IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 12, 2021, accepted August 11, 2021, date of publication August 16, 2021, date of current version August 31, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3104861

Efficient Short Group Signatures for Conditional Privacy in Vehicular Ad Hoc Networks via ID Caching and Timed Revocation

L. ELLEN FUNDERBURG 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) funded by the Ministry of Education under Grant NRF-019R1A2C1085718, in part by the Soonchunhyang University Research Fund, and in part by the Brain Korea 21 (BK21) FOUR (Fostering Outstanding Universities for Research) under Grant 5199990914048.

ABSTRACT Vehicular Ad hoc Networks (VANETs) are a subset of the Internet of Things (IoT) that are used in smart traffic applications. Due to their high speed, mobility, and exposure to the environment, the security requirements for VANETs result in the conflicting design goals of protecting member privacy while also ensuring non-repudiation. Group signature schemes can fulfill these requirements, but often at the cost of expensive bilinear pairing operations. Furthermore, the cost of updating the group key information can be costly. Accordingly, this paper has two goals. First, it presents a group signature scheme that has been modified to remove pairing operations by caching computed values, while still preserving the critical requirement of conditional privacy. Second, this paper presents an argument for the abandonment of perfect forward and backward secrecy in VANET schemes in order to prevent the generation of keys that are never used, or used only once, and reduce the twin burdens of excessive key recalculation and key redistribution on the system.

INDEX TERMS Short group signatures, conditional privacy, revocation, forward secrecy, backward secrecy, elliptic curve caching, VANET, timed key updates.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are a specialization of Mobile Ad hoc Networks (MANETs) [1] connecting vehicles with other vehicles as well as roadside infrastructure [2]. The goals of a VANET may include maintaining smooth traffic flow, improving safety for traffic as well as pedestrians, and providing comfort, entertainment, or quality of life services to drivers and passengers [3]. In a typical VANET, vehicles communicate via wireless connections with neighboring vehicles, vehicle-to-vehicle (V2V), as well as fixed-location devices located along the roadways, vehicle-to-infrastructure (V2I) [3]. The latter are typically called Road Side Units (RSUs). In general, VANETs usually consist of a top-level, fully-trusted server, known as a Trusted Authority (TA) or Service Provider (SP), a middle level of semi-trusted RSUs, and a final level of vehicles containing computers known as On-Board Units (OBUs).

While VANET is an application of Internet of Things (IoT), the security requirements of VANET are a bit different than other IoT systems. Most of the data collected from vehicles in a VANET does not contain sensitive information [4] and has low value for attackers. In general, the data are publicly observable quantities such as vehicle speed, heading, breaking status, etc. Additionally, the data are usually ephemeral so protecting access to previously collected data is also not a priority. A much more costly, and potentially dangerous, class of attacks on VANET involve the injection of false data into the system, and in particular Sybil attacks [5]. This places a high priority on securing the identity and authentication of message sources [6]. Conversely, another attack of significant concern is malicious entities tracking individual vehicles, which places a seemingly contradictory importance on privacy [7]. Finally, the highly dynamic nature of the system makes efficiency even more important than usual as algorithms must execute quickly to ensure the updates do not arrive too late to be of use.

As a practical matter, VANETs often divide vehicles into groups based on RSU locations. Accordingly, there are many

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

VANET schemes using group key sharing or group signatures [8]. In these schemes, the questions of how and when to update the group keys are critical. In many IoT applications, such as smart factories or smart power grids, the groups are static or change only slowly over time. However, in the case of VANET, group membership is highly dynamic. Depending on the traffic situation, group membership may change as, or possibly even more, frequently than the standard rate of safety message updates [9].

When groups change, group key and group signature schemes must concern themselves with the issues of forward secrecy, joining members can't read old messages, and backward secrecy, departed members can't read new messages [10]. The concept of backward secrecy can be extended in the case of group signatures to be departed members can't sign future messages. The decision of when and when not to update the group keys is critical for performance, but not often closely examined by VANET group key schemes. In particular, some schemes assume group keys will update every time a vehicle leaves [2], or even every time group membership changes [11], [12], which may be impractical given the highly-dynamic nature of VANET group membership.

This paper has two main goals: 1) We present a scheme increasing the efficiency of group signatures via a method of caching pairing calculations, as pairings are a relatively slow mathematical operation. 2) We propose to use a fixed interval for triggering group key updates instead of perfectly preserving forward and backward secrecy, and provide a thorough analysis in support of this proposition over other methods.

The remainder of the paper is organized as follows. Section II presents a summary of recent work on the topic. Section III contains the proposed scheme. Section IV gives an analysis of our scheme and evidence in support of fixed interval group key updates. Section V concludes the paper.

II. RELATED WORK

VANET schemes can be primarily divided into schemes using group keys and schemes using group signatures. Group key schemes focus on efficient group key agreement and rekeying algorithms. They often use symmetric group keys without verification of the sender's true identity, only verifying that they are in possession of the current group key. Group signature schemes, on the other hand, attempt to also track the identity of the message sender and frequently use zero-knowledge proofs, where the sender proves possession of a secret without revealing anything about that secret, with bilinear pairings in order to provide conditional privacy. The sender's identity is protected from other group members, but the possessor of the tracing key can reveal the identity in cases of malicious behavior or disputes.

As noted above, many VANET schemes propose to use symmetric group keys following vehicle authentication. While using symmetric group keys makes for quick encryption and decryption times, there is no way to guarantee non-repudiation. All vehicles in the system have identical keys and any identifying information included in the message could have been forged or stolen. This results in a system that is highly vulnerable to the injection of bad data, without a reliable way to trace and remove the offending vehicles even in the case such data is detected. For example, among recently proposed group key schemes, schemes by Cui *et al.* [13], Islam *et al.* [14], Liu *et al.* [15], and Paliwal and Chandrakar [16] assign traceable pseudo-IDs to vehicles, but the identities are only authenticated when the vehicle joins (and for some schemes when it leaves) a group. When the vehicles are within the system, they are free to create mayhem. Without per-message pseudo-ID authentication, malicious vehicles could use fake identities to appear as multiple vehicles or copy the identities of other vehicles for use in impersonation attacks. While join-time authentication is an important layer of security, it is reasonable to expect that a malicious entity may obtain valid credentials through offline theft or forgery. Therefore, non-repudiation and traceability are important features of VANET systems, and vehicles should not be considered fully-trusted even after their credentials have been authenticated.

In order to provide authentication, privacy, and non-repudiation for messages by vehicles after they have joined the system, some VANET schemes use group signatures with conditional privacy. With conditional privacy, vehicle identities are protected from other vehicles but may be revealed by a trusted entity. Many of these schemes use bilinear pairing operations. One scheme using pairings for privacy preserving authentication is the DIKE scheme by Lu *et al.* [2]. Unfortunately, this scheme contains no tracing key, and it is not possible to entirely revoke the privacy for a vehicle and reveal its true identity. In this case, the scheme can only reveal if a malicious entity is attempting to join the group multiple times using the same private key or after being previously revoked. The Alimohammadi & Pouyan scheme [17] uses the same basic algorithm, but applies it to detecting duplicated messages rather than duplicated join request. This scheme shares the same problem that there is no mechanism for tracing the true identity of the offending entity, only detecting the attempt.

Zhang *et al.* proposed a different scheme using pairings for privacy preserving signatures [18]. In this scheme, RSUs can trace the identity of malicious nodes, however the trace requires up to n pairing operations, where n is the number of vehicles in the group. Signature verification also requires 3 pairing operations, although the verifications may be batched.

Another scheme using pairings was proposed by Azees *et al.* in [19]. Certificates containing pseudo-IDs are sent along with each message to provide authentication. There is only one pseudo-ID per vehicle and the IDs are included on the certificates, so it is easy for other vehicles to link messages from the same sender. In addition, while pairings are not used for authentication, they are used for checking message integrity and $n + 1$ pairings are required for n messages. Finally, while the TA can reveal the true identity of a malicious node, there is no mechanism for revoking the certificates of such nodes.

The short group signature algorithm proposed by Boneh, Boyen, and Shacham (BBS) [20] provides conditional privacy preservation and forms the basis of the Lim *et al.* [21] and Hao *et al.* [22] group signature schemes. These BBS signatures have the advantage of providing a tracing key that may be used to reveal the identities of message signers. However, they require pairing operations to authenticate the signatures, which are relatively expensive mathematical operations.

While many VANET signature schemes use elliptic curve pairings to provide authenticated conditional privacy, Zhong *et al.* [23] proposed a scheme without them. In the Zhong scheme, the RSU for the group authenticates the signatures and broadcasts a Bloom filter list of valid and invalid messages to the vehicles. This method requires RSUs to issue validation messages for every vehicle message before other vehicles will process it, which increases message traffic and creates a delay in time-critical V2V message processing as vehicles wait for the message confirmation. The use of a Bloom filter also introduces the problem of false positives.

Another set of schemes uses individual signatures, rather than group signatures, to validate the messages. These schemes use traceable pseudo-IDs in order to hide the origin of the messages from other vehicles in the system. Two schemes using similar signatures were proposed by Zhang *et al.* [24] and Cui *et al.* [25]. The Zhang scheme uses the Chinese Remainder Theorem in order to quickly and efficiently handle both initial key distribution and key updates when group members change. The Cui scheme focuses on the use of content sharing among neighboring vehicles in order to reduce the network burden of accessing content from distant servers. In both schemes, vehicles create traceable pseudo-IDs for message signing, but there is no authentication in the signatures of the real IDs used to create the pseudo-IDs. Malicious vehicles could use random numbers in place of their real identifiers in order to create untraceable pseudo-IDs. The schemes assume a theoretical tamper-proof device in order to prevent this behavior.

Zhang *et al.* [26] present another scheme in this category. Their scheme involves a future-facing system that uses selected vehicles as edge nodes in order to take advantage of 5G technology and remove the need for cumbersome RSUs. As with the previous two schemes, this scheme does not validate the real IDs (5G_ID) during the signature verification phase. Therefore, a malicious vehicle could sign a message using a random value for its "real" identifier and remain untraceable. This scheme does have an advantage over the previous two in that it is possible for the TA to detect a fake real ID given a message signature. However, the messages would still have been received and processed by the vehicles in the group before the TA could detect the problem. In addition, this requires the TA to check all messages from all vehicles in the system to detect a problem. Finally, the TA can only detect fake IDs by looping through a database of stored identity tuples in order to confirm that none of the real IDs stored match the "real" ID used for signing. As the number of registered vehicles in the system grows, it will become increasingly difficult to detect fake identities in real-time.

A final category of VANET schemes uses methods that preclude broadcast messaging, such as asymmetric encryption or 1:1 symmetric keys for communication between each vehicle pair. One example is signcryption schemes such as those proposed in Zhou *et al.* [27] and Ali *et al.* [28], which require the public key of the receiver. Schemes using 1:1 symmetric keys include Xiong and Tang [29] and Li *et al.* [30]. Due to the large group sizes, high speeds, and time criticality of the data, schemes that lack support for broadcast communication to anonymous receivers are impractical for VANET applications. Furthermore, the above schemes require unique keys for every member of the system, which presents a risk to privacy.

To overcome the shortcomings of the schemes discussed in this section, we propose a new scheme that uses the caching of pre-computed bilinear pairing values and restricts routine group secret updates to timed intervals. These modifications preserve the advantages of existing schemes with regards to message authentication and conditional privacy while providing increased efficiency. A table comparing the proposed scheme with recent similar schemes is included in the Analysis section.

III. PROPOSED SCHEME

The basis of our scheme is a system using Boneh, Boyen, and Shacham short group signatures [20] that has been configured for detecting Sybil attacks as described in [9]. In a Sybil attack a vehicle sends messages appearing to come from many different vehicles in order to create the illusion of additional traffic or out-vote honest vehicles to create erroneous condition reports [31].

The system used in this scheme consists of 3 levels as shown in Fig. 1: a top level with one or more TAs that control the group master keys, a middle level of more numerous

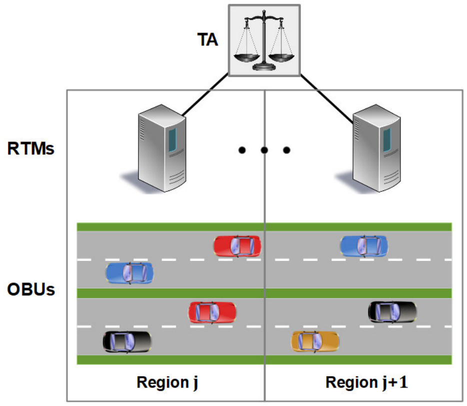


FIGURE 1. System Hierarchy.

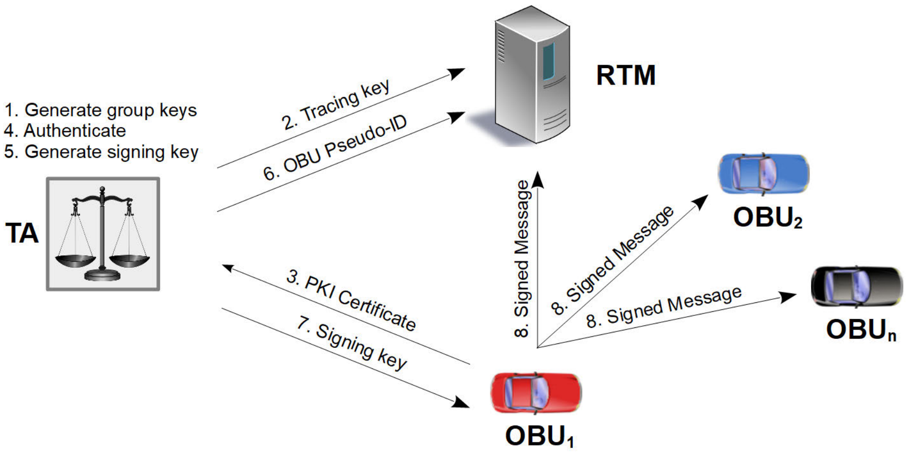


FIGURE 2. Messaging.

Regional Traffic Monitors (RTMs) that manage and monitor the vehicles within their respective geographic coverage areas, and a final level for the OBUs. In this system, the RSUs are only semi-trusted relay nodes that convey the short-range wireless communications of the vehicles to the RTMs or TAs..

All OBUs within a single RTM's geographic coverage area form a group. The OBUs communicate with each other and that RTM using privacy-preserving group signatures via a Dedicated Short-Range Communication (DSRC) standard such as IEEE 802.11p for Wireless Access in Vehicular Environments (WAVE) [32]. The RTM is responsible for monitoring the group to detect Sybil attacks, as well as other malicious behavior, and reporting traffic and road conditions to other parts of the system.

A. OVERVIEW

The TA initially generates the group public, master, and tracing keys for each RTM. Each tracing key is distributed to the corresponding RTM, but the master keys are held by the TA so that semi-trusted RTMs may not generate group keys. When an OBU enters the coverage area of an RTM, the OBU contacts the TA in order to authenticate its identity and receive a group secret key to use for signing messages within that RTM group. The TA notifies the appropriate RTM of the new group member, and sends the pseudo-ID for that OBU to that RTM. The RTM can then use the tracing key to monitor message signatures and detect when an OBU is sending more messages than it should in an attempt to perform a Sybil attack. In the event a Sybil attack, or any other malicious behavior is detected, the RTM can report the pseudo-ID of the malicious node to the TA, which can regenerate group keys to exclude the malicious node as well as map the pseudo-ID of the OBU to its real-world ID for reporting to law enforcement or other authorities.

The scheme presented here differs from the system in [9] and other schemes using BBS signatures because it caches some of the pairing calculations to reduce the cost of signature verification. In this scheme, a single pairing operation is required the first time an OBU signature is verified, but all subsequent signature verifications for that OBU are pairing free.

The proposed scheme consists of 8 steps, as can be seen in Fig. 2: 1) The TA generates the group public parameters as well as the master and tracing keys. 2) The tracing key is sent to the RTM in charge of the group. 3) An OBU wishing to join the group sends its identification to the TA via an RSU relay or direct 5G connection to the internet. 4) The TA authenticates the OBU, and 5) generates a private group signing key for that OBU. 6) The TA informs the RTM of the OBU joining the group. 7) The TA sends the signing key to the OBU. 8) The OBU sends messages to the RTM and other group members signed with its signing key.

B. DETAILS

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

TABLE 1. Notations.

Symbol	Definition
γ_j	Master key for the group in the region of RTM j
p_g, p_{1j}, p_{2j}	Precomputed pairings for group j
ζ_{1j}, ζ_{2j}	Tracing key for group j
A_{ji}	Pseudo-ID for OBU i in group j
p_{ji}	Precomputed pairing for OBU i in group j
α, β	Random values for masking the pseudo-ID
T_1, T_2, T_3	Masked pseudo-ID
H	Publicly known hash function
M	Message
c	Challenge
σ	Signature

1) BILINEAR MAPS

For each RTM, G_1 and G_2 are two bilinear, multiplicative, cyclic groups of prime order p. g_1 is a generator of G_1 and g_2

is a generator of G_2. e is a computable map $e : G_1 \times G_2 \rightarrow G_T$ and $e(g_1, g_2) \neq 1$.

2) INITIALIZATION

For each RTM, the TA configures a signature group. The TA randomly selects $h_j \leftarrow G_1 \backslash \{1_{G_1}\}$ and $\zeta_{1j}, \zeta_{2j} \leftarrow \mathbb{Z}_p^*$ and sets $u_j, v_j \in G_1$ such that

$$u_j^{\zeta_{1j}} = v_j^{\zeta_{2j}} = h_j. \tag{1}$$

Then it randomly selects the group master key $\gamma_j \leftarrow \mathbb{Z}_p^*$ and sets

$$w_j = g_2^{\gamma_j}. \tag{2}$$

In order to reduce pairing computations when generating and evaluating signatures, the TA also precomputes the pairings [20]

$$p_{1j} = e\left(h_j, w_j\right), \tag{3}$$

$$p_{2j} = e\left(h_j, g_2\right), \tag{4}$$

$$p_g = e\left(g_1, g_2\right). \tag{5}$$

The public parameters for group j are $(g_1, g_2, p_g, h_j, u_j, v_j, w_j, p_{1j}, p_{2j})$ and the tracing key is (ζ_{1j}, ζ_{2j}). The public parameters are distributed to all entities in the group, as well as new OBUs on joining. The tracing key is sent to the RTM in charge of group j, RTM$_j$.

3) OBU JOINING

When an OBU enters an RTM coverage area, the OBU contacts the TA to obtain its group signature key for that RTM. The TA authenticates the real identity of the OBU via a Public Key Infrastructure (PKI). Offline, each OBU receives an identity certificate signed by an issuing authority when the vehicle is registered with the government. When an OBU contacts the TA in order to join an RTM's group, the TA checks the signature of that certificate in order to verify the real identity of the OBU. If the certificate is valid, the TA uses the public key included with the certificate to establish a secure channel with the OBU. Note that this certificate is used only for the initial authentication step.

After the OBU's real identity is verified as being allowed to join the system, the TA generates a private signing key for the OBU by randomly selecting $x_{ji} \leftarrow \mathbb{Z}_p^*$ then calculating the pseudo-ID for the OBU as

$$A_{ji} \leftarrow g_1^{1/(\gamma_j + x_{ji})}, \tag{6}$$

where j is the RTM group and i is the OBU. Additionally, $p_{ji} = e\left(A_{ji}, g_2\right)$ will be precomputed. The private signing key for OBU$_i$ is then (A_{ji}, x_{ji}, p_{ji}).

The private signing key and group public parameters are then encrypted with the public key from the OBU's PKI certificate and sent securely to the OBU. The pseudo-ID for the OBU, A_{ji}, is also sent to the RTM via a secure channel. The second component of the OBU's signing key, x_{ji}, will not be known by the RTM.

4) SIGNATURE GENERATION

Following the BBS short group signature algorithm, when an OBU wants to send a message, it signs the message using its private signing key as follows:

1. Choose random values for $\alpha, \beta \leftarrow \mathbb{Z}_p$.
2. Compute $T_1 \leftarrow u_j^{\alpha}$, $T_2 \leftarrow v_j^{\beta}$, $T_3 \leftarrow A_{ji} h_j^{\alpha+\beta}$, $\delta_1 \leftarrow x_{ji}\alpha$, and $\delta_2 \leftarrow x_{ji}\beta$.
3. Choose random values for $r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \leftarrow \mathbb{Z}_p$.
4. Compute $R_1 \leftarrow u_j^{r_\alpha}$, $R_2 \leftarrow v_j^{r_\beta}$, $R_3 \leftarrow e\left(T_3, g_2\right)^{r_x} \cdot e\left(h_j, w_j\right)^{-r_\alpha - r_\beta} \cdot e\left(h_j, g_2\right)^{-r_{\delta_1} - r_{\delta_2}}$, $R_4 \leftarrow T_1^{r_x} \cdot u_j^{-r_{\delta_1}}$, and $R_5 \leftarrow T_2^{r_x} \cdot v_j^{-r_{\delta_2}}$.
5. Construct a challenge value using a publicly known hash function and the values computed above: $c \leftarrow H\left(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5\right) \in \mathbb{Z}_p$.
6. Compute $s_\alpha = r_\alpha + c\alpha$, $s_\beta = r_\beta + c\beta$, $s_x = r_x + cx_{ji}$, $s_{\delta_1} = r_{\delta_1} + c\delta_1$, and $s_{\delta_2} = r_{\delta_2} + c\delta_2$.
7. Set the final signature value as $\sigma \leftarrow (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$.

This creates a zero-knowledge proof of signature. Without access to the tracing key, verifiers cannot know the pseudo-ID of the OBU that signed the message. They can only know that the message was signed by an OBU with a valid private key. This prevents malicious OBUs from impersonating the signer by reusing its pseudo-ID, as well as providing some privacy to the OBU.

The pairing calculations can be completely eliminated from message signing [20]. The pairings using g_2, h_j, and w_j were included in the public parameters, so the R_3 calculation becomes

$$R_3 \leftarrow e\left(T_3, g_2\right)^{r_x} \cdot p_{1j}^{-r_\alpha - r_\beta} \cdot p_{2j}^{-r_{\delta_1} - r_{\delta_2}}. \tag{7}$$

Furthermore, the $e\left(T_3, g_2\right)$ pairing can also be eliminated by using the precomputed pairing provided as part of the private signing key [20]. Substitute $A_{ji} h_j^{\alpha+\beta}$ for T_3 to get

$$e\left(A_{ji} h_j^{\alpha+\beta}, g_2\right) \tag{8}$$

and separate the terms into

$$e\left(A_{ji}, g_2\right) e\left(h_j^{\alpha+\beta}, g_2\right). \tag{9}$$

Then it can be seen that both pairings can be done using precomputed values

$$e\left(A_{ji}, g_2\right) e\left(h_j, g_2\right)^{\alpha+\beta}. \tag{10}$$

This makes the final R_3 calculation

$$R_3 \leftarrow \left(p_{ji} \cdot p_{2j}^{\alpha+\beta}\right)^{r_x} \cdot p_{1j}^{-r_\alpha - r_\beta} \cdot p_{2j}^{-r_{\delta_1} - r_{\delta_2}}. \tag{11}$$

For reasons detailed in the next section, Signature Verification, in this scheme random values of α and β will only be used for the initial signature. Subsequent signatures will reuse the same α and β values. This will greatly increase the efficiency of the algorithm at the potential cost of some loss of privacy due to the values of the T parameters remaining constant across all messages signed by the same OBU. This trade-off, including the reasons that this weakening of privacy is not as consequential as might be feared at first glance, is discussed further in the Analysis section.

5) SIGNATURE VERIFICATION

When group members receive a message, they can verify the signature as follows:

1. Compute $\tilde{R}_1 \leftarrow u_j^{s_\alpha}/T_1^c$, $\tilde{R}_2 \leftarrow v_j^{s_\beta}/T_2^c$, $\tilde{R}_3 \leftarrow e(T_3, g_2)^{s_x} \cdot e\left(h_j, w_j\right)^{-s_\alpha - s_\beta} \cdot e\left(h_j, g_2\right)^{-s_{\delta_1} - s_{\delta_2}} \cdot \left(\frac{e(T_3,w_j)}{e(g_1,g_2)}\right)^c$, $\tilde{R}_4 \leftarrow T_1^{s_x}/u_j^{s_{\delta_1}}$, and $\tilde{R}_5 \leftarrow T_2^{s_x}/v_j^{s_{\delta_2}}$.
2. Verify the challenge by checking $c = H(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$.

As in the case of signature generation, several pairings can be eliminated from the verification process by using the precomputed values provided as part of the public parameters. However, unlike in the case of signature generation, two pairings remain, $e(T_3, g_2)$ and $e\left(T_3, w_j\right)$. These pairings can be combined into a single pairing [20],

$$e\left(T_3, w_j^c g_2^{s_x}\right). \tag{12}$$

This can be seen by rewriting the pairings as $e\left(T_3, g_2^{s_x}\right)$ and $e\left(T_3, w_j^c\right)$ then combining them. The $\tilde{R}_3$ calculation can then be written as

$$e\left(T_3, w_j^c g_2^{s_x}\right) \cdot p_{1j}^{-s_\alpha - s_\beta} \cdot p_{2j}^{-s_{\delta_1} - s_{\delta_2}} \cdot p_g^{-c}. \tag{13}$$

While a single pairing is much better than five, pairings are still very expensive compared to other mathematical operations [13], [23], [33]. In order to achieve performance similar to a pairing-free algorithm, while retaining the critical security features provided by group signatures, we propose to cache the T_3 pairing.

In the original BBS short group signature scheme, T_3 changed with every signature. In the proposed scheme, signers will use constant values for T_3. With T_3 constant, verifiers can compute the T_3 pairing just once, the first time a message is received from that signer, and cache that value. Subsequent messages from the same signer can accordingly be verified without any pairing calculations.

6) TRACING

When malicious activity is detected, an RTM can use the tracing key to unmask the pseudo-ID of the offending node as shown:

$$A_{ji} \leftarrow T_3/(T_1^{\zeta_{1j}} \cdot T_2^{\zeta_{2j}}). \tag{14}$$

The pseudo-ID is reported to the TA, which regenerates the group keys using the steps above for Initialization and OBU Joining, maps the pseudo-ID to a real-world ID, and reports the real-world ID to the appropriate agencies. A list of banned IDs is maintained by the TAs and these IDs will not be allowed to rejoin the system.

7) OBU LEAVING

When an OBU leaves the group naturally, i.e. by exiting the area or disconnecting from the system, no action is taken. Instead, the group keys will be periodically updated at rate t_{re-key}, which can be determined according to the traffic density and infrastructure capabilities in an installed area.

As discussed below in the Analysis section, the highly ephemeral nature of groups in VANET makes it extremely inefficient to perfectly preserve forward and backward secrecy, and the nature of the message contents makes it unnecessary. The main goal of a VANET group key scheme should be to prevent malicious nodes from injecting false data or otherwise corrupting the system. Accordingly, valuable bandwidth and computation time should not be expended to immediately remove group privileges from OBUs that traversed the region without exhibiting any malicious behavior.

On the other hand, when a malicious node is detected its access to the system will be immediately removed. The RTM will notify the TA of the malicious node and the TA will regenerate and reissue group keys for all other OBUs following the same steps described above in Initialization and OBU Joining.

IV. ANALYSIS

A. SCHEME SECURITY AND EFFICIENCY

VANET security schemes should seek to balance the opposing needs of authentication/non-repudiation and privacy. Authentication and non-repudiation prevent the injection of potentially dangerous false data into the system, while protecting privacy is necessary to prevent the stalking or targeting of individual users. In addition, efficiency is particularly important in VANET applications due to the time-sensitive nature and volume of the data. Table 2 shows a comparison of the proposed scheme with other recently proposed schemes.

1) AUTHENTICATION

In order to forge a signature, an attacker must create a valid signature with an arbitrary value for one half of the $\left(A_{ji}, x_{ji}\right)$ pair without knowing the master key. If an attacker chooses an arbitrary value for A_{ji}. In order to obtain a matching x_{ji} the attacker must invert (6), but without knowing the master key, the value of x_{ji} that successfully completes the challenge cannot be distinguished from a random member of the set $\mathbb{Z}_p$. The same holds if the attacker chooses an arbitrary x_{ji} and attempts to obtain the corresponding A_{ji}. If the value of γ_j used to compute A_{ji} does not match the value of γ_j used to compute w_j the $\tilde{R}_3$ challenge will fail and the signature will be flagged as invalid. Furthermore, obtaining the γ_j from (2) requires solving the Discrete Logarithm Problem.

2) NON-REPUDIATION

The property of non-repudiation holds for the signatures. After a valid signature has been produced and authenticated, a vehicle cannot plausibly deny producing that signature when its pseudo-ID, A_{ji}, has been revealed via the tracing key.

TABLE 2. Comparison of proposed scheme with existing schemes N/A = not applicable.

	Cui18 [13]	Liu19 [15]	Paliwal19 [16]	Zhang19 [18]	Lim19 [21]	Zhang20 [26]	Zhang21 [24]	Proposed
Message Authentication	Symmetric	Symmetric	Symmetric	ECC	BBS	ECC	ECC	Cached BBS
Signatures	No	No	No	Yes	Yes	Yes	Yes	Yes
Tracing	No	No	No	Yes	Yes	Yes	Yes	Yes
Tracing Method	N/A	N/A	N/A	Table Loop	Direct	Table Loop	Direct	Direct
Real Identity Authentication	No	No	No	Yes	Yes	No	No	Yes
Signature Pairings	N/A	N/A	N/A	0	3n	0	0	0
Verification Pairings	N/A	N/A	N/A	3n, 3 batched	5n	0	0	1st message only
Key Update Trigger	Always	Always	Always	Always	Never	Always	Always	Timed

First, a vehicle cannot produce a valid signature without including an A_{ji} value calculated using the master key, γ_j. If a random value is used for A_{ji}, the $\tilde{R}_3$ portion of the challenge will fail. In order to pass the $\tilde{R}_3$ challenge,

$$e\left(A_{ji}, w_j g_2^{x_{ji}}\right) \tag{15}$$

must equal

$$e\left(g_1, g_2\right). [20] \tag{16}$$

For the first pairing, substitution yields

$$e\left(g_1^{1/(\gamma_j+x_{ji})}, g_2^{\gamma_j} g_2^{x_{ji}}\right), \tag{17}$$

and by rearranging the terms to

$$e\left(g_1^{-\gamma_j-x_{ji}}, g_2^{\gamma_j+x_{ji}}\right) \tag{18}$$

it can be seen that value of γ_j used to compute A_{ji} must equal the value of γ_j used to compute w_j.

Second, a vehicle cannot reuse the T_1, T_2, T_3 values from another vehicle's signature. Computing the value of A_{ji} from T_1, T_2, T_3 without the tracing key requires solving the Decision Linear Problem [20]. Furthermore, even if a malicious vehicle were able to obtain the A_{ji} for another vehicle, the challenge will fail without the corresponding value of x_{ji}, as seen from the $\tilde{R}_3$ challenge above in (17) where the value of x_{ji} in $g_2^{x_{ji}}$ must match the x_{ji} used to compute A_{ji}.

Third, a vehicle cannot reuse the signature of another vehicle. The challenge hash calculation includes the message contents, M; therefore, the signature value will change for each message. A malicious vehicle can merely replay an identical message, which is easily detected through the use of timestamps or incrementing message serial numbers, for example.

Fourth, a malicious vehicle cannot collude with a malicious RSU in order to steal the A_{ji} of another vehicle (via the RSU's access to the tracing key) and use that to create a valid signature. The challenge will fail without knowledge of the corresponding x_{ji} value as discussed in the second point.

Finally, a vehicle cannot use its own private signature key values A_{ji} and x_{ji} to compute the value of the TA's master key from (6) because that requires solving the Discrete Logarithm Problem to obtain a value for $1/(\gamma_j+x_{ji})$ before solving for γ_j.

3) PRIVACY

The proposed scheme preserves the over-all privacy of the vehicles. The pseudo-ID contains no information about the real-world identity of the vehicle. The mapping of pseudo-ID to real-world identity is stored in a table accessible only to the TA, which is fully trusted. An RTM may easily obtain a vehicle's pseudo-ID from its signature via the tracing key, but it cannot associate that pseudo-ID with the vehicle's real-world identity. In addition, as discussed above in Non-Repudiation, vehicles cannot trace the pseudo-IDs of other vehicles without solving the Decision Linear Problem.

Although knowledge of a vehicle's real-world identity as well as its pseudo-ID is protected in the proposed scheme, the scheme does allow some tracking of a vehicle in exchange for an increase in efficiency compared to similar schemes. Because the T_3 value for a vehicle is fixed, other members of the group can use the T_3 value to track a vehicle within the group until the group key updates. However, the T_3 values are not linked following group key updates, so the tracking will not continue beyond the specified group key update rate.

Another consideration is that vehicles may be tracked using some combination of known physical factors such as position, heading, speed, etc. [34]. In fact, the contents of the standard messages of intelligent transportation systems, for example the Cooperative Awareness Message (CAM) [35] from the European Telecommunications Standards Institute (ETSI) and the Basic Safety Message (BSM) [36] of the SAE J2735

TABLE 3. Execution times for cryptographic operations.

Operation	Execution Time (ms)
Map String to Point in G_1	0.1755
Scalar Multiplication in G_1	0.2665
Pairing	2.7837
Exponentiation in G_T	1.2259

standard, are designed to aid trajectory prediction. While the intention is to allow vehicles to predict the future positions of other vehicles in order to avoid collisions, this means that by design it should be easy to track the position of a target vehicle in a VANET without any identifying information. Therefore, the ability to track vehicles due to the use of fixed values for T_3 is of minimal impact.

4) EFFICIENCY

By using a mixture of pre-computed and cached pairing results, the proposed scheme gains an efficiency advantage during signature verification over other schemes. Moreover, this efficiency is not gained at the price of conditional privacy preservation. In the proposed scheme it is still possible for the group manager to quickly trace the identities of any nodes exhibiting malicious behavior. At the same time, vehicles in the group cannot determine the pseudo-IDs of any other vehicles in the group from their signatures.

The performance of the proposed scheme was compared to existing schemes [18] and [21] as these schemes are the only schemes reviewed that also provide tracing and authentication of vehicle's real identities. The estimated times required for message signing and verification for the three schemes are presented in Fig. 3. Timings for the non-negligible constituent operations are presented in Table 3. The operation times were measured using the C MIRACL Core Cryptographic Library [37] on an Intel Core i7-8700 CPU @ 3.2 GHz with 32 GB of RAM running the Windows 10 operating system, averaged over many iterations in order to account for interrupts due to background system operations.

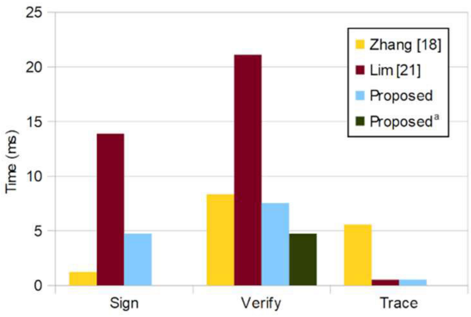


FIGURE 3. Comparison of execution times.

A Barreto-Naehrig curve, BN462, was used for all three schemes. This curve provides 128-bit security [38]. Both the Zhang *et al.* scheme and Lim *et al.* scheme state isomorphism between groups as a requirement, so as written they are not compatible with BN462, which is a Type 3 curve [38]. However, the isomorphism requirement was originally included by Boneh *et al.* in order to satisfy their definition of the Strong Diffie-Hellmann (SDH) assumption given in [20]. In a later paper, Boneh and Boyen introduced an updated definition of SDH that does not require isomorphism [39], [40]. This revised definition allows the use of the faster Type 3 curves with short group signature schemes, and therefore the BN462 curve may be safely used in this analysis.

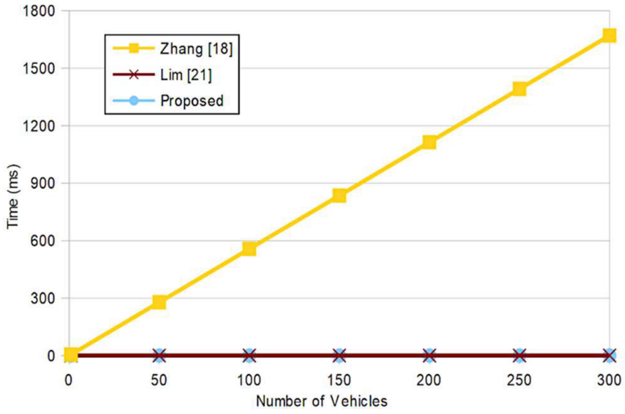


FIGURE 4. Tracing times for various group sizes.

As can be seen from Fig. 3, the proposed scheme has a performance advantage over the Lim scheme for all actions and the Zhang scheme for unbatched signature verification and tracing. In cases where message batching is possible, the Zhang scheme will outperform the proposed scheme for signature verification as the time remains essentially constant regardless of the number of messages verified. However, there may be many times in VANETs where message caching is undesirable, for example in the cases of time-critical safety or emergency messages.

The main disadvantage of the Zhang scheme compared to the other two schemes lies in its message tracing algorithm. The Zhang scheme traces message senders by looping through a table of stored tracing and identity parameters with one entry for each member of the group. Fig. 4 shows the effect of this iteration on tracing time in relation to group size, assuming that on average the tracing will find the correct vehicle after searching half of the table. The tracing times of the other two schemes remain constant as the identities are computed directly and not dependent on the size of the group.

The ability to revoke privacy and trace a message signer is an important part of identifying and removing malicious vehicles in VANETs. For example, in order to detect Sybil attacks, it must be possible for some monitoring authority to quickly link messages sent by the same vehicle using different pseudo-IDs. As traffic density grows, the Zhang scheme's tracing algorithm quickly becomes inadequate for detecting these kinds of attacks.

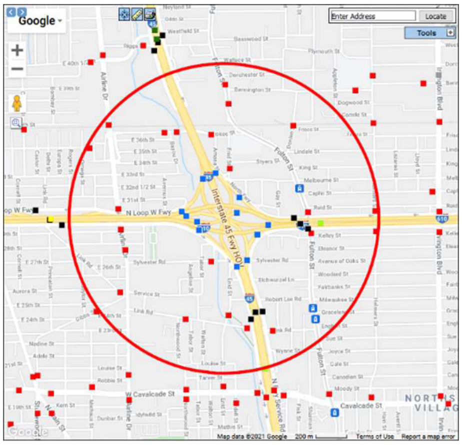


FIGURE 5. Houston (I-45/610).

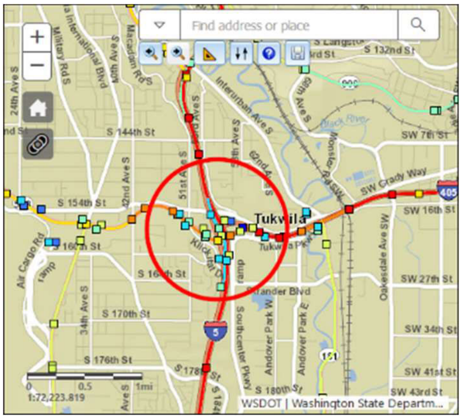


FIGURE 6. Seattle (I-5/405).

Finally, our scheme proposes to restrict group key updates to timed intervals in the case of normal operation. This would greatly reduce group key updates compared to other schemes, and therefore also provide increased efficiency by reducing the messaging and calculations associated with updating the group keys. A detailed analysis of group key update frequency is presented below.

B. ANALYSIS OF FORWARD & BACKWARD SECRECY

Some schemes propose to preserve forward and backward secrecy perfectly by updating the group secret for every vehicle that leaves and, in many current schemes, also for joining members [2], [11]–[13], [15], [16], [18], [24], [26]. In order to investigate the required update frequency for such a strategy under some common traffic conditions, publicly available traffic count data for three US cities: Houston [41], Seattle [42], and New York [43] were analyzed.

In each city, a busy interchange was chosen for the investigation. Sample locations are shown in Figs. 5, 6, and 7. A 1km radius was used to mark the group boundaries as that is typically defined to be the area covered by a single RSU as it is the maximum transmission distance in the WAVE standard [6].

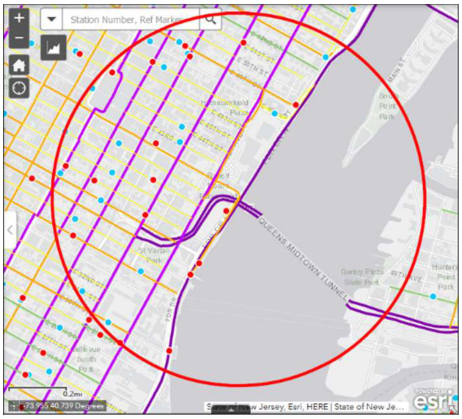


FIGURE 7. New York (Queens-Midtown Tunnel).

Traffic counts were obtained for morning and evening rush hour periods. Rush hour is often not the busiest time of day for each of the interchanges analyzed, but it represents a typical period of heavy traffic in US cities. Traffic counts were taken from 2019 in order to avoid undercounts in 2020 due to a dramatic, and atypical, reduction in traffic during the COVID-19 pandemic [44].

A few assumptions were made due to the limited availability of data samples, which were generally only measured on major roads. First, only traffic on major roads was considered. Traffic entering or leaving the group on side streets was considered negligible. Second, traffic on major roads was assumed to continue on the major roads without exiting. This assumption was necessary due to the distance of some count sensors from the 1km radius. A comparison of Annual Average Daily Traffic (AADT) counts, which were often closer to the group boundary modeled but do not report the required fine-grained hourly data, supported this assumption. Finally, in several cases hourly traffic counts were not available for one of the routes included. In those cases, an hourly estimate was made using the 2019 AADT for that route. It's important to note that the first and third assumptions almost certainly lead to an undercount, which means the required group rekeying time would likely be somewhat greater than these calculations show.

Tables 4, 5, and 6 show the traffic counts leaving the 1 km radius circle for each metropolitan area, and Table 7 shows the resulting calculations of the required frequency of group secret updates in order to perfectly maintain forward or backward secrecy. In the case of Houston, between 7am and 8am 24040 vehicles cross the RSU boundary at the studied intersection to leave the group. This is the highest volume of traffic that occurs at that intersection during the three hours we investigated. With 24040 vehicles leaving the area over the course of an hour, just over 6 vehicles will leave the area per second. The group key schemes referenced in this paper define their groups based on geographical location. This means that around 6 cars will leave the group per second. If the group keys are updated every time a car leaves the

TABLE 4. Houston traffic counts.

Monitoring Station Identifier	Location	7 to 8 AM	5 to 6 PM	6 to 7 PM
HP844A	North of I45/610	6252	7124	7700
HP856	South of I45/610	7210	5344	5082
102H77B	East of I45/610	3791 [a]	3791 [a]	3791 [a]
S157	West of I45/610	6787	6228	6070

[a] Estimated from AADT

TABLE 5. Seattle traffic counts.

Monitoring Station Identifier	Location	7 to 8 AM	5 to 6 PM	6 to 7 PM
S202	Due North of I5/405	8209	9429	8771
S839	North West of I5/405	1402	2076	1294
S205	South of I5/405	8435	6900	5605
S827	East of I5/405	4659	4695	4619
518 Milepost 2.91 A to 3.33 A	West of I5/405	2770 [a]	2770 [a]	2770 [a]

[a] Estimated from AADT

TABLE 6. New York City traffic counts.

Monitoring Station Identifier	Location	7 to 8 AM	5 to 6 PM	6 to 7 PM
050054	Long Island Expressway	1654	3010	2556
040903	FDR (Northbound)	4374	3118	3289
	FDR (Southbound)	4790	4100	4718
041268	1st Avenue	1248	1180	1311
041272	2nd Avenue	1542	1619	1638
041110	3rd Avenue	1686	1476	1713
041157	Lexington Avenue	1126	1192	1280
041281	Park Ave (Northbound)	768	1036	1004
	Park Ave (Southbound)	766	812	898

TABLE 7. Total traffic counts and rate of group exit at peak traffic.

City	7 to 8 AM	5 to 6 PM	6 to 7 PM	Peak Time	Leaving Rate
Houston	24040	22487	22643	7 to 8 AM	150 ms/car
Seattle	25475	25870	23059	5 to 6 PM	139 ms/car
New York City	17954	17543	18407	6 to 7 PM	196 ms/car

group, the group keys will change at a rate of 150ms. The worst case rate of our sampled locations requires the group key to update every 139ms.

The BSM of the SAE J2735 standard should be sent about every 100ms [36]. Using actual traffic counts, in all of the sampled cases, at most two BSMs could be sent before a car departed the group. In fact, it can clearly be seen that two messages would be a best case scenario. At almost all of the sample times and locations, keys could only be guaranteed to be used to send at most one BSM. Additionally, these random samples do not even represent worst-case scenarios. At all locations there were times of day and days of the year that exceeded the traffic counts used in our analysis. Furthermore, there is no reason to think these samples capture the busiest traffic locations in the US, or the world.

Given the calculated rate of group change, updating group keys for every vehicle that leaves or joins a group is a waste of the work done to calculate and distribute the keys in the first place, and may even be impossible with real-world transmission times and processor loads. Similarly, attempting to preserve forward and backward secrecy by alternative methods, such as maintaining some form of revocation list, would require those structures to grow and change at an impractical rate. When real-world traffic conditions are considered, it makes sense that some forward and backward secrecy is sacrificed in the absence of known malicious VANET members in order to allow the use of group keys for more than a single message before regenerating and redistributing a new shared secret. The appropriate timing of the updates will likely vary given the traffic and network characteristics of any given area.

While relaxing forward and backward secrecy introduces some security risks, these risks should be minimal. In the case of vehicles that join a group, access to previously sent messages is of little use in VANET due to the ephemeral and open nature of the data. In the case of vehicles that leave a group, vehicles that leave the group by crossing a geographic boundary have already had access to the group keys and could have attempted insider attacks at any time. When a vehicle leaves a group without having committed any attacks against the group, it is reasonable to continue trusting that vehicle for some short time more until the next scheduled group key update. On the other hand, if a malicious vehicle is detected, the group secret should be updated immediately in order to preserve secrecy in the presence of a known bad actor.

At this point, it is reasonable to question why the group key should ever be updated barring malicious activity. There are several arguments in favor of periodic group key updates. First, pseudo-IDs will remain the same until the group key updates. This makes it easier to track vehicles by their pseudo-IDs, although as discussed above there are other, physical means of tracking vehicles. A second argument is that the longer the group keys remain the same, the more time an attacker has to amass a set of valid keys in order to perform a Sybil attack, for example. Finally, changing the group key "resets" the group, which clears old data from tables and memory caches in order to prevent them from growing too large and slowing down the system as vehicles that have departed the geographic area need no longer be monitored or processed by the RTM.

V. CONCLUSION

In this paper, we presented an improved VANET security scheme using short group signatures which increases signing and signature validation efficiency by reducing pairing operations through the use of cached calculation results. In addition, the scheme also improves overall system efficiency by using timed group key updates instead of changing the keys in response to members departing the group. This extends the life of the group keys, which reduces the computation and communication burdens present in other schemes due to the wasteful key updates that would result under real-world traffic conditions.

In the future, we plan to explore methods to completely eliminate pairings and other costly operations from both message signing and signature validation operations without sacrificing the benefits of short group signatures which include conditional privacy, non-repudiation, and broadcast messaging ability. Furthermore, traffic and network simulations could be created using real-world traffic count data to better model the actual performance issues involved with VANET and group keys.

REFERENCES

[1] R. Vishwakarma, R. Barskar, and M. Ahirwar, "Secure key management in vehicular ad-hoc network: A review," in *Proc. SCOPES*, Odisha, India, 2016, pp. 1688–1694.

[2] 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.

[3] 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, Aug. 2019, doi: 10.3390/s19163589.

[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[5] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017, doi: 10.1016/j.adhoc.2017.03.006.

[6] 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.

[7] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. HotNets*, College Park, MD, USA, 2005, pp. 1–6.

[8] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247, doi: 10.1016/j.vehcom.2020.100247.

[9] L. E. Funderburg and I.-Y. Lee, "A privacy-preserving key management scheme with support for sybil attack detection in VANETs," *Sensors*, vol. 21, no. 4, p. 1063, Feb. 2021, doi: 10.3390/s21041063.

[10] H. Alzaid, D. Park, J. G. Nieto, C. Boyd, and E. Foo, "A forward and backward secure key management in wireless sensor networks for PCS/SCADA," in *Proc. S-CUBE*, Pisa, Italy, vol. 24, 2009, pp. 66–82, doi: 10.1007/978-3-642-11528-8_6.

[11] K. K. Chauhan, S. Kumar, and S. Kumar, "The design of a secure key management system in vehicular ad hoc networks," in *Proc. Conf. Inf. Commun. Technol. (CICT)*, Gwalior, India, Nov. 2017, doi: 10.1109/INFOCOMTECH.2017.8340636.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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

[17] M. Alimohammadi and A. A. Pouyan, "Sybil attack detection using a low cost short group signature in VANET," in *Proc. ISCISC*, Rasht, Iran, 2015, pp. 23–28.

[18] 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, Dec. 2019, doi: 10.1109/ACCESS.2019.2958356.

[19] 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.

[20] 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.

[21] 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.

[22] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011, doi: 10.1109/JSAC.2011.110311.

[23] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, Dec. 2018, doi: 10.1109/ACCESS.2017.2782672.

[24] 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. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar. 2021, doi: 10.1109/TDSC.2019.2904274.

[25] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5G-enabled vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 24, 2020, doi: 10.1109/TITS.2020.3023797.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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, pp. 1–13, Dec. 2019, doi: 10.1155/2019/7871067.

[31] 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, doi: 10.1109/MOBIQ.2007.4451013.

[32] 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.

[33] 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.

[34] J. Petit, S. Dietzel, and F. Kargl, "Privacy of connected vehicles," in *Handbook Mobile Data Privacy*, 1st ed. A. Gkoulalas-Divanis C. Bettini, eds. Berlin, Germany: Springer, 2018, pp. 229–251.

[35] *Intelligent Transport Systems (ITS) Vehicular Communications Basic Set of Applications Part 2: Specification of Cooperative Awareness Basic Service*, document ETSI Technical Specification 102 637-2, V1.2.1, 2011.

[36] B. Cronin, "Vehicle based data and availability," in *Proc. ITSPAC*. Washington, DC, USA: United States 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

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

[38] 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, 2019, pp. 191–196, doi: 10.1109/CANDAR.2019.00032.

[39] 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.

[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] *Texas Statewide Traffic Analysis and Reporting System (STARS II)*. Accessed: Apr. 28, 2021. [Online]. Available: https://www.txdot.gov/inside-txdot/division/transportation-planning/stars.html

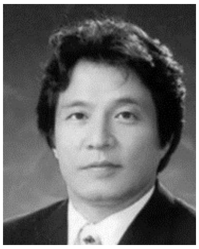
[42] *Washington State Traffic Data GeoPortal*. Accessed: Apr. 28, 2021. [Online]. Available: https://www.wsdot.wa.gov/mapsdata/tools/trafficplanningtrends.htm

[43] *New York State Traffic Data Viewer*. Accessed: Apr. 19, 2021. [Online]. Available: https://www.dot.ny.gov/tdv

[44] J. Du, H. A. Rakha, F. Filali, and H. Eldardiry, "COVID-19 pandemic impacts on traffic system delay, fuel consumption and emissions," *Int. J. Transp. Sci. Technol.*, vol. 10, no. 2, pp. 184–196, Jun. 2021, doi: 10.1016/j.ijtst.2020.11.003.

L. ELLEN FUNDERBURG received the B.S. degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1999, and the M.S. degree in electrical and computer engineering from The University of Texas at Austin, 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.



IM-YEONG LEE was born in Busan, Republic of Korea, in 1958. He received the B.S. degree from Hongik University, Seoul, South Korea, in 1981, and the M.S. and Ph.D. degrees from Osaka University, Osaka, Japan, in 1986 and 1989, respectively. His research interests include information security, cryptographic protocols, information theory, and data communications.