

LSKA-ID: A lightweight security and key agreement protocol based on an identity for vehicular communication

Murtadha A. Alazzawi¹, Mohammed Tali Almalchy², Ahmed Al-Shammari³,
Ahmed Salih Al-Khaleefa⁴, Hayder M. Albehadili¹

¹Department of Computer Techniques Engineering, Imam Al-Kadhumi College (IKC), 10001, Baghdad, Iraq

²Department of Mechanical Engineering, Faculty of Engineering, University of Misan, 62001, Iraq

³Department of Computer Science, College of Computer Science and Information Technology, University of Al-Qadisiyah, Al Diwanayah, 58002, Iraq

⁴Department of Physics, Faculty of Education, University of Misan, 62001, Iraq

Article Info

Article history:

Received Aug 14, 2022

Revised Dec 14, 2022

Accepted Feb 16, 2023

Keywords:

Authentication

Chinese remainder theorem

Privacy preserving

Security

VANETs

ABSTRACT

Recently, a huge effort has been pushed to the wireless broadcasting nature in the open area. However, the vehicular ad hoc network (VANET) is disposed to various kinds of attacks. Hence, keeping the security in VANET is the most critical issue because of the VANET network related to human life. Thus, we propose a robust and lightweight security and key agreement-based identity protocol LSKA-ID for vehicular communication. Our protocol utilizes the elliptic curve cryptography, Chinese remainder theorem, and identity (ID)-based cryptosystem to resolve the issues found in the previously proposed schemes, in which our protocol can resolve the key escrow issues accompanied in most ID-based schemes. Also, it does not need batch verification operations, which cause some problems to the verifier in case the batch beacons have one or more illegal beacons. Moreover, the LSKA-ID protocol addresses the dependency on the trusted authority (TA) during the high frequent handover between the groups that may cause a bottleneck problem on the TA. The security analysis proves the correctness of the LSKA-ID protocol by using the random oracle model and has shown to be effective in a performance evaluation.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Murtadha A. Alazzawi

Department of Computer Techniques Engineering, Imam Al-Kadhumi College (IKC)

10001, Baghdad, Iraq

Email: murtadhaali@alkadhumi-col.edu.iq

1. INTRODUCTION

To enhance the transportation, the car companies have started equipping vehicles by sensors to collect surrounding information including traffic- and safety-related information to be shared with other vehicles. Thus, a new technology named vehicular ad hoc network (VANET) have appeared recently. The VANET network is defined as a part of the mobile ad hoc network (MANET) and each vehicle in VANET represents a mobile node [1]. VANET provides not only traffic- and safety-related information but also other services such as live news, entertainment, and social interaction [2]. According to the high mobility property of the vehicles, a special protocol created for this network named dedicated short-range communication (DSRC) [3]. The last consents each vehicle equipped with onboard unit (OBU) to communicate with other vehicles by a technique called vehicle to vehicle (V2V) communication and with road-side units (RSUs) by vehicle to infrastructure (V2I) or infrastructure to vehicle (I2V) communication [4]. The RSUs, OBUs, and the trusted authority (TA) are the main components of VANET network [5], [6]. The TA sustains the entire system and utilizes a secure wired

channel to exchange the information with the RSUs distributed alongside roads and also is responsible managing s road traffic. The OBU is a device equipped with every vehicle and organized to work with DSRC.

As mentioned earlier, three types of communications, depended on DSRC in VANET, are called V2V, V2I, and I2V, means, vehicles can communicate with two VANET's different components simultaneously to receive the required traffic and safety information. Consistent with DSRC protocol, a vehicle equipped with OBU broadcasts one traffic- and safety-related message per 100–300 ms to cover a few hundred meters [3]. Along with the broadcast using the wireless channels, communication among the components in VANETs is susceptible to numerous attacks such as eavesdropping, impersonation, replaying, modification, forgery, and man in the middle attacks. Hence, to improve VANET network and motivate community using it, the security and privacy challenges should be enhanced [7], [8]. The authentication mechanism is considered the basic in VANET system to guarantee security, which involves identifying authentication and message integrity [8]-[10]. An attacker can broadcast messages by impersonating an authorized vehicle and gaining illegitimate benefits if the identity authentication does not ensure. Moreover, if message integrity is not fulfilled, attacker also may alter messages or broadcast forged information to completely disrupt traffic without being stopped. Hence, authentication has to be carried out to validate an identity of the vehicle and to ensure the received messages integrity. Besides, the privacy also essential for VANET [11], [12], where the infiltration of the vehicle's real identity can reveal driver's information such as current location, movement, and driver's identity. Consequently, the vehicle's anonymity must satisfy in VANET to preserve the vehicle's identity unless it achieves malicious activities. Once the authentication and privacy in VANET are satisfied, the other requirements such as non-repudiation, un-linkability, traceability, and revocation as well as resistance to attacks should be kept. Additionally, the efficient costs for computation and communication should be taken into consideration.

To address the prior security requirements, massive academic studies with several approaches have been presented. Depending on the public key infrastructure (PKI), the pseudonyms-based scheme [10] was first working to provide the security requirements in VANET, where each vehicle is preloaded with thousands of certificates with corresponding public/private key pairs. Then, a group signature (GS)-based schemes are proposed [13]-[15]. To override the drawbacks in the pseudonyms-based and GS-based works, many researchers adopted the identity (ID)-based encryption [16]-[24] to carry out their efforts. At the beginning, the bilinear pairing operation was used to product the ID-based schemes, but it miscarried later due to high costs in computation and communication. However, the high costs were mitigated by using the elliptic curve cryptography (ECC). Recently, [25]-[28] used the ID-based concept with making the VANET network as groups, and each RSU considered the group's manager that responsible for the joining the members and verifying the beacons. These schemes use either the bloom filter or the cuckoo filter to notify the vehicles which beacons are legal. Additionally, nowadays, some academic studies have been proposed rely on the certificateless cryptography [5], [29], [30].

Motivated by the VANET-related drawbacks mentioned earlier, in this work, we have proposed a lightweight ID-based protocol for VANET. Our protocol is different from other ID-based schemes, in which it can resolve security-related issues and mitigates the computation and communication costs. The contributions of our work are presented as:

- The proposed LSKA-ID protocol resolves the key escrow issues accompanied in most ID-based schemes.
- LSKA-ID protocol uses the ECC without the need to batch verification operations, which cause some problems to the verifier in case the batch beacons have one or more illegal beacons.
- The proposed protocol diminishes the ECC operations during the beacons generation and verification by using the group key that generated via Chinese reminder theorem (CRT). Therefore, the cost of the computation and communication will be low and suitable to VANET network.
- Also, LSKA-ID protocol addresses the dependency on the TA during the high frequent handover between the groups that may cause a bottleneck problem on the TA.

2. RELATED WORKS

Pseudonyms-based, GS-based, and ID-based schemes are observed as three main approaches to provide anonymous authentication in VANETs. Besides, a few academic studies recently have been proposed depending on the certificateless cryptography. The pseudonyms-based schemes principally utilize PKI concept. Raya *et al.* [10] proposed an authentication scheme based on pseudonyms for VANET. This scheme meets the most requirements for VANET but require preload the OBU with a lot of certificates and their corresponding keys pair. This point leads to many drawbacks such as large memory storage on the vehicle to save these certificates and the certification revocation list (CRL) will grow exponentially to keep all revoked vehicle's certificates as well as an inefficient cost in terms of the computation and communication.

In GS-based schemes, the VANET can provide anonymity for the vehicle as well as treated the exponential growth problem for CRL in pseudonyms-based schemes to increase the CRL's size linearly.

In 2007, Lin *et al.* [13] utilizes the GS-based concept to present a new privacy-preserving authentication approach for VANET. The group master key is only known by the group manager that can trace the vehicle's real identity. Many schemes such as [14], [15] are better than [13] have been proposed based on GS later. However, they are still unsuitable to VANET network due to the high cost in computation and communication, group management matters, and choose the group manager is complicated because it can track any vehicle according to its knowledge about every member.

Using ID-based encryption, the VANET system can resolve the previously mentioned problems in pseudonyms-based and GS-based schemes. Sun *et al.* [16] proposed a security VANET scheme using ID-based encryption which can provide the privacy-preserving authentication and traceability requirements. In 2012, Shim [17] suggested a scheme named CPAS depending on pseudo ID-based encryption for VANET. In this scheme, the execution time of signature verification is decreased because of using the batch verification. Consequently, numerous schemes, used ID-based encryption, were proposed [18]-[20]. However, these schemes are inadequate such as inefficient cost in terms of the computation and communication. As also, they susceptible to the impersonation and modification attacks. In [21]-[24] mitigated the computation and communication overhead using the ECC. He *et al.* [21] constructed an ID-based authentication scheme for VANET, provided privacy-preserving authentication, but the author depended strongly on the tamper proof device (TPD). In 2016, Lo and Tsai [23] proposed an efficient ID-based authentication scheme does not rely on TPDs. Though, it requests a massive storage memory space to save its pseudo-IDs with the private keys. In addition to the high cost in terms of the computation and communication, the ID-based systems suffer from other issues such as the key escrow problems due to each OBU in VANET should know the system private key. In case one vehicle is compromised, key leakage will happen and the whole VANET system will be compromised. Also, it is easy to any trusted vehicle to broadcast by impersonating other or it can reveal the vehicle's real identity due to it has the system private key. Moreover, the batch verification considered a big issue, where one beacon invalid causes rejection for all the beacons or requires additional computation to determine which one is invalid.

Cui *et al.* [25], Zhong *et al.* [26], Cui *et al.* [27], and Alazzawi *et al.* [28] produced ID-based authentication schemes rely on the RSU in signatures verification, where the RSU verifies the receiving messages and broadcasts the valid and invalid with (bloom or cuckoo) filters. These schemes can resolve the key escrow problems and satisfy the security and privacy requirements for VANET, but still suffer from other issues. According to the handover in these types of approaches that is a frequent event, the bottleneck may be happening on the TA. Also, Cui *et al.* [25], [27] use the batch verification to mitigate the computation. Cui *et al.* [31] used the CRT to share key among RSU's group members that use the advanced encryption standard (AES) encryption to encrypt the messages by this key. This scheme also suffers from the bottleneck on the TA and does not meet the non-repudiation requirement. Zhang *et al.* [32] divided the VANET to domains and each domain is a group from many RSUs. The vehicles in the group can get the shared key via CRT.

To resolve the escrow problems, in 2018, Seyed *et al.* [33] proposed a novel and an efficient authentication scheme NECPPA. The concept behind the scheme is to save the system key into TPD on each RSU and the temporary key into TPD on OBU. That means, the vehicle has not the system key and only can get the temporary key from the RSU during the joining process to the RSU's group. NECPPA suffers from the high cost in terms of the computation and communication according to the cryptography operations that depending on the bilinear pairing operation. Depending on the certificate less cryptography [34], the [5], [29], [30] proposed a new authentication schemes for VANET networks. These schemes could avoid the key escrow problems that found in ID-based schemes, but they did not able to resolve the high costs in computation and communication as well as they used the batch operation in their works. Our protocol adopted the ECC with CRT to resolve the aforementioned issues by generating a new and lightweight ID-based protocol. The ECC is used to achieve the security and privacy requirements based on ID encryption, whereas the CRT is used to update the group key.

3. PRELIMINARIES

In this section we present the system model which discusses the three components used in our protocol, followed by a threat model which shows the main types of adversaries who can use security attacks. Moreover, we are going to explain the main security and privacy requirements for design goals. Lastly, the elliptic curve cryptography and the Chinese remainder theorem used in this work are explained.

3.1. The system model

Three components are used in our protocol as shown in Figure 1. The first one is the TA that is accountable to prepare the basic and secure parameters in VANET as well as allows other components to register with the network. The RSU is a second component in the protocol, which is allocated as a router along the roadside and considers the manager of group in our protocol. Whereas the last one is the vehicle equipped with the OBU.

The RSU utilizes the DSRC technology to communicate with the vehicle's OBU, and a wired channel with the TA. We assume that:

- The TA is completely trusted, always online, and will not be compromised.
- Comparing to OBU, achieving high computation operation by RSU influence power consumption because of its responsibility for vehicle authentication, generation shared group key. Also, RSU is capable of supporting TA to trace and revoke the identity of the malicious vehicles.

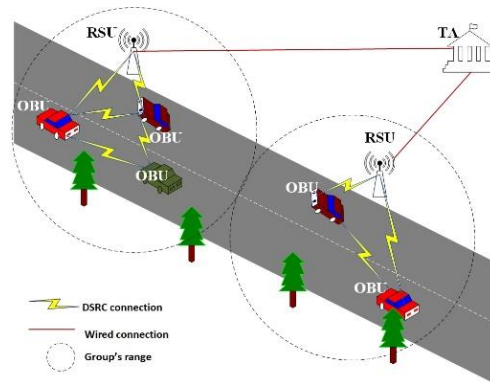


Figure 1. Illustration of system model components

3.2. Threat model

In our proposed LSKA-ID protocol, we make the assumption that the TA has the maximum level of security, making it extremely difficult for adversaries to attack it. The VANET network is prone to diverse security attacks according to the broadcasting nature in the open access. In like this networks, the following two main types of adversaries who can use security attacks [24].

- The external adversary: VANET network can be damaged by broadcasting various security attacks, such as (impersonation, modification, tampering, replay, man in the middle (MITM), and tracking) attacks. Attackers can violently surge essential information of VANET network and destroy critical network data.
- The internal adversary: this type is usually some malicious authenticated vehicles that probable to increase their interest by the security weaknesses of the VANET network. For example, a vehicle may issue false message about traffic jam to make the other vehicles to take other routes so that the malicious vehicle will obtain better road resources. What is more, other malicious vehicles able to tamper the location info to fleeing from traffic accountability.

3.3. Design goals

Zhong *et al.* [22] indicated that VANETs should fulfill numerous security and privacy requirements, excluding message authentication, identity privacy preservation, traceability, un-linkability, non-repudiation and resistance to various attacks. In addition to these requirements mentioned, we believe that the following properties should also be provided by a designed system.

- Key escrow challenge: a vehicle supposed to be not know the system private key to avoid some attack types especially insider attacks.
- Revocation: the TA is capable to revoke any vehicle in case this vehicle cause did some malicious activities.
- Not strong dependence on TA: the strong dependency on the TA in this network may lead to other issues on TA such as bottleneck problems.
- Computation time: according to the DSRC protocol broadcasts more than three beacons per second, the OBU should be correspond with this case in terms of the generation time and verification time of the beacons.

Thus, our scheme aims to achieve all the security and privacy requirements that mentioned above.

3.4. Elliptic curve cryptography

ECC was suggested in 1985 by Miller [35] and became widespread in design protocols of security. Let F_p and EC represent a finite field and an elliptic curve over F_p respectively, where p is a large prime number. The EC is based on the equation $y^2 = x^3 + ax + b \text{ mod } p$, where $(4a^3 + 27b^2) \text{ mod } p \neq 0$ and $x, y, a, b \in F_p$. We assume that O is an infinite point, and G is an additive group with order q and generator P .

The G contains all points on the EC . If the P and Q be two points on the EC , main representatives of the EC are listed as [36]:

- The point addition in G is defined as $P + Q = R$.
- The scalar point multiplication in G is defined as $sP = P + P + \dots + P$ (s times).
- The elliptic curve discrete logarithm problem (ECDLP). Based on EC , and given two points $P, Q \in G$, the task of ECDLP is finding an integer s that meets $Q = sP$.

3.5. Chinese reminder theorem CRT

CRT is a theorem that engenders a unique result to concurrent linear congruence with coprime moduli [37], [38]. The methodology of CRT is when the remainders of the Euclidean division of a number n by numerous numbers are known by someone, then he/she has been able to determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime. CRT's theorem states known the remaining numbers of the Euclidean division of an integer number n by several integer numbers, then it is possible to identify matchlessly the remainder of the division of n by the product of these integer numbers, where the condition that divisors are pairwise coprime is valid.

For more details, assume that $\{x_1; x_2 \dots \dots x_n\}$ are pairwise prime relatively positive integers, where, $n \geq 2$, set $X = x_1 x_2 \dots x_n = x_1 X_1 = x_2 X_2 = \dots = x_n X_n$, where, $X_i = X/x_i$, $i = 1, 2, 3 \dots n$. The positive integer number of the congruence (1) is $k \equiv \sum_{i=1}^n y_i X_i X'_i \equiv y_1 X_1 X'_1 + y_2 X_2 X'_2 + \dots + y_n X_n X'_n \pmod{X}$, where, X'_i is a positive integer number and meets the congruence equation $X_i X'_i \equiv 1 \pmod{x_i}$, $i = 1, 2, 3 \dots n$.

$$\begin{cases} k \equiv y_1 \pmod{x_1} \\ k \equiv y_2 \pmod{x_2} \\ \dots \dots \dots \\ k \equiv y_i \pmod{x_i} \end{cases} \quad (1)$$

4. THE PROPOSED LSKA-ID PROTOCOL

LSKA-ID protocol as mentioned in Figure 1 has three main components, TA, RSU, and vehicle. Mainly, seven phases are created to manage the LSKA-ID protocol, named initializing, registering, creating a shared key, joining, departing, signing and verifying, and revoking phases. The first two phases are responsible for initializing the system parameters and registering the vehicle respectively. During third phase, a group's shared key will be created. In forth phase, mutual authentication will create between the RSU and OBU without the need to the TA. After complete the mutual authentication correctly, the vehicle joins the group and can broadcast beacons. LSKA-ID protocol updates the group's shared key by using the sixth phase when the vehicle leaves the group. Last phase provides revocation process that allow to the TA to revoke any trusted vehicle when it starts to broadcast bogus beacons.

4.1. Initializing phase

The TA creates system parameters at this phase, including a finite field and an elliptic curve specified on it. Although this phase is standard, and the process seems identical. However, this phase is accomplished by the TA and the process of achieving it is followed the following steps and to adapt the system parameters are adjusted as:

- The TA prepares the ECC's parameters such as two large prime numbers p, q and an additive group G that contains all the elliptic curve EC 's points with order q and generator P . EC 's points defined by the equation $y^2 = x^3 + ax + b \pmod{p}$, where, $a, b \in F_p$.
- The TA generates random integer s and performs $P_k = sP$. Integer s is the private key and P_k is the public key.
- TA chooses a secure hash function h .
- TA sends the private key s to all RSUs.
- TA broadcasts the system parameters $\{p, q, P, P_k, h\}$ periodically.

4.2. Registering phase

This phase should be happened at first when someone wanted to join the VANET. The driver chooses password PW , and then sends the PW with the real identity of the vehicle RID to the TA via a secure channel. The TA computes vehicle's pseudonym $PID = h(RID)s$ and saves $\{RID, PID, PW\}$ into the vehicles' registration list. At the end, TA sends PID to the vehicle. The vehicle will save $\{RID, PID, PW\}$ into TPD inside the OBU.

4.3. Creating a shared key phase

This phase is responsible for creating the group's shared key depending on CRT. It achieved by the RSU in our proposed LSKA-ID protocol. The RSU completes the five steps during this phase:

- RSU rearranges the random integers m_i for all vehicles that have succeeded to join the group. Let us suppose there are n vehicles joined the group; the matching random integers are arranged as $m_1, m_2, m_3, \dots, m_n$.
- RSU generates a random integer Ks less than q .
- RSU computes $(\omega = \prod_{i=1}^n m_i)$, $(\alpha_i = \omega/m_i)$, $(\beta_i$ such that $\alpha_i \cdot \beta_i \equiv 1 \pmod{m_i})$, $(\lambda_i = \alpha_i \cdot \beta_i)$, $(\varphi = \sum_{i=1}^n \lambda_i)$, and $(\gamma = \varphi \cdot Ks)$.
- RSU broadcasts $\{T, \gamma, \sigma_{Ks}\}$, where $\sigma_{Ks} = h(T \parallel Ks)$.
- Any vehicle receives $\{T, \gamma, \sigma_{Ks}\}$, it will check the validity of the timestamp T . If it is not valid, the vehicle drops the message. Otherwise, it computes $Ks = \gamma \pmod{m_i}$ and checks if $\sigma_{Ks} =? h(T \parallel Ks)$. If not, drop the message. Otherwise, it keeps Ks inside the TPD and start broadcasting using Ks .

4.4. Joining phase

This phase happens between the OBU and RSU and responsible for allowing the vehicle to join the group and obtain the shared key. At first, the vehicle's driver should input the vehicle's real identity and the password when he/she turns on the vehicle to start the OBU. The following steps show the joining process.

- Firstly, OBU generates random integer $r \in Z^*$, and computes $U = rP$, $RID^* = h(RID) \oplus h(rP_k)$, and $PID^* = PID \oplus h(rP_k)$. Then, it sends message request to the RSU to join the group and obtain the shared key. The content of the message is $\{T_1, U, RID^*, PID^*, \sigma_{OBU}\}$, where $\sigma_{OBU} = h(T_1 \parallel U \parallel h(RID) \parallel PID)$.
- When the RSU receiving the message $\{T_1, U, RID^*, PID^*, \sigma_{OBU}\}$, it checks the validity of the timestamp. (Note: timestamps are checked by implement if $(\Delta T > (T_r - T_s))$, if it is true, then the time is valid, otherwise, the time is invalid, where, T_r is the receiving time, T_s is the sending time, and ΔT is the predefined delay time). If it is invalid, RSU drops the message. Otherwise, it computes:

$$h(RID) = RID^* \oplus h(U.s) \text{ and } PID = PID^* \oplus h(U.s), \text{ then it checks whether}$$

$$\sigma_{OBU} =? h(T_1 \parallel U \parallel h(RID) \parallel PID).$$

If not, RSU drops the message. Otherwise, it ensured the message integrity and will check RID in the revocation list RL to ensure the vehicle does not revoked. After that it implements (2) to test the vehicle' legitimacy.

$$PID.P = h(RID).P_k \tag{2}$$

Proof of correctness:

L. H. S. PID.P

Due to:

$$\begin{aligned} PID &= h(RID).s \\ &= h(RID).s.P \\ &= h(RID).P_k \end{aligned}$$

R. H. S.

Consequently, the (2) is correct.

If (2) does not hold, that means the vehicle illegal. Otherwise, RSU generates random integer $m_i \in Z^*$ and inserts the information $\{h(RID), PID, U, m_i\}$ to the group list GL . Lastly, it computes $Sig = h(U).s$ as a signature to the vehicle and sends $\{T_2, Ks^*, m_i^*, Sig^*, \sigma_{RSU}\}$ to OBU, where $Ks^* = Ks \oplus h(RID)$, $m_i^* = m_i \oplus h(RID)$, $Sig^* = Sig \oplus h(RID)$ and $\sigma_{RSU} = h(T_2 \parallel Ks \parallel m_i \parallel Sig)$.

- When the OBU receiving the message $\{T_2, Ks^*, m_i^*, Sig^*, \sigma_{RSU}\}$, it checks the validity of the timestamp T_2 , if it is invalid, it drops the message. Otherwise, it computes $Ks = Ks^* \oplus h(RID)$, $m_i = m_i^* \oplus h(RID)$, and $Sig = Sig^* \oplus h(RID)$. Lastly, it checks whether $\sigma_{RSU} =? h(T_2 \parallel Ks \parallel m_i \parallel Sig)$. If not, it drops the message. Otherwise, the joining process has been completed and the vehicle joined the group.

4.5. Departing phase

This phase happens when the vehicle leaves the group. Therefore, the RSU should update the shared key Ks to prevent the departing vehicle from access to the group. When the vehicle leaves the group, the RSU will implement the creating a shared key phase after remove the m_i of leaving vehicle from the list.

4.6. Signing and verifying phase

This phase happens when the vehicle wants to broadcast or it is receiving beacons as:

- Signing process: it is responsible for signing the beacon using Ks and Sig . Firstly, the OBU computes $\sigma_{Sig} = h(Sig.P \parallel T)$ and $\sigma_M = U \oplus h(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$, then broadcasts the beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$.

$$h(P.Sig \parallel T) = h(h(U).P_k \parallel T) \quad (3)$$

- Verifying process: it is responsible for verifying the receiving beacons. When the OBU receives beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$, it checks the validity of the timestamp T . If it is invalid, it drops the beacon. Otherwise, it computes $U = \sigma_M \oplus h(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$ and implements (4).

$$\sigma_{Sig} = h(h(U).P_k \parallel T) \quad (4)$$

Proof of correctness:

$$\begin{aligned} L.H.S. \sigma_{Sig} &= h(Sig.P \parallel T) \\ &= h(h(U).s.P \parallel T) \\ &= h(h(U).P_k \parallel T) \\ R.H.S. & \end{aligned}$$

Consequently, the (4) is correct. If (4) does not hold, the OBU drops the beacon. Otherwise, it accepts the beacon and the vehicle sender is trusted.

4.7. Revoking phase

This phase happens when any trusted vehicle broadcasts spurious beacons. To protect the VANET system from the insider attack, the TA should be able to trace and revoke such as this vehicle. Our scheme provides revocation procedure as:

- When the trusted vehicle starts broadcasts spurious beacons, the RSU can retrieve vehicle's information from GL according to U that compute by implement $U = \sigma_M \oplus h(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$, then it sends this information to the TA.
- When the TA receiving the vehicle's information, it revokes the vehicle by adding its real identity to the revocation list RL , then it sends response message to the RSU and forwards the RL to all RSUs.
- When the RSU receiving the response message from the TA, it implements the departing phase to prevent the vehicle from continuation as member in the group.

5. SECURITY PROOF AND ANALYSIS OF THE LSKA-ID

In this section, we analyze LSKA-ID protocol with respect to the security and privacy requirements. Assume the ECDLP is difficult, we demonstrate the LSKA-ID protocol can force non-forgery. Security proof, security analysis and comparison and attack scenarios analysis are clarified in section 5.1 to section 5.3.

5.1. Security proof

In this subsection we are going to analyze our proposed LSKA-ID protocol formally. Based on the adversary activity and the VANET's system model, the security model of LSKA-ID protocol is defined through a game between two parties. The first one is an adversary adv and the other is a challenger cha .

- Theorem 1: LSKA-ID protocol can force non-forgery of messages under an adaptively chosen message attack in the random oracle model (ROM).
- Proof: we suppose that Adv has ability to forge a genuine signature $\{T, M, \sigma_{Sig}, \sigma_M\}$ for the the traffic message M . Also, suppose that a ECDLP instance $(P, Q = sP)$ is given for 2 points P, Q on E/E_p , where $s \in Z_q^*$. Now, by running Adv as a subroutine, Cha has been able to resolve the ECDLP with non-negligible probability.
- Setup: Cha computes $P_k = Q = sP$ as a public key and establishes public parameters $Pars = \{q, P_k, P, h\}$. Cha then sends $Pars$ to Adv as well as constructs and maintains the following lists:
 - HL_1 -oracle: Cha constructs HL_1 in the form $\langle Sig, T, \sigma_{h_1} \rangle$ and sets it to empty. Once receiving a request from Adv with a message (Sig, T) , Cha directly looks whether the tuple $\langle Sig, T, \sigma_{h_1} \rangle$ is in HL_1 . If it is occurred, Cha sends $\sigma_{h_1} = h_1(Sig.P \parallel T)$ to Adv . If it is not occurred, Cha will randomly select $\sigma_{h_1} \in Z_q^*$ and insert $\langle Sig, T, \sigma_{h_1} \rangle$ into HL_1 . Then Cha sends $\sigma_{h_1} = h_1(Sig.P \parallel T)$ to Adv .

- b) HL_2 -oracle: Cha constructs HL_2 in the form $\langle T, M, \sigma_{Sig}, Ks, \sigma_{h_2} \rangle$ and sets it to empty. Once receiving a request from Adv with a message (T, M, σ_{Sig}, Ks) , Cha directly looks whether the tuple $\langle T, M, \sigma_{Sig}, Ks, \sigma_{h_2} \rangle$ is in HL_2 . If it is occurred, Cha sends $\sigma_{h_2} = h_2(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$ to Adv . If it is not occurred, Cha will randomly select $\sigma_{h_2} \in Z_q^*$ and insert $\langle T, M, \sigma_{Sig}, Ks, \sigma_{h_2} \rangle$ into HL_2 . Then Cha sends $\sigma_{h_2} = h_2(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$ to Adv .
- c) Sign-oracle: once receiving a sign request over message M , Cha generates two random numbers $\sigma_{Sig} = \sigma_{h_1}, \sigma_{h_2} \in Z_q^*$ and computes $\sigma_M = U \oplus \sigma_{h_2}$. Then it adds $\langle Sig, T, \sigma_{Sig} \rangle$ into HL_1 and $\langle T, M, \sigma_{Sig}, Ks, \sigma_{h_2} \rangle$ into HL_2 . At last, Cha builds a beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$ and sends it to Adv .
- d) Output: finally, Adv outputs a beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$. Cha will verify this beacon by utilizing (5).

$$\sigma_{Sig} = h(h(U).P_k \parallel T) \quad (5)$$

If (5) is valid, Cha finishes the game. Consistent with the forgery lemma in [18], Adv can yield another legal beacon $\{T, M, \sigma_{Sig}^*, \sigma_M^*\}$ that meets (6):

$$\sigma_{Sig}^* = h(h(U^*).P_k \parallel T) \quad (6)$$

Based on (5) and (6), we can infer:

$$\begin{aligned} (\sigma_{Sig} - \sigma_{Sig}^*) &= h(h(U).P_k \parallel T) - h(h(U^*).P_k \parallel T) \\ &= h(h(U).s.P \parallel T) - h(h(U^*).s.P \parallel T) \end{aligned} \quad (7)$$

However, the result in (7) contradicts the hardness of ECDLP. Thus, our proposed scheme under the ROM is resistant against a chosen adaptive message. Where the Sig is a signature of the vehicle that is calculated by RSU during the joining phase by using $Sig = h(U).s$.

5.2. Security analysis and comparison

A comprehensive study of identifying the robustness of proposed protocol LSKA-ID with recently three proposed Cui *et al.* [27], Ming and Cheng [30], and Pournaghi *et al.* [33] schemes in terms of the mentioned security properties in section 3.3. Let SP-1, SP-2, SP-3, SP-4, SP-5, SP-6, SP-7 and SP-8 denote message authentication, identity privacy preservation, traceability, revocation, un-linkability, non-repudiation, key escrow challenges, and not strong dependence on TA respectively. Table 1 shows the comparison results for security properties in VANETs. Next, we prove that LSKA-ID protocol can meet these properties as:

- Message authentication: according to Theorem 1, no polynomial adversary can forge a valid message if the ECDLP is hard. Thus, the verifier could check the validity and integrity of the beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$ by verifying whether the equation $\sigma_{Sig} = h(h(U).P_k \parallel T)$ holds. Thereby, the message authentication property is offered in LSKA-ID protocol.
- Identity privacy preservation: in LSKA-ID protocol, the vehicle broadcasts the beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$ that has not information about the real identity of the vehicle, where, $\sigma_{Sig} = h(Sig.P \parallel T)$ and $\sigma_M = U \oplus h(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$. Therefore, the attacker cannot obtain the RID even he/she has the shared key Ks . Thereby, the identity privacy preservation property is offered in LSKA-ID protocol.
- Traceability and revocation: according to revoking phase mentioned in section 4, the TA in LSKA-ID protocol can trace and revoke a trusted vehicle. Thereby, the traceability and revocation properties are offered in LSKA-ID protocol.
- Un-linkability: in LSKA-ID protocol, the vehicle broadcasts the beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$ that will be different for each broadcasting process, where, $\sigma_{Sig} = h(Sig.P \parallel T)$ and $\sigma_M = U \oplus h(T \parallel M \parallel \sigma_{Sig} \parallel Ks)$. Thereby, the un-linkability property is offered in LSKA-ID protocol.
- Non-repudiation: in LSKA-ID protocol, once any vehicle wants to broadcast beacons, adding to Ks it should its own signature Sig that got it during the joining phase. Therefore, it cannot deny their broadcasted beacons. Thereby, the non-repudiation property is offered in LSKA-ID protocol.
- The key escrow challenges: as mentioned early, the vehicle in LSKA-ID protocol cannot obtain the system private key and got only a pseudonym during the registering phase as well as a shared key during the joining phase, which is updated after leaving or joining vehicle. Thereby, the key escrow challenges are offered in LSKA-ID protocol.
- Not strong dependence on TA: in LSKA-ID protocol, the repeated operations like handover do not require to the TA intervention and only done between the RSU and OBU as mentioned in the joining phase. Thereby, the not strong dependence on TA property is offered in LSKA-ID protocol.

Table 1. Comparison results for security properties in VANETs

Properties	Cui <i>et al.</i> [27]	Ming and Cheng [30]	Pournaghi <i>et al.</i> [33]	LSKA-ID protocol
SP-1	Yes	Yes	Yes	Yes
SP-2	Yes	Yes	No	Yes
SP-3	Yes	Yes	Yes	Yes
SP-4	No	No	No	Yes
SP-5	Yes	Yes	Yes	Yes
SP-6	Yes	Yes	No	Yes
SP-7	Yes	Yes	No	Yes
SP-8	No	No	No	Yes

5.3. Attack scenarios analysis

This subsection presents that LSKA-ID protocol is safe and can avoid various attacks. In the following theorems we are going to give a different attacks scenarios. However, every scenario will prove that LSKA-ID protocol is resisted in all of them as:

- Theorem 2: LSKA-ID protocol can avoid the replay attack.
- Proof: replay attack is a type from network attacks working to repeat legal messages falsely. In LSKA-ID protocol, the timestamp T is inserted to a beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$. By verifying freshness of T , the beacon receiver can resist this type of attacks. Thereby, the replay attack is resisted in LSKA-ID protocol.
- Theorem 3: LSKA-ID protocol can avoid the impersonation attack.
- Proof: to issue an impersonation attack, a fake beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$ that meets (2) should be generated by attacker. According to Theorem 1, the probability of the bogus beacon for the attacker to meet (2) can be negligible.
- Theorem 4: LSKA-ID protocol can avoid the modification attack.
- Proof: in the proposed LSKA-ID protocol, a digital signature σ_{Sig} is included on the beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$. According to Theorem 1, (3) will not be held in case any modified on the beacon $\{T, M, \sigma_{Sig}, \sigma_M\}$. Thereby, the modification attack is resisted in LSKA-ID protocol.
- Theorem 5: LSKA-ID protocol can avoid the MITM attack.
- Proof: according to Theorem 1, it is difficult for an attacker to issue this type of attack. Thereby, the MITM attack is resisted in LSKA-ID protocol.

6. PERFORMANCE ANALYSIS OF THE LSKA-ID

In this section, we achieve a performance analysis of our proposed protocol in terms of both computation and communication overhead. Besides, we present comparative the proposed protocol with three most recent Cui *et al.* [27], Ming and Cheng [30], and Pournaghi *et al.* [33] approaches. The cryptography operations in [33] are built on bilinear pairings and what was proposed in [27], [30] and proposed protocol uses ECC. To provide an 80-bit security level, we use in bilinear pairings, the additive group \bar{G} generated based on EC \bar{E} : $y^2 = x^3 + x \text{ mod } \bar{p}$, where, \bar{p} is a 512-bit prime number, and in ECC, the additive group G generated based on EC E : $y^2 = x^3 + ax + b \text{ mod } p$, where p is a 160-bit prime number and $a, b \in Z_p^*$.

6.1. Computation cost

This section investigates the computation cost of LSKA-ID protocol against a few existing approaches. Message signing (MS), verification of single message (VSM), verification of multiple messages phases (VMM). To guarantee comparison accuracy, the execution time of cryptographic operations must be under the same environments. In the experiment of LSKA-ID, the same execution time is employed, which is computed by Alshareeda *et al.* [39] scheme using the MIRACL library, as shown in Table 2. Figure 2 demonstrates the comparison result of the computation cost among three related approaches for MS and VMS , and Figure 3 shows the computation costs of VMM for a number of beacons.

Table 2. The execution time results of cryptographic operations

Cryptography operation	Execution time (ms)	Description
T_{bp}	5.811	Bilinear pairing operation
T_{sm-bp}	1.5654	Scalar multiplication operation in a group based on bilinear pairing
$T_{sm-bp-s}$	0.1829	Small scalar point multiplication operation in a group based on bilinear pairing
T_{pa-bp}	0.0106	Point addition operation in a group based on bilinear pairing
T_{mtp}	4.1724	Map-to-point hash function
T_{sm-ecc}	0.6718	Scalar multiplication operation in a group based on ECC
$T_{sm-ecc-s}$	0.0665	Small scalar point multiplication operation in a group based on ECC
T_{pa-ecc}	0.0031	Point addition operation in a group based on ECC
T_h	0.001	General hash function operation

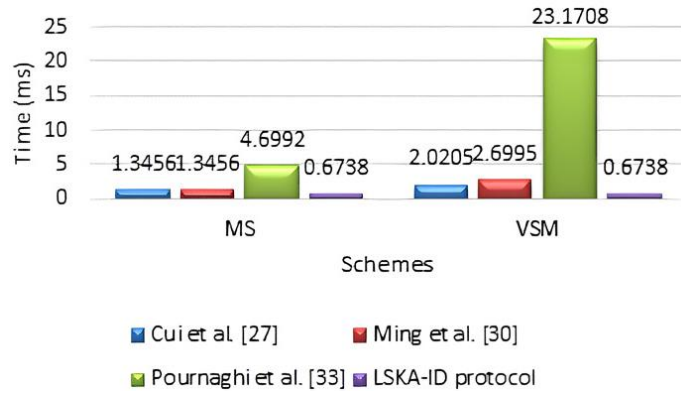


Figure 2. The computation costs of MS and VSM

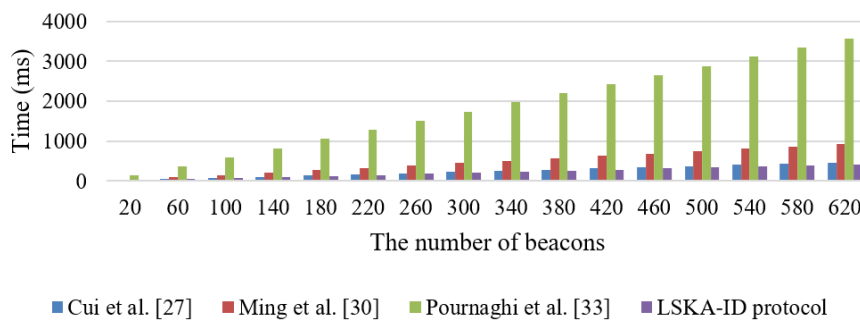


Figure 3. The computation costs of VMM

In the scheme of Cui *et al.* [27], the MS needs to $(2T_{sm-ecc} + 2T_h = 1.3456)$, the VSM needs to: $(3T_{sm-ecc} + T_{pa-ecc} + 2T_h = 2.0205)$

And VMM needs to:

$$((2 + n)T_{sm-ecc} + T_{pa-ecc} + nT_{sm-ecc-s} + 2nT_h = 1.3467 + 0.7403n).$$

In the scheme of Ming *et al.* [30], the MS needs to $(2T_{sm-ecc} + 2T_h = 1.3456)$, the VSM needs to:

$$(4T_{sm-ecc} + 3T_{pa-ecc} + 3T_h = 2.6995)$$

And VMM needs to:

$$((2 + 2n)T_{sm-ecc} + 4nT_{pa-ecc} + 2nT_{sm-ecc-s} + 3nT_h = 1.3436 + 1.492n).$$

In the scheme of Pournaghi *et al.* [33], the MS needs to $(3T_{sm-bp} + 3T_h = 4.6992)$, the VSM needs to:

$$(3T_{bp} + T_{sm-bp} + T_{mtp} = 23.1708)$$

And VMM needs to:

$$(3T_{bp} + nT_{sm-bp} + nT_{mtp} = 17.433 + 5.7378n).$$

In the proposed LSKA-ID protocol, the MS needs to: $(T_{sm-ecc} + 2T_h = 0.6738)$, the VSM needs to:

$$(T_{sm-ecc} + 2T_h = 0.6738)$$

And VMM needs to:

$$(nT_{sm-ecc} + 2nT_h = 0.6738n).$$

6.2. Communication cost

This section investigates the communication cost of LSKA-ID protocol against a few existing approaches. As mentioned previously, the size of p and \bar{p} elements in G and \bar{G} are 160 bit and 512 bit, respectively, meaning that the size of each element in G is 320 bit and the size of each element in \bar{G} is 1024 bit. Also, let us assume that the size of each hash function and each element in Z_q^* are 160 bit, and 32 bit in the timestamp. Table 3 shows the comparison of costs.

Table 3. A comparison results of the computation cost among three related approaches and LSKA-ID protocol

Protocols	The size of beacon (bit)
Cui <i>et al.</i> [27]	800
Ming and Cheng [30]	1560
Pournaghi <i>et al.</i> [33]	1344
LSKA-ID protocol	352

In Cui *et al.* [27], the vehicle broadcasts the following message $\{PID_i, M_i, \sigma_i\}$, where $PID_i = \{PID_i^1, PID_i^2\} \in G$ and $\{\sigma \in Z_q^*\}$, therefore the whole communication cost is $320 + 320 + 160 = 800$ bit. In the same method, the communication cost for each of Ming and Cheng [30], and Pournaghi *et al.* [33] approaches are computed. However, in the LSKA-ID protocol, the vehicle broadcasts the message $\{T, M, \sigma_{sig}, \sigma_M\}$, where $\{\sigma_M, \sigma_{sig} \in Z_q^*\}$ and T is a timestamp, therefore the whole communication cost is $160 + 160 + 32 = 352$ bit. Thus, the proposed LSKA-ID protocol is more efficient than these protocols of Cui *et al.* [27], Ming and Cheng [30], and Pournaghi *et al.* [33] approaches in terms of communication costs.

7. CONCLUSION

In this work, we propose lightweight security and key agreement-based identity protocol LSKA-ID for vehicular communication. The proposed LSKA-ID protocol can provide the security requirements, such as message authentication, identity privacy preservation, traceability, and revocation. additionally, it is secure against the most well-known attacks. Besides, under the ROM, the proposed LSKA-ID protocol proves non-forgery in an adaptively chosen message attack. Moreover, the performance evaluation illustrations that the computational cost of the proposed LSKA-ID protocol is lower when compared to state-of-the-art schemes. Consequently, our proposed LSKA-ID protocol can resolve these challenges positively and is appropriate for vehicular communication.




REFERENCES

- [1] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014, doi: 10.1016/j.comcom.2014.02.020.
- [2] G. Li, Q. Zhang, J. Li, J. Wu, and P. Zhang, "Energy-Efficient Location Privacy Preserving in Vehicular Networks Using Social Intimate Fogs," in *IEEE Access*, vol. 6, pp. 49801–49810, 2018, doi: 10.1109/ACCESS.2018.2859344.
- [3] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," in *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011, doi: 10.1109/JPROC.2011.2132790.
- [4] X. Yang *et al.* "A lightweight authentication scheme for vehicular ad hoc networks based on MSR," *Vehicular Communications*, vol. 15, pp. 16–27, 2019, doi: 10.1016/j.vehcom.2018.11.001.
- [5] Y. Ming and X. Shen, "PCPA: A Practical Certificateless Conditional Privacy Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *Sensors*, vol. 18, no. 5, 2018, doi: 10.3390/s18051573.
- [6] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad-Hoc Network," in *IEEE Access*, vol. 7, pp. 71424–71435, 2019, doi: 10.1109/ACCESS.2019.2919973.
- [7] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," in *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004, doi: 10.1109/MSP.2004.26.
- [8] X. Liu, Z. Fang, and L. Shi, "Securing Vehicular Ad Hoc Networks," *2007 2nd International Conference on Pervasive Computing and Applications*, Birmingham, UK, 2007, pp. 424–429, doi: 10.1109/ICPCA.2007.4365481.
- [9] F. Kargl *et al.*, "Secure vehicular communication systems: implementation, performance, and research challenges," in *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008, doi: 10.1109/MCOM.2008.4689253.
- [10] M. Raya and J. -P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007, doi: 10.3233/JCS-2007-15103.
- [11] F. Qu, Z. Wu, F. -Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015, doi: 10.1109/TITS.2015.2439292.
- [12] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, 2015, doi: 10.1109/COMST.2014.2345420.
- [13] X. Lin, X. Sun, P. -H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," in *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007, doi: 10.1109/TVT.2007.906878.
- [14] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBa: Robust Location Privacy Scheme for VANET," in *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007, doi: 10.1109/JSAC.2007.071007.




- [15] L. Zhang, Q. Wu, A. Solanas, and J. D. -Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606-1617, 2010, doi: 10.1109/TVT.2009.2038222.
- [16] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, 2010, doi: 10.1109/TPDS.2010.14.
- [17] K. -A. Shim, "CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks," in *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874-1883, 2012, doi: 10.1109/TVT.2012.2186992.
- [18] J. H. Zhang and Y. W. Xu, "On the Security of a Secure Batch Verification Scheme for VANET," *Advanced Materials Research*, vol. 760-762, pp. 862-866, 2013, doi: 10.4028/www.scientific.net/amr.760-762.862.
- [19] J. Li, H. Lu, and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938-948, 2015, doi: 10.1109/TPDS.2014.2308215.
- [20] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, 1733-1743, 2015, doi: 10.1007/s11276-014-0881-0.
- [21] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681-2691, 2015, doi: 10.1109/TIFS.2015.2473820.
- [22] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," in *Tsinghua Science and Technology*, vol. 21, no. 6, pp. 620-629, 2016, doi: 10.1109/TST.2016.7787005.
- [23] N. -W. Lo and J. -L. Tsai, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319-1328, 2016, doi: 10.1109/TITS.2015.2502322.
- [24] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, 2017, doi: 10.1177/1550147717700899.
- [25] J. Cui, J. Zhang, H. Zhong and Y. Xu, "SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET With Cuckoo Filter," in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283-10295, 2017, doi: 10.1109/TVT.2017.2718101.
- [26] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks," in *IEEE Access*, vol. 6, pp. 2241-2250, 2018, doi: 10.1109/ACCESS.2017.2782672.
- [27] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621-1632, 2019, doi: 10.1109/TITS.2018.2827460.
- [28] M. A. Alazzawi, K. Chen, A. A. Yassin, H. Lu, and F. Abedi, "Authentication and Revocation Scheme for VANETs Based on Chinese Remainder Theorem," 2019 *IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2019, pp. 1541-1547, doi: 10.1109/HPCC/SmartCity/DSS.2019.00212.
- [29] I. A. Kamil and S. O. Ogundoyin, "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks," *Journal of Information Security and Applications*, vol. 44, pp. 184-200, 2019, doi: 10.1016/j.jisa.2018.12.004.
- [30] Y. Ming and H. Cheng, "Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs," *Mobile Information Systems*, vol. 2019, 2019, doi: 10.1155/2019/7593138.
- [31] 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," *Vehicular Communications*, vol. 14, pp. 15-25, 2018, doi: 10.1016/j.vehcom.2018.09.003.
- [32] 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," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722-735, 2021, doi: 10.1109/TDSC.2019.2904274.
- [33] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Computer Networks*, vol. 134, pp. 78-92, 2018, doi: 10.1016/j.comnet.2018.01.015.
- [34] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," *International Conference on the Theory and Application of Cryptology and Information Security*, 2003, vol. 2894, pp. 452-473, doi: 10.1007/978-3-540-40061-5_29.
- [35] V. S. Miller, "Use of Elliptic Curves in Cryptography," *Conference on the Theory and Application of Cryptographic Techniques*, 1986, vol. 218, pp. 417-426, doi: 10.1007/3-540-39799-X_31.
- [36] D. S. Gupta, and G. P. Biswas, "An ECC-based authenticated group key exchange protocol in IBE framework," *International Journal of Communication Systems*, vol. 30, no.18, 2017, doi: 10.1002/dac.3363.
- [37] J. Zhou and Y. -H. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme," *Journal of the Chinese Institute of Engineers*, vol. 32, no.7, pp. 967-974, 2009, doi: 10.1080/02533839.2009.9671584.
- [38] D. S. Gupta, S. H. Islam, M. S. Obaidat, P. Vijayakumar, N. Kumar, and Y. Park, "A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for IIoT Environments," in *IEEE Systems Journal*, vol. 15, no. 2, pp. 1732-1741, 2021, doi: 10.1109/JSYST.2020.3004551.
- [39] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-Based Privacy-Preserving Communication Scheme," in *IEEE Access*, vol. 8, pp. 150914-150928, 2020, doi: 10.1109/ACCESS.2020.3017018.

BIOGRAPHIES OF AUTHORS






Murtadha A. Alazzawi    received the B.Sc. and M.Sc. degrees in computer science from the Science College, University of Basrah, Iraq, in 2010 and 2013, respectively, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, Hubei, China, in 2020. He is currently working with the Department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC). His research interests include security and privacy issues in VANETs, IOT and WSNs. He can be contacted at email: murtadhaali@alkadhum-col.edu.iq.






Mohammed Tali Almalchy    a lecturer at Imam Ja'afar Al-Sadeq university. He holds a PhD degree in information technology from University Politehnica of Bucharest in 2020 and a MSc of computer science from Hamdard university, India in 2012. Also, he received his BSc in Software Engineering from Iraq in 2009. His main research interests include Deep learning, wireless body area network, Wireless sensor network, cryptography, information security, Wireless sensor network, Artificial Intelligence and Computer Networks. He can be contacted at email: Almalchy.leader@gmail.com.






Ahmed Al-Shammari    received the B.Sc. in Computer Science from the University of Al-Qadisiyah, Iraq 2010, and the M.Sc. in Information Technology (Computer Science), from the UKM, Malaysia, 2013. He received the PhD in ICT from the Swinburne University of Technology, Melbourne, Australia, 2019. He works in the areas of Data Mining, Machine Learning, Data Streams Management, Health Informatics, and Service Computing. He is a member of IEEE, and Australian Computer Society (ACS). He also serves as a senior reviewer in the Journal of Network and Computer Applications (JNCA) and Journal of Information Sciences (INS)-Elsevier with Outstanding Contribution Awards in reviewing. He can be contacted at email: ahmed.alshammari@qu.edu.iq.



Ahmed Salih Al-Khaleefa    received the B.Sc. degree in software engineering from Imam Ja'afar Al-Sadiq University, Iraq, in 2013, and the M.Sc. degree in computer science networks department from Universiti Kebangsaan Malaysia, Malaysia, in 2017. He received Ph.D. degree in telecommunication engineering from the Faculty of Electronic Engineering and Computer Engineering (FKEKK), Universiti Teknikal Malaysia Melaka, Malaysia. He is currently serving as Senior Lecturer in the Department of Physics, Faculty of Education, University of Misan, Misan, Iraq. His research interests include communication, security, routing protocols, artificial intelligence, IoT, Optimization, and Localization. He can be contacted at email: alkhaleefa.as@uomisan.edu.iq.



Hayder M. Albehadili    Hayder is a renowned machine learning and AI expert who has achieved exceptional success in his career. He obtained his PhD in machine learning and artificial intelligence from the prestigious University of Missouri in Columbia. Currently serving as a senior engineer at Maysan Oil Company, Hayder has been instrumental in optimizing the company's operations using his expertise in data analysis, computer vision, and machine learning. He's widely recognized for his research contributions, having published numerous papers and articles, and his knowledge is frequently sought by organizations seeking to harness the power of AI. Hayder is a true inspiration in his field, demonstrating the limitless potential of machine learning and AI to solve real-world problems. He can be contacted at email: Phd.hayder@gmail.com.