IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 11, 2021, accepted November 22, 2021, date of publication November 29, 2021,
date of current version December 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131189

Pairing-Free Signatures With Insider-Attack Resistance for Vehicular Ad-Hoc Networks (VANETs)

L. ELLEN FUNDERBURG, HUIMIN REN, AND IM-YEONG LEE
Department of Software Convergence, Soonchunhyang University, Asan 31538, South Korea

Corresponding author: Im-Yeong Lee (imylee@sch.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) by the Ministry of Education under Grant NRF-019R1A2C1085718, in part by the Soonchunhyang University Research Fund, and in part by the Republic of Korea's Ministry of Science and ICT (MSIT) under the High-Potential Individuals Global Training Program supervised by the Institute of Information and Communications Technology Planning and Evaluation (IITP) under Grant 2021-0-01516.

ABSTRACT Vehicular Ad-hoc Networks (VANETs) are a type of Internet of Things system where groups of vehicles communicate with each other and traffic monitoring infrastructure in order to provide safety and quality of life improvements for drivers and others in the area. Vehicles in a VANET are responsible for reporting their own status, as well as the statuses of the roadway, traffic, and environment in their immediate vicinity, to the system controller and other drivers for processing. VANET systems are open to the public, with vehicles joining and leaving at a high rate. This feature results in two high-priority requirements for VANET security: vehicles in a VANET must be held responsible for the correctness of the information that they report, and schemes ensuring message security must be quick. This paper presents an efficient, pairing-free signature scheme for VANETs that prevents the forgery of signer identities, including in the case of insider attacks, without the use of a tamper-proof device.

INDEX TERMS VANET, insider attacks, elliptic curve cryptography, signatures, authentication, non-repudiation, tracing.

I. INTRODUCTION

As electronics have become cheaper, vehicle ownership has increased, and wireless technology has improved, the possibilities for intelligent transportation systems and connected vehicles have expanded. These new technologies offer a broad range of benefits over the vehicles and transportation systems of previous generations. Better wireless connections can provide expanded information and entertainment options to drivers and passengers, and connections with neighboring vehicles can increase traffic safety [1].

Conversely, these same technologies and increasing system complexity also introduce new security vulnerabilities that did not exist before. Internet-connected information and entertainment systems offer new avenues for personal information theft and privacy breaches while connections with roadside devices and other vehicles can be used for denial-of-service attacks [2] or to introduce false information [3], either of which can create safety hazards that aren't present in unconnected cars. Accordingly, information security is essential for modern vehicles participating in Vehicular Ad-hoc Networks (VANETs).

This paper is organized as follows: The remainder of this section provides background information on VANETs and their security requirements. Section II gives an overview of related VANET security schemes. Section III presents a new VANET signature scheme. Section IV gives the analysis of that scheme with respect to the security requirements of VANETs and the performance of the proposed scheme. Section V concludes the paper.

A. VANET STRUCTURE

VANETs are a type of Mobile Ad-hoc Network (MANET) composed of groups of vehicles and, optionally, roadside infrastructure. A typical VANET has three levels as shown in Fig. 1: a top-level Trusted Authority (TA) and/or Service Provider (SP), a middle level of semi-trusted devices known as Road-Side Units (RSUs), and a final level of

The associate editor coordinating the review of this manuscript and approving it for publication was Xianzhi Wang.

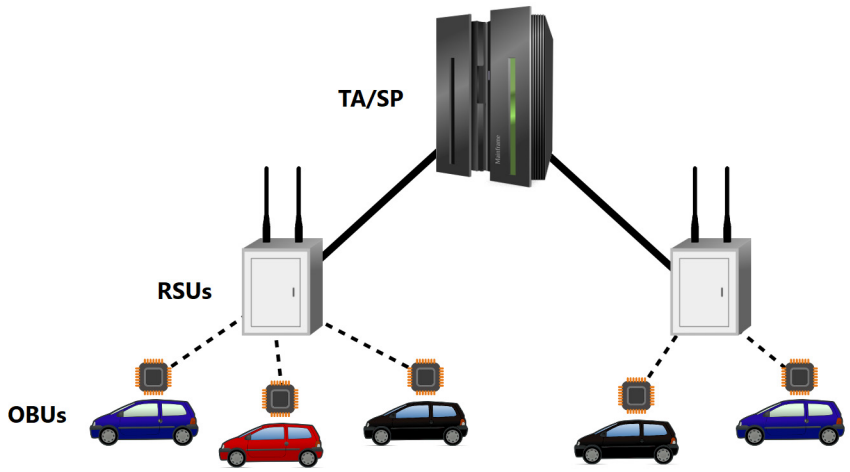


FIGURE 1. Typical VANET hierarchy.

vehicles containing processors referred to as On-Board Units (OBUs) [1].

1) TA/SP LEVEL

A highly-trusted, well-equipped, top-level server or servers. This level may provide identity authentication, access to services such as information or entertainment, or both.

2) RSU LEVEL

Most VANET systems have a middle level of hardware nodes that are usually fixed equipment installed along the roadside for short-range communication with the OBUs. These devices are installed and controlled by authorities, but are usually only semi-trusted as they are exposed to the environment, which makes hardware tampering possible. As 5G networks become more common, the need for dedicated relay hardware will likely decrease, and nodes at this level may evolve into regional servers more closely resembling the TA/SP level or disappear entirely.

3) OBU LEVEL

Every vehicle in a VANET is equipped with an OBU. These OBUs are the lowest level nodes of a VANET system. OBUs are more powerful than many other types of IoT nodes and hand-held mobile devices as vehicles can provide both ample space and electricity [4]. In addition, the comparatively high price of a vehicle means processor cost is also not as much as an issue compared to many other IoT systems. However, like other consumer IoT systems, OBUs are under control of the users and vulnerable to physical attacks [2] so should be considered untrusted.

B. VANET SECURITY

The most outstanding feature of VANETs, compared to other IoT systems, is the high mobility of the members [4]. This mobility leads to dynamic group membership that changes at a much greater rate than most MANETs or other IoT applications. At highway speeds, in densely populated areas, group membership can change every 140ms or more [5]. In addition, group membership and wireless connections are open to the public, so members should be untrusted.

1) INTEGRITY

Message integrity is fundamental to secure messaging systems, including VANETs. Systems must have mechanisms to prevent, or at least detect, both intentional and accidental message corruption. In addition, message integrity checks ensure that message data is not modified as it travels between nodes in order to produce a valid message with false contents.

2) AUTHENTICATION

As with most security applications, ensuring message integrity alone is not sufficient for secure VANETs. The system must also ensure that only authorized parties can generate messages for the system. Identity authentication prevents attackers from joining the system using forged or modified credentials. Message authentication, usually in the form of message signatures, prevents attackers who are not part of the system from injecting false data.

3) PRIVACY

In the context of VANET, privacy is used to mean both protecting the real identity of drivers, i.e. official vehicle registration information and personal identifying information, and preventing message linking. Message linking refers to the ability to associate two or more messages with the same vehicle. For example, schemes frequently use pseudo-IDs in order to hide the real identities of message senders. If two or more messages are sent using the same pseudo-ID, then receivers can assume they were sent by the same vehicle. By collecting these messages and analyzing the location history of a vehicle, malicious entities can infer the real identity of the vehicle or other sensitive information [6].

Many schemes attempt to prevent message linking by using such methods as dynamic pseudo-IDs that change every message or zero-knowledge signatures. Unfortunately, this is probably wasted effort. In order to provide collision avoidance, possibly the most critical feature of VANET safety applications, safety systems require message linking for path prediction. The major European intelligent transportation communications spec, ETSI TS 102 637-2 [7], includes an explicit sender ID fields to allow message linking in its basic communication messages. Furthermore, even if this information was not provided, as is the case in the competing SAE J2735 specification [8], it is possible to predict short-term position change using the position, heading, and speed information [9] and link the messages that way. For example, an attacker uses that information to predict the next position of the vehicle and assumes any message it receives with the predicted position was sent by the same vehicle.

While periodically changing pseudo-IDs in order to at least make linking more difficult is probably worthwhile, preventing all message linking is likely futile and at odds with the needs of many VANET applications. Accordingly preventing all message linking is not a necessary goal for VANET security. Instead, the focus of privacy in VANET systems should be protecting the real identities of vehicle drivers.

4) TRACING

Tracing refers to matching a message back to the vehicle that sent it. This can include revealing the real-world identity of the sender, which is also known as conditional privacy. While the real identities of drivers should be protected from other vehicles in the system, for the purposes of non-repudiation and revocation it is essential that some governing authority has the power to reveal the real identity of a message sender.

5) NON-REPUDIATION

The property of non-repudiation means that a vehicle cannot deny or otherwise hide the fact that it was the source of a message. Non-repudiation is required to properly identify malicious vehicles when they attempt to inject erroneous data or otherwise interfere with the VANET operation. It is especially critical for the detection of Sybil attacks. In a Sybil attack, a single vehicle masquerades as more than one vehicle, usually in an attempt to force the system into a false state. For example, a Sybil attack could create the illusion of heavy traffic or trigger a false accident report by ''out-voting'' honest vehicles [10].

6) REVOCATION

Many VANET systems organize their member vehicles into groups. These groups often have some shared secret that allows them to read encrypted messages and/or create message signatures. Revocation is the process of removing access to that shared secret from malicious vehicles or vehicles that no longer fit the requirements for group membership, usually due to leaving some geographic area. This can entail updating the group secret such that whatever information the revoked vehicle has is no longer sufficient to prove group membership or updating the secret and reissuing all keys to all vehicles in the group, minus the revoked vehicle. Some schemes use Certificate Revocation Lists (CRLs) that contain the IDs of revoked vehicles, but maintaining and transmitting a list to all vehicles is cumbersome compared with simply updating a shared secret or even reissuing all keys.

7) INSIDER ATTACK RESISTANCE

Because VANETs are used by the public and have highly dynamic membership, it is easier for attackers to join the system than it is in IoT applications where hardware nodes are difficult to physically access or where group membership is largely static. If an attacker steals or forges an identity certificate then they can freely join the system. As a result, entities at the OBU level must be considered fully untrusted. Their actions should be closely monitored

Another possibility to consider is attacks by compromised TAs or SPs. While top-level servers are easier to defend than OBU hardware because they are fewer in number and unlikely to be physically accessible to attackers, it is worth considering the risks posed by insider attacks at all levels. Compromised TAs could collude with malicious vehicles in order to admit them to the system. If key material is stolen from top-level servers, attackers could sign messages using the stolen keys in order to implicate innocent vehicles in attacks or perform Sybil attacks.

II. RELATED WORK

Most VANET schemes group vehicles with others in the same geographic area at the bottom of a two- or three-level hierarchy. Vehicles then request group membership upon entering the area and are granted access by entities at one of the upper levels. After authentication, vehicles receive the keys necessary to communicate within the group. These can be symmetric keys, asymmetric keys, or group keys.

Although broadcast messaging is usually desirable for group communication, some VANET schemes don't support it. These schemes typically use either one-to-one symmetric keys [11]–[13] or signcryption [14], [15]. In one-to-one symmetric key schemes, each vehicle shares a unique key with each other member of the group. A VANET group for a 1km radius circle – the communication range of the Wireless Access in Vehicular Environments (WAVE) standard [4] – could contain thousands of vehicles in a densely populated metropolitan area. This would require an impractical number of keys for vehicles within such a group as well as increased message traffic due to the need for unicast messaging. As for signcryption, while it has many advantages, it is less useful in the case of VANETs as it typically requires the public key of message receivers, which also limits it to unicast messaging.

Instead of allowing vehicles to communicate directly, a few schemes require RSUs to handle all communications. In one example [16], RSUs distribute symmetric keys that are unique

to each vehicle and vehicles can use these keys only to communicate with the RSU. Inserting an extra hop of communication and requiring RSUs to process all messages prior to retransmission adds extra latency to the system. In addition, because each vehicle has a unique key that it shares with the RSU, broadcast messaging is not possible.

Due to the desire for broadcast messaging in VANETs, most schemes use some form of group keys or group signatures. The simplest schemes in this category create a single, shared symmetric key that all members of the group use for communication with each other [17]–[23]. Unfortunately, VANET schemes where all members use the same key and generate identical signatures are highly vulnerable to insider attacks. When a malicious vehicle injects bad data or masquerades as other vehicles, it is very difficult to detect or attribute such attacks if all vehicles use the same key and there is no ID validation.

The final category of VANET schemes reviewed use traceable signatures. Schemes using traceable signatures attempt ensure that each message can be attributed back to the vehicle that sent it. They often use conditional privacy, where the message sender's identity is masked from the other vehicles in the system but can be revealed by a more trusted entity such as a group leader, RSU, or TA. Schemes in this category can be further subdivided into schemes that use elliptic curve pairings and schemes that do not.

Schemes using elliptic curve pairings include those proposed by Azees *et al.* [24], Vijayakumar *et al.* [25]–[27], Ahamed *et al.* [28], Zhang *et al.* [29], Lim *et al.* [30], and Funderburg and Lee [5]. The Azees *et al.* scheme uses pairings for confirming message integrity and anonymous, short-term identity certificates for authenticating the sender. It provides reliable tracing and non-repudiation, but the vehicle identity and authorization parameters are installed offline and cannot be revoked without revoking all registered vehicles. In addition, the TA knows all secret values used by each vehicle for signing messages so a compromised TA could forge signatures to execute an insider attack.

Although relatively efficient, the three Vijayakumar *et al.* schemes share the same shortcomings of the Azees *et al.* scheme. Namely, vehicles receive their private keys offline, which complicates revocation, and the TA contains all vehicles' private keys so they are vulnerable to forgery attacks if this database is breached. Finally, two of the Vijayakumar schemes, [25], [27], don't authenticate the pseudo-IDs (VANET license and FID) as part of the signature verification so a malicious vehicle could use a false pseudo-ID when signing messages to prevent tracing by the TA.

The scheme by Ahamed *et al.* uses pairings to validate message contents and senders, but doesn't include an explicit method of tracing the message source. Furthermore, it is also vulnerable to insider attacks in the case where vehicles' private keys are stolen from the TA.

Zhang C. *et al.* prevents insider attacks from compromising vehicle private keys by having RSUs certify the vehicles' public keys, rather than generating the vehicles' key pairs itself. After a vehicle has been authorized, and its public key has been certified, the vehicle signs messages which are then authenticated by other vehicles using pairings to check the validity of the signatures. The scheme supports batch verification, so it is relatively efficient, however, it does not provide quick tracing of message senders in case of dispute or to detect such attacks as masquerade attacks or Sybil attacks. Tracing is possible, but it requires a database search with one pairing calculation per vehicle stored in the database.

The final two pairing-based schemes, Lim *et al.* and Funderburg & Lee, both use the short group signatures first presented in Boneh *et al.* [31]. The TA generates a key pair for each vehicle that joins the system, and the vehicles sign and verify messages using pairings. The second scheme is more efficient than the first for signing and verifying messages due to caching of pairing values, but both schemes result in messages that are quickly traceable. The schemes share a vulnerability to insider attacks due to the TA's knowledge of all vehicles' key pairs.

The He *et al.* [32] scheme is the first member of the pairing-free category to discuss. In the He *et al.* scheme, the vehicle's real-world identity and the group private key are saved on a tamper-proof device (TPD). Each time a vehicle needs to sign a message, the vehicle's TPD generates a random pseudo-ID that incorporates the real-world identity and signs using that along with the group private key. While this scheme is efficient and ensures the vehicle cannot forge its real-world identity, it is vulnerable to insider attacks by a compromised TA as the TA can forge a signature for any vehicle given its knowledge of the vehicle's real-world identity and the group private key. In addition, the group private key is distributed offline, so there is no practical way to update that key for all vehicles in order to revoke a malicious vehicle.

More recent pairing-free schemes include two schemes proposed by Zhang J. *et al.*, which are both similar to the He *et al.* scheme with respect to signature generation and verification. In the first scheme [33], unlike the He *et al.* scheme, no TPDs are required. However, it lacks a direct way to trace the message sender as the tracing algorithm requires the TA to loop through a database of stored values to find a match and reveal the sender's real-world ID. Finally, as with the He *et al.* scheme, this scheme is vulnerable to insider attacks due to compromised TAs.

The second Zhang *et al.* scheme [34], uses the Chinese Remainder Theorem to distribute the group private key to the TPDs. This allows the scheme to revoke malicious vehicles as the group private key can be updated online, unlike in the case of the He *et al.* scheme. On the other hand, this scheme shares the He *et al.* scheme's weaknesses of reliance on TPDs and susceptance to insider attacks due to the TA's knowledge of the group private key and vehicle real-world identities.

In addition to the schemes proposed in the academic literature, government and industry are developing or have developed standards for VANET security. Two important English-language standards are IEEE 1609.2 "IEEE Standard for

Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages" [35], [36] and TSI TS 102 940 from ETSI "Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; Release 2" [37]. These standards began initial development prior to much of the academic security research focused on VANET, and they propose to use certificate hierarchies similar to public key infrastructure (PKI) models. In order to sign messages, OBUs are provided with a large number of pre-installed certificates or authorization tickets, which they can switch at set intervals in order to maintain some level of anonymity. The certificates can be traced in case of a dispute or malicious activity, but other vehicles cannot link them to the vehicle's real identity. Compared to academic schemes, these standards require more space due to the need to store multiple certificates/authorization tickets for message signing, and the revocation process may be more complicated, including the use of CRLs. On the other hand, the model of using certificates/authorization tickets in a PKI setting is well established so it is easier to implement and the security of such systems has been extensively studied and tested in real-world situations.

In comparison to our scheme proposed in [5], this work will present a new scheme that uses pseudonyms rather than Short Group Signatures as a base and therefore does not require pairings, which will result in much faster execution times. Furthermore, in our new scheme, the TA will not know the vehicles' private keys, in contrast to the scheme from [5]. In the previous scheme, the TA has full knowledge of all vehicles' private keys and the system is therefore vulnerable to attacks targeting the TA that result in the theft of key material.

III. PROPOSED SCHEME

Our scheme divides entities into three levels: TA, RSUs, and OBUs. The TA authenticates the OBUs and ensures the vehicles cannot forge identities when signing messages. OBUs create and sign messages containing vehicle telemetry and traffic data that are sent to neighboring vehicles as well as the TA. The RSUs are communications relay nodes and may be replaced by direct 5G connections between the OBUs and the internet as wireless technology evolves.

A. COMPONENTS

The proposed scheme uses the typical TA-RSU-OBU VANET hierarchy. We now will briefly summarize the roles of each level in our scheme:

1) TA LEVEL

The TA is a well-equipped central server that is connected to government databases in order to authenticate vehicles that wish to join the system. The TA is also responsible for validating vehicle keys in order to ensure a vehicle cannot sign a message using a false identity and tracing the message signers' real identities in case of a dispute. For practical reasons, the TA may actually consist of multiple, distributed servers, but conceptually they function as a single entity in this scheme.

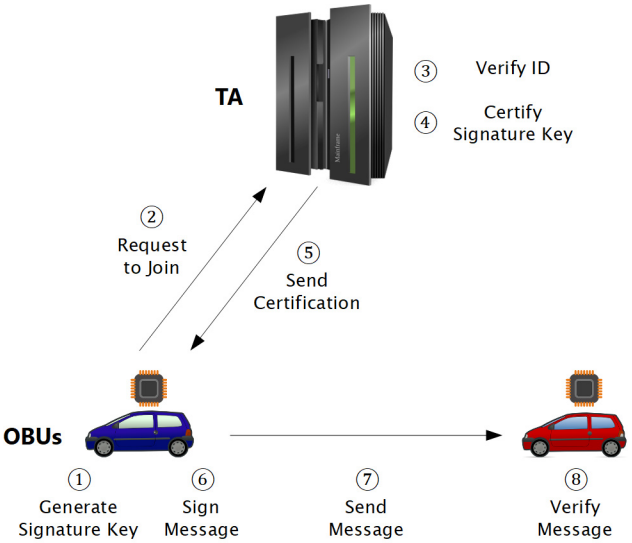


FIGURE 2. Process.

2) RSU LEVEL

RSUs in the proposed scheme are used to provide geographical groupings for the OBUs based on their locations, but serve no function beyond wireless messaging relays between the vehicles' radio signals and a hard-wired connection to the TA.

3) OBU LEVEL

OBUs are microchips installed in every vehicle that provide secure communications with other vehicles. OBUs contain the officially-signed certificates required to authenticate the vehicles when they request to join the system. They also generate and store keys for message signing, and interact with the TA in order to certify their keys, which is required to create valid signatures.

B. OVERVIEW

The sequence of the scheme is shown in Fig. 2. OBUs are placed in groups based on their distance from an RSU. Each RSU provides communications relays to the TA for all vehicles within its wireless signal range. When an OBU enters a new region and wishes to join a group, it sends a message with its signed, government-issued certificate containing the vehicle's real identity and a public key that the vehicle will use when signing group messages to the TA, called a signature key, via the relay RSU. The TA validates the identity certificate, stores a mapping of the vehicle's signature key to the real identity, certifies the vehicle's signature key for use in the group, and sends the signature key certification back to the vehicle.

When a vehicle wishes to send a message to the other group members, it signs the message using its private key, then broadcasts the message, along with its signature key

TABLE 1. Notations.

Symbol	Definition
P	Point on an Elliptic Curve
GK	Group Public Key
x	Group Private Key
i	Index of OBU
y	OBU i's Private Key
PK_i	OBU i's Signature Key
σ_{PKi}, A	OBU i's Signature Key Certification
M	Message
T	Timestamp
σ_M, B	Message Signature Parameters

and signature key certification. Message recipients use the signature key certification and group public key to validate the signature key, which ensures that a vehicle cannot use a forged identity to sign the message, and the signature key to validate the signature, which ensures that the message has not been tampered with and that a vehicle cannot use a stolen identity to sign a message.

C. DETAILS

The notations used in this paper are shown in Table 1.

1) INITIALIZATION

Prior to joining the system, vehicle owners obtain a signed vehicle registration certificate from the appropriate government authority. This certificate contains the identity of the vehicle owner and ensures that the TA can determine the real identity of any vehicle in the VANET in case of malicious behavior or other problems.

When vehicles join the system, they will be grouped with other vehicles in the same geographic area because of limitations on wireless transmissions and also so the burden of system management can be distributed across multiple TAs and RSUs. For each group, the responsible TA chooses a point, P, on an elliptic curve. The TA then generates a public/private key pair for the group as:

$$x \in \mathbb{Z}_p^*, \quad GK = x * P \tag{1}$$

The private key, x, is randomly selected and known only to the TA. Finally, the TA chooses a secure hash function H() that maps to $\mathbb{Z}_p^*$. The public parameters for the group will be P, GK, and H

2) VEHICLE JOINS A GROUP

When vehicle i enters a new region, first, it will generate a public/private key pair using the same method as the TA, where private key y is randomly chosen:

$$y \in \mathbb{Z}_p^*, \quad PK_i = y * P \tag{2}$$

The public key will be used for validating the vehicle's signature and will be referred to in this paper as the vehicle's signature key. The private key is known only to vehicle i and will be used to generate signatures.

After generating the key pair, vehicle i will send a message to the TA requesting to join the group. The message will contain vehicle i"s official registration certificate, received offline, and the vehicle's public key. The TA will receive the message and verify the vehicle's registration certificate. If it is valid, the TA will store a mapping of PK_i to the vehicle's registration information so that PK_i can be used to trace the owner's identity in case of malicious behavior or dispute.

Next, in order to prevent a malicious vehicle from thwarting the tracing by changing its public key later, the TA will choose a random number $a \in \mathbb{Z}_p^*$ and sign PK_i as follows:

$$A = a * P \tag{3}$$

$$\sigma_{PKi} = x + a * H(PK_i||A) \tag{4}$$

Finally, the TA will send σ_{PKi} and A to vehicle i.

3) VEHICLE SENDS A MESSAGE

When vehicle i sends a message, it uses its private key and the signature key certification parameters received from the TA in order to sign the message. The signature assures receivers that the message was sent by an authenticated member of the group and was not changed during transmission. In order to sign the message, the vehicle first chooses a random number $b \in \mathbb{Z}_p^*$ and generates a timestamp T. M is the message to sign. The signature is then generated as shown:

$$B = b * P \tag{5}$$

$$\sigma_M = \sigma_{PKi} + y + b * H(M||T||B) \tag{6}$$

After generating the signature, vehicle i broadcasts message M along with σ_M, PK_i, T, A, and B.

4) RECEIVERS VALIDATE THE MESSAGE

Any receiver of the message who wishes to validate it first checks the timestamp. If $T_{now} - T > T_{replay}$ then the message will be discarded as a potential replay attack. Next, receivers validate the signature by checking if the following equation holds:

$$\sigma_M * P = GK + A * H\,(PK_i||A) + PK_i + B * H(M||T||B) \tag{7}$$

The correctness of this equation can be seen from:

$$\begin{aligned}
\sigma_M * P &= (\sigma_{PKi} + y + b * H(M||T||B)) * P \\
&= ((x + a * H(PK_i||A)) + y + b * H(M||T||B)) * P \\
&= (x + a * H(PK_i||A) + y + b * H(M||T||B)) * P \\
&= (x * P + a * P * H(PK_i||A) + y * P + b * P \\
&\quad * H(M||T||B)) \\
&= GK + A * H(PK_i||A) + PK_i + B * H(M||T||B)
\end{aligned}$$

5) REVOCATION

As discussed in section I-B,7 "Insider Attack Resistance", VANETs need to be particularly concerned with the case

of vehicles behaving maliciously after gaining access to the system. When an insider attack is detected, the system must revoke that vehicle's ability to generate valid messages. In the proposed scheme, the TA will revoke malicious vehicles by randomly choosing a new group private key and regenerating the signature key certifications for all non-revoked vehicles. When a revoked vehicle attempts to generate a signature, σ'_M, using its old signature key and signature key certification with the new group public key, the signature validation will fail as follows.

First, the vehicle creates a signature using the old, pre-revocation, values:

$$\sigma'_M * P = (\sigma'_{PKi} + y' + b * H(M||T||B)) * P \tag{8}$$

Then, receivers test for message validation using the new, post-revocation, group key:

$$\sigma'_M * P = GK + A' * H(PK'_i||A') + PK'_i + B * H(M||T||B) \tag{9}$$

However,

$$\begin{aligned}
&\sigma'_M * P \\
&\quad = ((x' + a' * H(PK'_i||A')) + y' + b * H(M||T||B)) * P \\
&\quad = (x' + a' * H(PK'_i||A') + y' + b * H(M||T||B)) * P \\
&\quad = (x' * P + a' * P * H(PK'_i||A') + y' * P + b * P \\
&\qquad * H(M||T||B)) \\
&\quad = GK' + A' * H(PK'_i||A') + PK'_i + B * H(M||T||B)
\end{aligned}$$

Therefore, because the old group public key, GK', is not equal to the new group public key, GK, the validation will fail for revoked vehicles:

$$\begin{aligned}
&GK' + A' * H(PK'_i||A') + PK'_i + B * H\,(M\,||T||\,B) \\
&\qquad \neq GK + A' * H(PK'_i||A') + PK'_i + B * H(M||T||B)
\end{aligned}$$

IV. ANALYSIS

We will first present a detailed analysis of the proposed scheme in light of VANET security requirements. After that, we will analyze performance and signature size compared to similar schemes.

A. SCHEME SECURITY

1) INTEGRITY

The proposed scheme ensures message integrity by including the message as input to the hash used in the signature. If M is modified during transmission, then the final signature validation will fail as $H(M'||T||B)$ will not equal $H(M||T||B)$ when using a cryptographically secure hash function. Furthermore, a timestamp integrity check is also included with the message integrity check in order to prevent replay attacks by ensuring the timestamp cannot be modified without affecting the signature value.

2) AUTHENTICATION

The proposed scheme ensures vehicles that have not been authenticated by the TA cannot send messages within the system. Only the TA is capable of generating a valid signature key certification. While the value of GK is public, obtaining x from GK cannot be done without solving $GK = x * P$, which is the Elliptic Curve Discrete Logarithm Problem (ECDLP) [38]. If a malicious vehicle attempts to create a forged signature key certification, $\sigma'_{PKi} = x' + a' * H(PK_i||A')$, the signature validation check will fail as can be seen from the following:

$$\sigma'_M * P = (\sigma'_{PKi} + y + b * H\,(M|\,|T|\,|B)) * P \tag{10}$$

where substitution gives:

$$\begin{aligned}
&= ((x' + a' * H(PK_i||A')) + y + b * H(M|\,|T|\,|B)) * P \\
&= (x' + a' * H(PK_i||A') + y + b * H(M|\,|T|\,|B)) * P \\
&= (x' * P + a' * P * H(PK_i||A') + y * P + b * P \\
&\quad * H(M|\,|T|\,|B)) \\
&= GK' + A' * H(PK_i||A') + PK_i + B * H(M||T||B)
\end{aligned}$$

Therefore, the validation will fail because GK' calculated from the forged signature will not equal the group public key, GK, so:

$$\begin{aligned}
&GK' + A' * H(PK_i||A') + PK_i + B * H(M||T||B) \\
&\qquad \neq GK + A' * H\left(PK_i||A'\right) + PK_i + B * H(M||T||B)
\end{aligned}$$

3) PRIVACY

The proposed scheme ensures vehicle privacy by hiding the real-world identities of vehicle owners. Vehicles in the group are identified by their signature keys and only the TA has access to the vehicle registration information. It is not possible for any vehicle or RSU to map a vehicle's signature key to its registration information because the signature keys are generated using a random number that is unrelated to the vehicle identity.

4) TRACING

While vehicle identities are protected from other entities, the proposed scheme allows the TA to quickly trace the real-world identity of any vehicle committing, or suspected of, malicious behavior. The TA stores a mapping of signature keys to vehicle registration information. This allows a quick look-up of registration information when required. Such look-ups can also be used for the purpose of providing services such as toll road fee collection or auto insurance billing.

5) NON-REPUDIATION

As shown above in section 2 "Authentication", when using the proposed scheme it is not possible for a vehicle to forge a signature key certification and use a signature key that is unknown to the TA. In addition, it is not possible for a vehicle to "steal" the signature key of another vehicle

TABLE 2. Comparison of proposed scheme with existing schemes.

	He15 [32]	Azees17 [24]	Vijaya.17 [26]	ZhangC19 [29]	Lim19 [30]	ZhangJ20 [33]	ZhangJ21 [34]	Funder.21 [5]	Proposed
Direct Tracing	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
CRL-Free Revocation	No	No	No	Yes	No	No	Yes	Yes	Yes
Insider Attack Resistance	No	No	No	Yes	No	No	No	No	Yes
No TPD	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Pairing Free	Yes	No	No	No	No	Yes	Yes	No	Yes

and use that for an impersonation attack. When a vehicle signs a message, it sends σ_M, PK_i, T, A, and B along with the message itself, M. The values σ_{PKi}, y, and b are known only to the message signer. The values of y and b cannot be calculated from PK_i or B without solving the ECDLP. In addition, without knowing either y or b, the value of σ_{PKi} cannot be calculated from σ_M, so it is also unknown. Therefore, a vehicle that attempts to generate a signature using a stolen PK_i with random values for σ_{PKi} and y where $\sigma'_M = \sigma'_{PKi} + y' + b' * \mathrm{H}(M||T||B')$ will fail as shown:

$$\sigma'_M * P = (\sigma'_{PKi} + y' + b' * H\left(M||T||B'\right)) * P \quad (11)$$

where distribution gives:

$$\begin{aligned} &= \sigma'_{PKi} * P + y' * P + b' * P * H(M||T||B') \\ &= \sigma'_{PKi} * P + PK'_i + B' * H(M||T||B') \end{aligned}$$

And it can be seen that

$$\begin{aligned} &\sigma'_{PKi} * P + PK'_i + B' * H\left(M||T||B'\right) \\ &\quad \neq GK + A * H\left(PK_i||A\right) + PK_i + B' * H(M||T||B') \end{aligned}$$

Because a valid signature may only be generated with knowledge of the corresponding values of σ_{PKi}, y, and PK_i, a vehicle cannot claim their public key was falsely used to sign a message in their name.

6) INSIDER ATTACK RESISTANCE

Finally, the proposed scheme is resistant to insider attacks not only by other vehicles, as discussed previously in sections 2 "Authentication" and 5 "Non-Repudiation", but also by the theft of key material stored on the TA. In many VANET schemes, the TA is fully trusted and generates, or possess direct knowledge of, the private keys of all vehicles in the system. This makes such schemes vulnerable to insider attacks due to compromised TAs.

In the proposed scheme, the TA can generate a valid signature key certification for a vehicle's public key, but cannot use that key certification to generate a valid message signature without the vehicle's private key. Therefore, vehicles cannot perform a masquerade attack against other vehicles, even with the TA's assistance. If a compromised TA or a malicious vehicle attempts to create a signature without the private key y that corresponds to the signature key that received the certification, such that $\sigma'_M = \sigma_{PKi} + y' + b * \mathrm{H}(M||T||B)$, the signature validation check will fail due to the following:

$$\sigma'_M * P = (\sigma_{PKi} + y' + b * H(M||T||B)) * P \quad (12)$$

where substitution gives:

$$\begin{aligned} &= ((x + a * H(PK_i||A)) + y' + b * H(M||T||B)) * P \\ &= (x + a * H(PK_i||A) + y' + b * H(M||T||B)) * P \\ &= (x * P + a * P * H(PK_i||A) + y' * P + b * P \\ &\quad * H(M||T||B)) \\ &= GK + A * H(PK_i||A) + PK'_i + B * H(M||T||B) \end{aligned}$$

Validation will fail because $PK'_i \neq PK_i$.

While gaining control of a TA may be comparatively difficult, concentrating all of the private keys of all vehicles for a VANET in the TA would make the TA a particularly tempting target for key theft. An improperly secured key database could provide attackers with huge numbers of compromised keys to execute massive Sybil attacks or system-wide attacks on non-repudiation. In the proposed scheme, vehicles are the sole possessors of their own private keys. While the TA validates the signature keys, it cannot obtain the vehicles' corresponding private keys without solving the ECDLP. This makes the proposed scheme particularly secure in comparison to many existing VANET schemes with fully-trusted TAs.

7) SUMMARY

All schemes examined ensure message integrity, prevent vehicles from sending messages without prior authentication, protect the privacy of the members' real-world identities, and ensure vehicles can't sign messages with forged identities.

Table 2 shows a functionality comparison between the proposed scheme and recent existing schemes for VANET signatures. Only the proposed scheme protects non-repudiation by ensuring members can only create signatures that are guaranteed to be quickly traceable back to their real-world identities without using expensive pairing operations or abstract TPDs. In addition, the proposed scheme resists insider attacks due

TABLE 3. Execution times for cryptographic operations.

Operation	Execution Time (ms)
Addition in G_1 (Type 1)	0.0055
Addition in G_1 (Type 3)	0.0156
Addition in G_2 (Type 3)	0.0366
Scalar Multiplication in G_1 (Type 1)	1.0149
Scalar Multiplication in G_1 (Type 3)	3.8979
Scalar Multiplication in G_2 (Type 3)	8.7108
Map to Point in G_1 (Type 3)	2.4737
Pairing	28.3853
Multiplication in G_T	0.0597
Exponentiation in G_T	10.7267

to compromised TAs. The Zhang C. *et al.* scheme is the only other scheme to do this, but at the cost of expensive pairing operations.

B. SCHEME PERFORMANCE

In this section, the performance of the proposed scheme is compared to existing schemes. The timings were measured using the C MIRACL Core Cryptographic Library [39] running on an Intel Core i7-4790 processor at 3.6 GHz with 4.0 GB of RAM using the Windows 10 operating system. The resulting times for the non-negligible operations measured are shown in Table 3.

For schemes that do not require pairings, a Type 1 curve, ED25519, was used. For schemes that use pairings, a Type 3 Barreto-Naehrig curve, BN462, was used. Although the schemes with pairings require Type 2 curves as specified in order to meet the Strong Diffie-Hellman (SDH) assumption [40], Boneh and Boyen reformulated their definition of SDH to allow the use of Type 3 curves [41], which are generally more efficient [42]. Using a Type 3 curve in this analysis gives a fairer comparison to pairings-free schemes. Both ED25519 and BN462 provide 128-bit security [42], [43].

As can be seen from Fig. 3, on the tested hardware the schemes using pairings (shown with a dashed outline) were much slower for both signature generation and verification than pairing-free schemes. The Azees *et al.* scheme is significantly faster than the other pairings-based schemes for signing because it precomputes partial signatures for k messages in advance, but it has a similar speed to the others for signature verification. The pairing-free schemes were much faster than schemes using pairings in all cases but the aforementioned Azees *et al.* scheme for signing. Comparing only the pairing-free schemes it can be seen they have approximately the same cost as each other for both signature generation and verification.

The performance data shows that the proposed scheme has similar performance to existing schemes while providing additional features. It provides tracing without a costly table search, does not require a TPD, provides a simple means of revocation, and protects against insider attacks due to compromised TAs. It combines all of these features while maintaining performance equivalent to existing schemes without them.

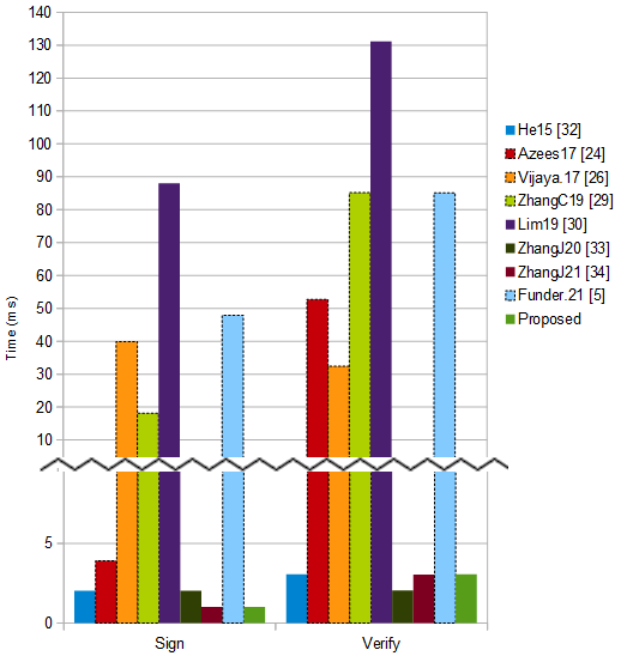


FIGURE 3. Performance comparison.

TABLE 4. Signature lengths.

Scheme	Signature Size (bytes)
He15 [32]	124
Azees17 [24]	848
Vijayakumar17 [26]	1044
ZhangC19 [29]	532
Lim19 [30]	508
ZhangJ20 [33]	124
ZhangJ21 [34]	84
Funderburg21 [5]	504
Proposed	144

C. SIGNATURE OVERHEAD

Finally, this section compares the cost in message size of adding the proposed signature to messages. In all schemes compared the message content is assumed to be identical so only the size of the signature portion will be considered. This analysis uses a size of 128 bytes for elements of G in pairing-based schemes and 40 bytes in pairing-free schemes [33]. Elements of $\mathbb{Z}_p^*$ are 20 bytes and timestamps are 4 bytes. The resulting signature sizes are shown in Table 4.

In the He *et al.* scheme, $AID_{i,1}$, $R_i \in G$ and $AID_{i,2}$, $\sigma_i \in \mathbb{Z}_p^*$. In Azees *et al.*, sig, Y_k, E_i, DID_{u_i}, γ_U, $\gamma_V \in G$ and c, λ, δ_1, $\delta_2 \in \mathbb{Z}_p^*$. In Vijayakumar *et al.*, Puk_{U_i}, Sig_i, J_1', J_2', J_3', J_4, G_v, $FI_{U_i} \in G$ and $SLC \in \mathbb{Z}_p^*$. In the Zhang C. *et al.* scheme, σ_i^1, σ_i^2, σ_i^3, $\sigma_i^4 \in G$ and $\sigma_i^5 \in \mathbb{Z}_p^*$. In Lim *et al.* and

Funderburg *et al.*, T_1, T_2, $T_3 \in G$ and c, s_α, s_β, s_x, s_{δ_1}, $s_{\delta_2} \in \mathbb{Z}_p^*$. Lim *et al.* includes an extra timestamp field that is absent in the second paper so the two signatures differ slightly in length. In the 2020 Zhang J. *et al.* scheme, $PID_{j,1}$, $Y_j \in G$ and $PID_{j,2}$, $S_j \in \mathbb{Z}_p^*$. In the 2021 Zhang J. *et al.* scheme, $ID_{i,1} \in G$ and $ID_{i,2}$, $\sigma_j \in \mathbb{Z}_p^*$. Finally, in the proposed scheme, PK_i, A, $B \in G$ and $\sigma_M \in \mathbb{Z}_p^*$.

The analysis shows that the signature length of the proposed scheme is comparable to other pairing-free schemes, all of which are much less than the signature length of pairing-based schemes. The proposed scheme adds resistance to TA-level insider attacks due to key material theft at the cost of only 20 additional bytes of signature length and without using the TPD required by two out of the three the other pairing-free schemes.

V. CONCLUSION

This paper presents a scheme using elliptic curves without pairings in order to sign and authenticate messages sent within a VANET group. When vehicles enter the coverage area of a VANET group, they contact a TA to validate their identity information and provide a signature key certification that can then be used to sign messages within the group. If a vehicle misbehaves, for example by reporting incorrect position or traffic data, its ability to sign messages for the group can be revoked by updating the group keys.

The scheme provides important VANET features, such as message integrity, sender authentication, and quick tracing. In contrast to other pairing-free schemes, it does not require abstract TPDs – which are unlikely to be achievable in real-world situations – in order to ensure non-repudiation and it offers CRL-free revocation. In addition, the proposed scheme protects against the case of insider attacks from a compromised TA by ensuring only a vehicle knows its own private key, while many other VANET systems are vulnerable to this avenue of attack.

In future research the problem of preserving driver privacy by preventing vehicle tracking in light of the location linking and prediction requirements of VANET anti-collision algorithms should be considered. If future anti-collision algorithms are developed that can function without also allowing vehicle location tracking, the proposed scheme should be updated in order to prevent the reuse of signature keys that allows message linking. In addition, while this scheme addresses the most likely type of TA-level insider attack, the possibility of a malicious TA distributing keys improperly to unauthorized vehicles should be considered by future schemes.

REFERENCES

[1] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019, doi: 10.3390/s19163589.

[2] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[3] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," in *Wireless Sensor and Mobile Ad-Hoc Networks*. Berlin, Germany: Springer, 2015, pp. 217–247, doi: 10.1007/978-1-4939-2468-4_10.

[4] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014, doi: 10.1016/j.vehcom.2014.05.001.

[5] L. E. Funderburg and I.-Y. Lee, "Efficient short group signatures for conditional privacy in vehicular ad hoc networks via ID caching and timed revocation," *IEEE Access*, vol. 9, pp. 118065–118076, 2021, doi: 10.1109/ACCESS.2021.3104861.

[6] M. Douriez, H. Doraiswamy, J. Freire, and C. T. Silva, "Anonymizing NYC taxi data: Does it matter?" in *Proc. DSAA*, Montreal, QC, Canada, Oct. 2016, pp. 140–148, doi: 10.1109/DSAA.2016.21.

[7] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI European Standard EN 302 637-2, Verion 1.3.2, 2014.

[8] B. Cronin, "Vehicle based data and availability," in *Proc. ITSPAC*, Washington, DC, USA: U.S. Department of Transportation, Oct. 2012, pp. 1–13. Accessed: May 8, 2021. [Online]. Available: https://www.its.dot.gov/itspac/october2012/PDF/data_availability.pdf

[9] R. Schubert, E. Richter, and G. Wanielik, "Comparison and evaluation of advanced motion models for vehicle tracking," in *Proc. FUSION*, Cologne, Germany, 2008, pp. 1–6.

[10] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks," in *Proc. MobiQuitous*, Philadelphia, PA, USA, 2007, pp. 1–8, doi: 10.1109/MOBIQ.2007.4451013.

[11] W. Xiong and B. Tang, "A cloud based three layer key management scheme for VANET," in *Proc. GSKI*, Chiang Mai, Thailand, 2017, pp. 574–587, doi: 10.1007/978-981-13-0896-3_57.

[12] T. Gao and J. Qi, "An anonymous access authentication scheme for VANETs based on ID-based group signature," in *Proc. BWCCA*, Taichung, Taiwan, 2018, pp. 490–497, doi: 10.1007/978-3-030-02613-4_43.

[13] Q. Li, C.-F. Hsu, K.-K. Raymond Choo, and D. He, "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 2019, Dec. 2019, Art. no. 7871067, doi: 10.1155/2019/7871067.

[14] F. Zhou, Y. Li, and Y. Ding, "Practical V2I secure communication schemes for heterogeneous VANETs," *Appl. Sci.*, vol. 9, no. 15, p. 3131, Aug. 2019, doi: 10.3390/app9153131.

[15] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11266–11280, Oct. 2020, doi: 10.1109/TVT.2020.3008781.

[16] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Feb. 2021, doi: 10.1155/2021/6679882.

[17] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–138, Mar. 2012, doi: 10.1109/TITS.2011.2164068.

[18] K. K. Chauhan, S. Kumar, and S. Kumar, "The design of a secure key management system in vehicular ad hoc networks," in *Proc. CICT*, Gwalior, India, Nov. 2017, pp. 1–6, doi: 10.1109/INFOCOMTECH.2017.8340636.

[19] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018, doi: 10.1016/j.future.2017.07.002.

[20] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Veh. Commun.*, vol. 14, pp. 15–25, Oct. 2018, doi: 10.1016/j.vehcom.2018.09.003.

[21] L. Liu, Y. Wang, J. Zhang, and Q. Yang, "A secure and efficient group key agreement scheme for VANET," *Sensors*, vol. 19, no. 3, p. 482, Jan. 2019, doi: 10.3390/s19030482.

[22] S. Paliwal and A. Chandrakar, "A conditional privacy preserving authentication and multi party group key establishment scheme for real-time application in VANETs," *Cryptol. ePrint Arch.*, pp. 1–27, Sep. 2019. [Online]. Available: http://ia.cr/2019/1041

[23] A. Mansour, K. M. Malik, A. Alkaff, and H. Kanaan, "ALMS: Asymmetric lightweight centralized group key management protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1663–1678, Mar. 2021, doi: 10.1109/TITS.2020.2975226.

[24] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017, doi: 10.1109/TITS.2016.2634623.

[25] P. Vijayakumar, M. Azees, and L. J. Deborah, "CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks," in *Proc. CSCloud*, New York, NY, USA, Nov. 2015, pp. 62–67, doi: 10.1109/CSCloud.2015.32.

[26] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2439–2450, 2017, doi: 10.1007/s10586-017-0848-x.

[27] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. P. C. Rodrigues, "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 4, 2021, doi: 10.1109/TITS.2021.3099488.

[28] A. B. S. Ahamed, N. Kanagaraj, and M. Azees, "EMBA: An efficient anonymous mutual and batch authentication schemes for vanets," in *Proc. ICICCT*, Coimbatore, India, Apr. 2018, pp. 1320–1326, doi: 10.1109/ICICCT.2018.8473110.

[29] C. Zhang, X. Xue, L. Feng, X. Zeng, and J. Ma, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access*, vol. 7, pp. 178310–178320, 2019, doi: 10.1109/ACCESS.2019.2958356.

[30] K. Lim, W. Liu, X. Wang, and J. Joung, "SSKM: Scalable and secure key management scheme for group signature based authentication and CRL in VANET," *Electronics*, vol. 8, no. 11, p. 1330, Nov. 2019, doi: 10.3390/electronics8111330.

[31] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. CRYPTO*, Santa Barbara, CA, USA, 2004, pp. 41–55, doi: 10.1007/978-3-540-28628-8_3.

[32] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015, doi: 10.1109/TIFS.2015.2473820.

[33] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7940–7954, Jul. 2020, doi: 10.1109/TVT.2020.2994144.

[34] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021, doi: 10.1109/TDSC.2019.2904274.

[35] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011, doi: 10.1109/JPROC.2011.2132790.

[36] W. Whyte, "IEEE 1609.2 and connected vehicle security: Standards making in a pocket universe," presented at the Secur. Standardization Res. Workshop, Gaithersburg, MD, USA: National Institute for Standards and Technology, 2016, doi: 10.13140/RG.2.2.30133.88802.

[37] *Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; Release 2*, Standard ETSI TS 102 940, Version 2.1.1, 2021.

[38] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 51–72, Jan. 2016, doi: 10.1007/s10623-015-0146-7.

[39] *MIRACL Core Cryptographic Library*. Accessed: Jul. 6, 2021. [Online]. Available: https://github.com/miracl/core

[40] A. L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in *Proc. CT-RSA*, San Francisco, CA, USA, 2009, pp. 309–324, doi: 10.1007/978-3-642-00862-7_21.

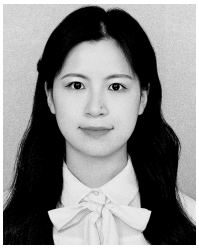
[41] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *J. Cryptol.*, vol. 21, no. 2, pp. 149–177, Apr. 2008, doi: 10.1007/s00145-007-9005-7.

[42] H. Okano, K. Emura, T. Ishibashi, T. Ohigashi, and T. Suzuki, "Implementation of a strongly robust identity-based encryption scheme over type-3 pairings," in *Proc. CANDAR*, Nagasaki, Japan, Nov. 2019, pp. 191–196, doi: 10.1109/CANDAR.2019.00032.

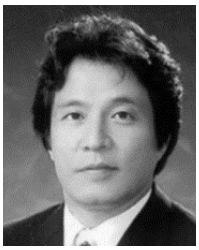
[43] K. Chalkias, F. Garillot, and V. Nikolaenko, "Taming the many EdDSAs," in *Security Standardisation Research*. Cham, Switzerland: Springer, 2020.

L. ELLEN FUNDERBURG received the B.S. degree in computer and systems engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 1999, and the M.S. degree in electrical and computer engineering from the University of Texas, Austin, TX, USA, in 2001. She is currently pursuing the Ph.D. degree with the Department of Software Convergence, Soonchunhyang University, Asan, South Korea.

She worked as a Senior Software Engineer, from 2001 to 2010. She has been a Lecturer with the Department of Software Convergence, Soonchunhyang University, since 2013. Her research interests include applications of the Internet of Things, group signature schemes, security of wireless communications, and VANET security.



HUIMIN REN received the B.S. degree in software engineering from Soonchunhyang University, Asan, South Korea, in 2020, and the B.S. degree in software engineering from the Anhui University of Chinese Medicine, Anhui, China. She is currently pursuing the M.S. degree with Soonchunhyang University. Her research interests include cryptographic protocols, key management, and authenticated group key agreement.



IM-YEONG LEE received the B.S. degree from Hongik University, Seoul, South Korea, in 1981, and the M.S. and Ph.D. degrees from the University of Osaka, Osaka, Japan, in 1986 and 1989, respectively. His research interests include information security, cryptographic protocols, information theory, and data communications.