] I. V. Technology, IEEE Standard for Wireless Access in Wireless Access in Vehicular Environments (WAVE)– Networking Services (2016).

[6] E. ITS, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications, https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf (2019).

[7] E. ITS, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.04.01_60/ts_102941v010401p.pdf (2021).

[8] I. V. Technology, IEEE standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages (2013).

[9] E. ITS, Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Pseudonym Change Management, https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf (2018).

[10] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, M. Raya, Architecture for Secure and Private Vehicular Communi-

cations, in: 2007 7th International Conference on ITS Telecommunications, IEEE, 2007, pp. 1–6.

[11] A. Boualouache, S.-M. Senouci, S. Moussaoui, A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks, IEEE Communications Surveys & Tutorials 20 (1) (2017) 770–790.

[12] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym Schemes in Vehicular Networks: A survey, IEEE communications Surveys & Tutorials 17 (1) (2014) 228–255.

[13] S. S. Manvi, S. Tangade, A survey on authentication schemes in vanets for secured communication, Vehicular Communications 9 (2017) 19–30.

[14] B. Wiedersheim, Z. Ma, F. Kargl, P. Papadimitratos, Privacy in inter-vehicular networks: Why simple pseudonym change is not enough, in: 2010 Seventh international conference on wireless on-demand network systems and services (WONS), IEEE, 2010, pp. 176–183.

[15] J. Cui, J. Wen, S. Han, H. Zhong, Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network, IEEE Internet of Things Journal 5 (5) (2018) 3491–3498.

[16] M. B. Mansour, C. Salama, H. K. Mohamed, S. A. Hammad, Vanet security and privacy-an overview, International Journal of Network Security & Its Applications (IJNSA) Vol 10 (2018).

[17] R. Al-ani, B. Zhou, Q. Shi, T. Baker, M. Abdlhamed, Adjusted location privacy scheme for vanet safety applications, in: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2020, pp. 1–4.

[18] M. Babaghayou, N. Labraoui, A. A. A. Ari, N. Lagraa, M. A. Ferrag, Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey, Journal of Information Security and Applications 55 (2020) 102618.

[19] A. R. Beresford, F. Stajano, Location privacy in pervasive computing, IEEE Pervasive Computing 2 (2003). doi:10.1109/MPRV.2003.1186725.

[20] J. Freudiger, M. Raya, M. Falegyhazi, P. Papadimitratos, J.-P. Hubaux, Mix-Zones for Location Privacy in Vehicular Networks, ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS) (2007).

[21] E. R. Verheul, Self-blindable credential certificates from the weil pairing, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2001, pp. 533–551.

[22] Y. Yang, X. Ding, H. Lu, J. Weng, J. Zhou, Self-Blindable Credential: Towards Anonymous Entity Authentication upon Resource Constrained Devices, in: Information Security, Springer, 2015, pp. 238–247.

[23] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, Journal of computer security 15 (1) (2007) 39–68.

[24] L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Transactions on vehicular Technology 59 (4) (2009) 1606–1617.

[25] A. Wasef, X. Shen, Emap: Expedite message authentication protocol for vehicular ad hoc networks, IEEE transactions on Mobile Computing 12 (1) (2011) 78–89.

[26] M. A. Simplicio Jr, E. L. Cominetti, H. K. Patil, J. E. Ricardini, M. V. M. Silva, Acpc: Efficient revocation of pseudonym certificates using activation codes, Ad Hoc Networks 90 (2019) 101708.

[27] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications, in: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, IEEE, 2008, pp. 1229–1237.

[28] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, in: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, IEEE, 2008, pp. 246–250.

[29] T. W. Chim, S.-M. Yiu, L. C. Hui, V. O. Li, Specs: Secure and privacy enhancing communications schemes for vanets, Ad Hoc Networks 9 (2) (2011) 189–203.

[30] S. Brands, Rethinking public key infrastructures and digital certificates: building in privacy, Mit Press, 2000.

[31] D. Chaum, Security without identification: Transaction systems to make big brother obsolete, Communications of the ACM 28 (10) (1985) 1030–1044.

[32] J. Camenisch, E. Van Herreweghen, Design and implementation of the idemix anonymous credential system, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 21–30.

[33] J. Camenisch, A. Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: International conference on the theory and applications of cryptographic techniques, Springer, 2001, pp. 93–118.

[34] J. Camenisch, M. Kohlweiss, C. Soriente, An accumulator based on bilinear maps and efficient revocation for anonymous credentials, in: International workshop on public key cryptography, Springer, 2009, pp. 481–500.

[35] M. H. Au, W. Susilo, Y. Mu, Constant-size dynamic k-taa, in: International conference on security and cryptography for networks, Springer, 2006, pp. 111–125.

[36] I. Teranishi, J. Furukawa, K. Sako, K-times anonymous authentication, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2004, pp. 308–322.

[37] Y. Zhou, X. Zhao, Y. Jiang, F. Shang, S. Deng, X. Wang, An enhanced privacy-preserving authentication scheme for vehicle sensor networks, Sensors 17 (12) (2017) 2854.

[38] J. Li, H. Lu, M. Guizani, Acpn: A novel authentication framework with conditional privacy-preservation and non-repudiation for vanets, IEEE Transactions on Parallel and Distributed Systems 26 (4) (2014) 938–948.

[39] B. Wang, Y. Wang, R. Chen, A Practical Authentication Framework for VANETs, Security and Communication Networks 2019 (2019).

[40] G. Ateniese, J. Camenisch, M. Joye, G. Tsudik, A practical and provably secure coalition-resistant group signature scheme, in: Annual international cryptology conference, Springer, 2000, pp. 255–270.

[41] G. Ateniese, B. de Medeiros, Efficient group signatures without trapdoors, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2003, pp. 246–268.

[42] D. Boneh, X. Boyen, Short signatures without random oracles, in: International conference on the theory and applications of cryptographic techniques, Springer, 2004, pp. 56–73.

[43] D. Boneh, H. Shacham, Group signatures with verifier-local revocation, in: Proceedings of the 11th ACM conference on Computer and communications security, 2004, pp. 168–177.

[44] D. Chaum, E. Van Heyst, Group signatures, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1991, pp. 257–265.

[45] J. Camenisch, M. Michels, A group signature scheme with improved efficiency, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 1998, pp. 160–174.

[46] R. L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2001, pp. 552–565.

[47] X. Lin, X. Sun, P.-H. Ho, X. Shen, Gsis: A secure and privacy-preserving protocol for vehicular communications, IEEE Transactions on vehicular technology 56 (6) (2007) 3442–3456.

[48] X. Zhu, S. Jiang, L. Wang, H. Li, Efficient privacy-preserving authentication for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 63 (2) (2013) 907–919.

[49] J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for vanets, IEEE Transactions on vehicular technology 65 (3) (2015) 1711–1720.

[50] J. Zhang, Z. Sun, S. Liu, P. Liu, On the security of a threshold anonymous authentication protocol for vanets, in: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, 2016, pp. 145–155.

[51] V. S. Naresh, S. Reddi, V. D. Allavarpu, Provable secure dynamic lightweight group communication in vanets, Transactions on Emerging Telecommunications Technologies (2021).

[52] L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, Z. Zhu, An efficient privacy-preserving mutual authentication scheme for se-

cure v2v communication in vehicular ad hoc network, IEEE Access 7 (2019) 55050–55063.

[53] M. J. Sadri, M. Rajabzadeh Asaar, A lightweight anonymous two-factor authentication protocol for wireless sensor networks in internet of vehicles, International Journal of Communication Systems 33 (14) (2020) e4511.

[54] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, M. Ohkubo, Structure-preserving signatures and commitments to group elements, in: Annual Cryptology Conference, Springer, 2010, pp. 209–236.

[55] J. Balasch, Smart ard implementation of anonymous redentials, Ph.D. thesis, Katholieke Universiteit Leuven (2008).

[56] D. Boneh, X. Boyen, H. Shacham, Short group signatures, in: Annual international cryptology conference, Springer, 2004, pp. 41–55.

[57] P. Bichsel, J. Camenisch, T. Groß, V. Shoup, Anonymous credentials on a standard java card, in: Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 600–610.

[58] M. Belenkiy, M. Chase, M. Kohlweiss, A. Lysyanskaya, P-signatures and noninteractive anonymous credentials, in: Theory of Cryptography Conference, Springer, 2008, pp. 356–374.

[59] J. Groth, A. Sahai, Efficient non-interactive proof systems for bilinear groups, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2008, pp. 415–432.

[60] A. Fiat, A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, in: Conference on the theory and application of cryptographic techniques, Springer, 1986, pp. 186–194.

[61] X. Boyen, A tapestry of identity-based encryption: practical frameworks compared, International Journal of Applied Cryptography 1 (1) (2008) 3–21.

[62] L. Nguyen, Accumulators from bilinear pairings and applications, in: Cryptographers' track at the RSA conference, Springer, 2005, pp. 275–292.

[63] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, Distributed aggregate privacy-preserving authentication in VANETs, IEEE Transactions on Intelligent Transportation Systems 18 (3) (2016) 516–526.

[64] P. Rajkumar, R. Sandhu, Safety decidability for pre-authorization usage control with identifier attribute domains, IEEE Transactions on Dependable and Secure Computing 17 (3) (2018) 465–478.

[65] R. PV, R. Sandhu, Poster: security enhanced administrative role based access control models, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1802–1804.

[66] M. Humbert, M. H. Manshaei, J. Freudiger, J.-P. Hubaux, Tracking games in mobile networks, in: International Conference on Decision and Game Theory for Security, Springer, 2010, pp. 38–57.

[67] M. Gerlach, Assessing and improving privacy in vanets, ESCAR, Embedded Security in Cars (2006).

[68] M. L. Yiu, C. S. Jensen, X. Huang, H. Lu, Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services, in: 2008 IEEE 24th International Conference on Data Engineering, IEEE, 2008, pp. 366–375.

[69] R. Cheng, Y. Zhang, E. Bertino, S. Prabhakar, Preserving user location privacy in mobile data management infrastructures, in: International Workshop on Privacy Enhancing Technologies, Springer, 2006, pp. 393–412.

[70] T. Hara, A. Suzuki, M. Iwata, Y. Arase, X. Xie, Dummy-based user location anonymization under real-world constraints, IEEE Access 4 (2016) 673–687.

[71] B. Niu, S. Gao, F. Li, H. Li, Z. Lu, Protection of location privacy in continuous lbss against adversaries with background information (2016) 1–6.

[72] B. Niu, Q. Li, X. Zhu, G. Cao, H. Li, Enhancing privacy through caching in location-based services (2015) 1017–1025.

[73] C.-Y. Chow, M. F. Mokbel, Enabling private continuous queries for revealed user locations (2007) 258–275.

[74] Z. Zhu, G. Cao, Toward privacy preserving and collusion resistance in a location proof updating system, IEEE Transactions on Mobile Computing 12 (1) (2011) 51–64.

[75] A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté, Location privacy in location-based services: Beyond ttp-based schemes (2008) 12–23.

[76] R. "Cramer, I. Damgård, B. Schoenmakers, Proofs of partial knowledge and simplified design of witness hiding protocols", in: Advances in Cryptology — CRYPTO '94", Springer, 1994, pp. 174–187.

[77] B. Schoenmakers, Lecture notes: cryptographic protocols, https://www.win.tue.nl/~berry/CryptographicProtocols/LectureNotes.pdf (Jan 2021).

[78] W. Diffie, P. C. Van Oorschot, M. J. Wiener, Authentication and authenticated key exchanges, Design Codes Cryptography (1992) 107–125doi:10.1007/BF00124891.

[79] IEEE, Ieee standard specifications for public-key cryptography - amendment 1: Additional techniques (2004).

[80] O. Uzunkol, M. S. Kiraz, Still wrong use of pairings in cryptography, Applied Mathematics and Computation 333 (2018) 467–479.

[81] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, M. K. Khan, Sebap: a secure and efficient biometric-assisted authentication protocol using ecc for vehicular cloud computing, International Journal of Communication Systems 34 (2) (2021).

[82] P. Rajkumar, R. Sandhu, Safety decidability for pre-authorization usage control with finite attribute domains, IEEE Transactions on Dependable and Secure Computing 13 (5) (2015) 582–590.

[83] P. Rajkumar, SK. Ghosh, D. Pallab, Concurrent usage control implementation verification using the spin model checker, international conference on network security and applications, Springer (2010) 214–223.

[84] P. Rajkumar, SK. Ghosh, D. Pallab, Application specific usage control implementation verification, International Journal of Network Security and Its Applications, Citeseer 1 (3) (2009) 116–128.