Hindawi
Security and Communication Networks
Volume 2022, Article ID 3214913, 10 pages
https://doi.org/10.1155/2022/3214913

Research Article

A New Certificateless Signcryption Scheme for Securing Internet of Vehicles in the 5G Era

Beibei Cui,[1,2] **Lu Wei**,[2] **and Wei He**[3]

[1]*Department of Electronic Information, Huishang Vocational College, Hefei 230039, China*
[2]*School of Computer Science and Technology, Anhui University, Hefei 230039, China*
[3]*School of Mechanical and Automotive Engineering, Anhui Water Conservancy Technical College, Hefei 231603, China*

Correspondence should be addressed to Beibei Cui; cuibei3@163.com

Received 25 February 2022; Revised 13 July 2022; Accepted 23 July 2022; Published 19 September 2022

Academic Editor: Anwar Ghani

The application of digital signature technology to the Internet of vehicles (IoV) is affected by its network and communication environment. In the 5G era, the influx of a large number of intelligent devices into the mobile Internet requires a low transmission delay and power consumption as well as high-security requirements. To the best of our knowledge, a well-designed solution in which signcryption technology is used has not been proposed in the IoV research area. Motivated by the fact, a certificateless signcryption scheme based on the elliptic curve digital signature algorithm, in which pseudonym and timestamp mechanism are also considered, has been designed in this paper. We prove that the scheme proposed by us can be reduced to solving the difficulty of the computational Diffie–Hellman problem with a standard model, showing that the scheme meets requirements on both security and efficiency, which provides a comparative analysis with the state-of-the-art schemes in terms of security analysis, computational cost, and communication cost, demonstrating that the scheme proposed by us is suitable to be deployed in the IoV environment, which is of the characteristics of high-speed vehicle movement.

1. Introduction

The Internet of vehicles (IoV) has made significant progress in the 5G era. To meet the needs of research and application, IoV communication can be divided into vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), and vehicle to network (V2N). We call them vehicle to everything (V2X). At present, data transmission of the IoV is realized with the help of the DSRC and cellular network, and then, data are stored in the cloud [1]. Among them, V2X communication is based on the 5G network [2], which has been widely used by global operators and automobile manufacturers. Security issues such as counterfeiting, manipulation, and forgery exist in all the IoV links [3]. Since they are critical aspects in solving the problems of information security and privacy protection, anonymous authentication has become a hotspot of research in recent years. Kamat et al. [4] proposed an identity-based and cryptography-based VANET security framework (IBC). Shamir[5] proposed the concept of an identity-based system. In 1984, a cryptosystem based on arbitrary strings could use conventional anonymity approach for the first time, which entails a third-party trustworthy institution storing the correspondence between all vehicles and anonymous certificates. According to the report, if the authority is not authorized, it may intentionally disclose personal information of the vehicle, forge, and tamper with the legal vehicle identification. Tzeng et al. [6] integrated the identity-based public-key cryptosystem into the Internet of vehicles to meet this challenge. The user's private key is generated by a third-party private key generator (PKG). What can be done if a third-party private key creation center is dishonest or malicious as public keys. For instance, Zhang et al. [7] recommended that fingerprint information be used for identity authentication. Cui et al. [8] adopted edge computing in VANETs to apply privacy protection. Raya and Hubaux[9] proposed that signature of any user can be forged, causing the problem of key escrow. As a result, Al-

Riyami and Paterson[10] presented the concept of a key generation center (KGC), pointing out that any effective key can be generated by the secret value of OBU and partial keys distributed by KGC. A certificateless signature system was presented by Liu et al. [11] in 2007. Keys are no longer solely determined by the CA, and the traditional signature method was broken. Shim [12] devised a novel certificateless signature system and assessed its security using computational Diffie–Hellman (CDH), and Yang et al. [13] considered that the scheme was vulnerable to malicious and passive KGC attacks. Thumbur et al. [14] suggested a certificateless signature technique without bilinear pairing in 2020, claiming that the scheme can be used in IoV with limited resources. Mei et al. [15] suggested a bilinear pairing-based certificateless signature aggregation approach with conditional privacy protection. Under the random oracle paradigm, the approach achieved complete aggregation and was proved to be safe. For V2V secure communication, Ali et al. [16] devised an identity-based message authentication technique without bilinear pairing. When vehicles request to register with the trusted authority (TA), the TA creates pseudonyms and keys for them to secure its anonymity during the communication process. Barbosa and Farshim[17] proposed the certificateless signcryption (CLSC) concept, which can transmit signing and encryption simultaneously. Processing time, broadband occupation, and key management can all benefit from signcryption, which was first proposed by Zheng [18]. Barbosa's method, however, has been shown to be vulnerable to malicious passive KGC assaults. For bilinear pairs, Barreto et al. [19] suggested a certificateless signcryption approach. Suzhen et al. [20] proposed a signcryption technique that includes a privacy protection feature in 2018. Vehicle keys and pseudonyms were generated by TA and PKG, respectively. The bilinear pairing operation was used in the same way in documents [20, 21], with low computational efficiency. Many researchers are now studying signcryption technology [22–25], but no systematic scheme is formed. Du et al. [26] put forward a certificateless signature scheme based on elliptic curve cryptosystems, but there is a replacement key attack. We improve Du et al.'s scheme, propose a new certificateless signcryption scheme based on an elliptic curve, and apply this scheme to the privacy protection of the IoV. We construct a new CLSC scheme to obtain a higher level of security. Our CLSC scheme proves its security of the scheme by using two different types of adversary selection message attacks. Compared with other existing schemes, this scheme avoids expensive bilinear pairing, is more cost-effective, and is suitable for rapidly changing IoV environment. The main contributions of this paper are as follows:

(i) To create pseudonyms, ECC cryptography is employed; the standard tamper-proof device (TPD) and password (PWD) are not used. Instead, the pseudonym is formed using the intermediate variables false identity and timestamp. Therefore, the hidden danger of password theft is avoided, and the system has a high level of privacy protection.

(ii) Combining certificateless and signcryption theory, anonymous is introduced into the scheme. Key generation is related to RSU, OBU, and KGC; the IBC algorithm is improved by two-way authentication among them. Thus, the security of the key is enhanced.

(iii) When compared to other related systems, the computational cost decreased. The scheme satisfies the security requirements of IND-CCA and EUF-CMA, giving the IoV system forward security, anonymity, traceability, and the capacity to prevent replay attacks.

2. Elliptic Curve

If q is a large prime, it satisfies $q \geq 2^{160}$, and Z_q includes all solutions in the finite domain F_q. Elliptic curve E: $y^2 = x^3 + ax + b \bmod q$, and $E(Z_q)$ denotes the set of pairs $(x, y) \in (Z_q \times Z_q)$, satisfying the above equation along with a special value O. That is, $E(Z_q) = \{(x, y) | x, y \in Z_q,\ y^2 = x^3 + ax + b \bmod q \cup O$. The elements $E(Z_q)$ are called the points on the elliptic curve E, where $4a^3 + 27b^2 \neq 0$, and O is called the point at infinity.

(i) Elliptic curve digital signature algorithm (ECDSA) [27]: it is an algorithm through which a random integer k is generated and calculates the point $P = kG$ as well as the number $r = x_p \bmod q$ is calculated, where x_p is the x coordinate of P. Finally, $s = k^{-1}(z + rd_A) \bmod q$ is calculated as a signature, and z is the hash truncation of message M.

(ii) Elliptic curve discrete logarithmic problem (ECDLP): there are two points M, N on the elliptic curve $E(a, b)$, and $M = k \cdot N (\forall k \in Z^*)$ is calculated, when the points M, N are known, the problem of solving the coefficient k is called an elliptic curve discrete logarithmic problem, and the coefficient k cannot be calculated in the polynomial time.

(iii) Elliptic curve Diffie–Hellman problem (ECDHP): the problem is that on inputs $a, b \in Z^*$, point G is taken as the base point in the finite field of elliptic curve $E(a, b)$ to have the given equation, $M = a \cdot G, N = b \cdot G, R = ab \cdot G$ when the values of M and N are known, solving the value of R is called an elliptic curve Diffie–Hellman problem, which cannot be effectively solved in the polynomial time.

2.1. System Overview. In our scheme, the IoV model consists of vehicles, roadside units, key generator centers, and trusted authorities. The specific division of labor is as follows:

Onboard unit (OBU): intelligent vehicles with OBU can exchange information and data with roadside units or other vehicles. Each vehicle periodically broadcasts information for safe driving. To ensure location privacy, each vehicle needs to use a pseudonym to replace its real identity to transmit information.

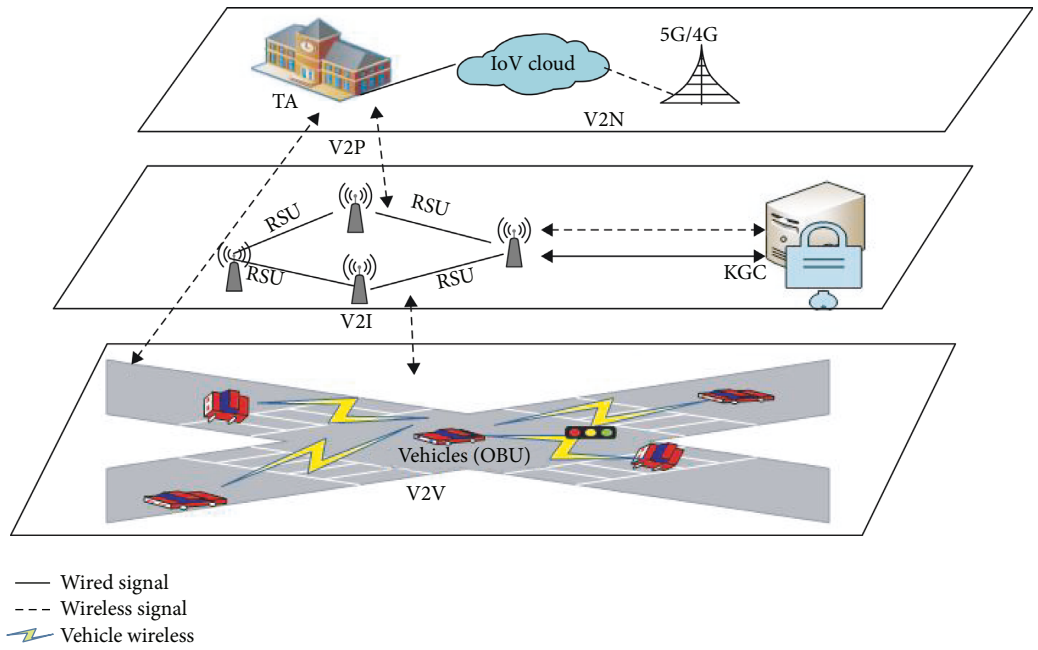

Figure 1: System structure diagram of the IoV.

RSUs (roadside units): RSUs are deployed alongside urban roads, which consist primarily of a wireless communication interface and a local data preprocessing unit. The roadside units are deployed by specific guidelines. As a result, the vehicle can access the roadside units. All the RSUs should be interconnected with the intelligent transportation information data center.

Trusted authority (TA): the TA is managed by the traffic management department and is mainly in charge of OBU identity registration and authentication. It is fully trusted in this scheme and is responsible for generating the false identity of the vehicle.

Key generation center (KGC): the KGC is in charge of communicating with TA to generate partial public/private keys for legitimate OBU and RSUs.

The model is shown in Figure 1.

2.2. Scheme. Our CLSC scheme is designed for IoV communication, eliminates the issue of key escrow, and makes use of a pseudonym mechanism to protect the real identities of both parties to the communication, so ensuring the privacy of the identity and vehicle traceability.

First, in order to eliminate the impact of replacing the public key, the system master key is added to the pseudonym generation formula to make it more difficult for attackers to forge signatures, and make the s impossible to bypass. It can be seen that in the Du et al.' scheme [26], part private key SK_i was calculated by the system master key. The malicious signer cannot calculate the value of the system master key and SK_i through technical means, but the public key of the certificateless signature scheme is not authenticated between the signer and the verifier. The malicious signer forges the signature by forging the secret value and bypassing the unknown system master key. Therefore, there is a key replacement attack. So, in our scheme, signcryption algorithm is introduced to ensure the confidentiality of transmission and improve transmission efficiency. Finally, the security of the scheme is proved in the standard model. The meaning of relevant symbols is shown in Table 1. The flowchart of the algorithm is shown in Figure 2. The algorithm steps are provided.

2.3. Algorithm. There are five participants in the improved certificateless signcryption scheme algorithm: KGC, TA, RSU, the sender of vehicle (V_A), and the receiver of vehicle (V_B). OBU and RSU conduct two-way authentication through TA [28]. We divide the entire scheme into six algorithms, which are listed as follows.

2.3.1. Initialization. The KGC chooses five collision-resistant Hash functions:

$$\begin{aligned} H_0&: \{0,1\}^* \longrightarrow Z_q^*, \\ H_1&: \{0,1\}^* \times G \longrightarrow Z_q^*, \\ H_2&: \{0,1\}^* \times G \times G \longrightarrow Z_q^*, \\ H_3&: \{0,1\}^* \times Z_q^* \times G \times G \longrightarrow Z_q^*, \\ H_4&: \{0,1\}^* \times G \times G \longrightarrow Z_q^*. \end{aligned} \tag{1}$$

The KGC secret saves system master key s and encrypted transmits s to TA, and TA saves (s, RID_i) and generates system public key $P_{\mathrm{pub}} = sP$. The common parameter is $pp = (q, G, P, P_{\mathrm{pub}}, H_0, H_1, H_2, H_3, H_4)$.

Table 1: Parameter description table.

Parameter	Implications
G	Additive cyclic group of order q
P	Generator of group G
s	System master key
Z_q^*	$Z_q^* = \{x: 0 < x < q, \gcd(x, q) = 1\}$
H_0, H_1, H_2, H_3, H_4	Five safe hash functions
P_j, K_j, k_j	The identity of roadside unit j, public key Y_j, and private key y_j
S_i	Partial private key
r_i	KGC generate the secret value to generate public/private keys
x_i	Secret value of the vehicle
ξ_i	Secret value for the RSU
PK_i, SK_i	Public key and private key for a vehicle
RID_i	List of true vehicle identities
F_i	False identity of a vehicle
FID_i	Pseudonym of a vehicle
T_i	Current timestamp of a vehicle
δ	Ciphertext between two vehicles
Y, Y^*	Encryption key and decryption key
V_A, V_B	Vehicle of data sender and vehicle of data receiver
$\mathbb{A}_I, \mathbb{A}_{II}$	Type-I and type-II adversaries

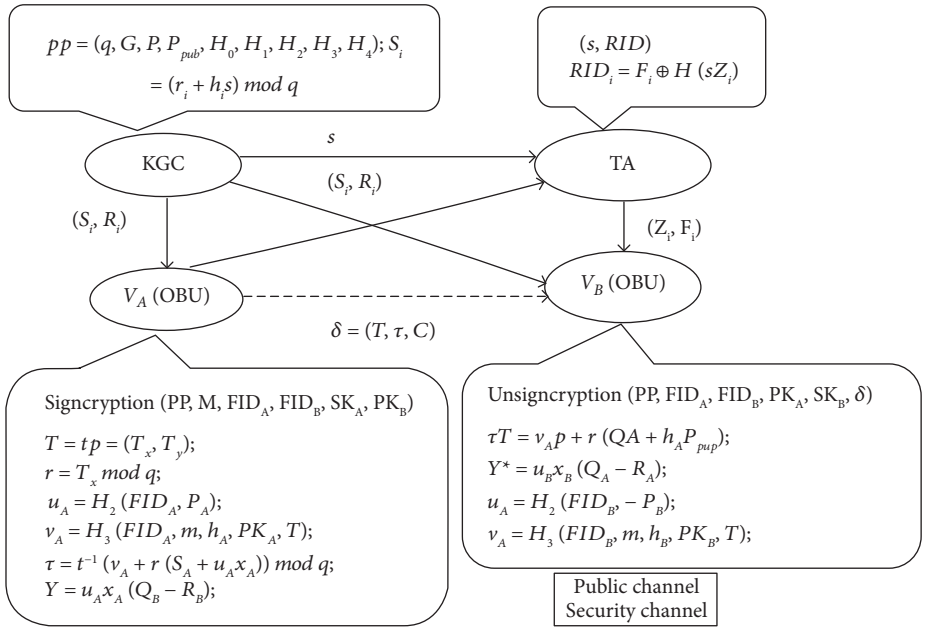

Figure 2: The CLSC of our scheme.

2.3.2. Registration. OBU executes the algorithm, randomly selects $z_i \in Z_i^*$, calculates the negotiation key [29] $Z_i = z_i P$, generates false identity $F_i = \mathrm{RID}_i \oplus H_0(z_i P_{\mathrm{pub}})$, and then sends (Z_i, F_i) to TA. The algorithm is executed by TA, and TA receives the message (Z_i, F_i) from OBU. TA calculates $\mathrm{RID}_i = F_i \oplus H_0(sZ_i)$ and queries whether the vehicle identity list containing RID_i. If not, the algorithm is terminated by TA, and the OBU is determined to be illegal. RSU sets identity as P_j, randomly selects $k_i \in Z_q^*$ as its private key, RSU calculates negotiation key $K_i = k_i P$ and public key $K_j = k_i P_{pub}$, and sends (P_j, K_i) to TA, and TA calculates $\mathbb{K}_j = sK_i$ and forwards $(P_j, \mathbb{K}_j)$ to the legitimate OBU.

2.3.3. Pseudonym Generation. The trusted organization no longer issues the public-key certificates (PKI) to vehicles but generates pseudonyms for them. In this scheme, the generation of a pseudonym consists of three parameters, including false identity of its own, RSU identity information, and timestamp, rather than the device password information. When the vehicle enters the area responsible for RSU, OBU receives K_j from the RSU broadcast. When OBU receives multiple RSU broadcast signals at the same time in a critical environment, it can only record the strongest RSU broadcast information and discard relatively weak RSU broadcast information. The OBU checks the RSU's public

key; if $K_j \notin (P_j, \mathbb{K}_j)$, the RSU will be illegal, and the algorithm will not be executed. Otherwise, OBU obtains the current timestamp T_i and the public key K_j of the current RSU, then selects the secret value $\xi_i \in Z_q^*$ for the RSU. The OBU calculates $\mathrm{FID}_{i1} = F_i \oplus H_0(K_j \xi_i \| T_i)$, $\mathrm{FID}_{i2} = P_j Q$, and sets the pseudonym of the vehicle $\mathrm{FID}_i = (\mathrm{FID}_{i1}, \mathrm{FID}_{i2}, T_i)$.

Through the above operations, TA indirectly judges the legitimacy of RSU. OBU generates the pseudonym through legal RSU, false identity of the vehicle, and the timestamp.

2.3.4. Key Generation

(i) Secret value: OBU chooses a random $x_i \in Z_q^*$ as its secret value. When the pseudonym is updated, the secret value should also be changed randomly, to maintain forward safety [30].

(ii) Partial private/public key: KGC inputs the pseudonym of the vehicle FID_i and the parameter value PP, KGC chooses $r_i \in Z_q^*$ randomly and calculates partial public key $R_i = r_i P$ and partial private key $S_i = (r_i + h_i s) \bmod q$, which is $h_i = H_1(\mathrm{FID}_i, R_i)$. KGC sends (S_i, R_i) to OBU via secure channel.

(iii) Public key extract: OBU calculates $P_i = x_i P$, $u_i = H_2(\mathrm{FID}_i, P_i)$, $Q_i = R_i + u_i P_i$ then generates the public key, which is $PK_i = (R_i, Q_i)$.

(iv) Private key extract: OBU checks whether the $S_i P = R_i + h_i P_{\mathrm{pub}}$ is established. If so, it will be accepted. If not, it will be rejected. The private key is generated as $SK_i = (S_i, x_i)$. Proof of correctness is as follows: $S_i P = (r_i + h_i s)P = R_i + h_i P_{\mathrm{pub}}$.

2.3.5. Signcryption. V_A is the sender of OBU, while V_B is the receiver of OBU, and V_A takes message M, $\mathrm{FID_A}$, FID_B, PP, SK_A, and PK_B as input; generates a random integer t; and produces signcryptext δ. The signcryption generation process is based on ECDSA, and the specific calculation process is as follows:

(i) $T = tP = (T_x, T_y)$, T_x, T_y are the x coordinate value and y coordinate value of point T.

(ii) $\tau = t^{-1}(v_A + r(S_A + u_A x_A)) \bmod q$, where $r = T_x \bmod q$ can be considered as an important parameter for verifying signatures, and there has three hash functions.

$$\begin{aligned} h_A &= H_1(\mathrm{FID}_A, R_A), \\ u_A &= H_2(\mathrm{FID}_A, P_A), \\ v_A &= H_3(\mathrm{FID}_A, m, h_A, PK_A, T). \end{aligned} \tag{2}$$

Hash functions h_1, h_2, and h_3 are used to protect the pseudonym FID_A, message m, and public key PK_A.

$$C = M \oplus w, \tag{3}$$

C is signcryptext, which is generated by M XOR W.

$$w = H_4(\mathrm{FID}_A, \mathrm{FID}_B, Y), \tag{4}$$

$$Y = u_A x_A (Q_B - R_B), \tag{5}$$

V_A sends $\delta = (T, \tau, C)$ to V_B.

2.3.6. Unsigncryption. V_B takes δ, FID_A, FID_B, PP, SK_B, and PK_A as input and returns massage M, if $\tau T = v_A P + r(Q_A + h_A P_{\mathrm{pub}})$ is hold. V_B performs the following steps:

$$w^* = H_4(\mathrm{FID}_A, \mathrm{FID}_B, Y^*), \tag{6}$$

$$\begin{aligned} Y^* &= u_B x_B (Q_A - R_A), \\ u_B &= H_2(\mathrm{FID}_B, P_B). \end{aligned} \tag{7}$$

V_B executes the algorithm $M = C \oplus w^*$ to decrypt the signcryption.

3. Correctness

Only if the following two equations are true, respectively, the scheme meets the correctness.

(i) Public verifiability. The message is signed by V_A, if the verification signature is valid, V_B receives the message. Otherwise, if the signature is invalid, V_B rejects the message.

$$\begin{aligned} \tau T &= t^{-1}(v_A + r(S_A + u_A x_A)) tp \bmod q \\ &= (v_A + r(r_A + h_A s + u_A x_A))P \\ &= v_A P + r(R_A + u_A P_A + h_A P_{\mathrm{pub}}) \\ &= v_A P + r(Q_A + h_A P_{\mathrm{pub}}). \end{aligned} \tag{8}$$

(ii) Consistency of encryption and decryption. If $Y^* = Y$ is true, $w^* = w$ must be true, and $M = C \oplus w^* = M \oplus w \oplus w^*$ must be established.

$$\begin{aligned} Y &= u_A x_A (Q_B - R_B) \\ &= u_A x_A u_B x_B P, \end{aligned} \tag{9}$$

$$\begin{aligned} Y^* &= u_B x_B (Q_A - R_A) \\ &= u_B x_B u_A x_A P. \end{aligned} \tag{10}$$

Both Y and Y^* are deduced from the public key generation algorithm $Q_A = R_A + u_A P_A$, $Q_B = R_B + u_B P_B$, $P_A = x_A P$, and $P_B = x_B P$. From the formulas (4), (6), (9), and (10), it is deduced that the equation $w^* = w$ holds.

$$\begin{aligned} M &= C \oplus w^* \\ &= M \oplus w \oplus w^* \\ &= M \oplus w \oplus w. \end{aligned} \tag{11}$$

Thus, the message M can be restored.

4. Security Proof

Two types of adversaries are considered to prove the security of our scheme [31]. These requirements on security are described via some games between adversaries ($\mathbb{A}_I$ or $\mathbb{A}_{II}$) and a challenger $\mathbb{C}$. Adversaries can be divided into two cases: one is that the adversary $\mathbb{A}_I$ is a malicious who does not know the system master key s, but can replace the public key of any user; the second type of adversary $\mathbb{A}_{II}$ is a malicious KGC attacker, who knows the master key s but cannot replace any public key. In our CLSC scheme, the adversaries may access the following oracles:

(i) H_{PK}: FID_i is entered as an identifier, and a public key PK_i matching FID_i will be returned.

(ii) H_d: FID_i is entered as an identifier, and a partial private key S_i will be returned.

(iii) $H_{\mathrm{Replace}.PK}$: FID_i is entered as an identifier, a new public key PK_i' that can be used will replace the original public key PK_i.

(iv) H_{SK}: FID_i is entered as an identifier, a private key SK_i matching FID_i will be returned, when the public key is not replaced.

(v) $H_{\mathrm{Signcrypt}}$: When there is a message M, identity of a sender is FID_A, and identity of a receiver is FID_B as input, and an available signcryption δ on M will be returned.

(vi) $H_{\mathrm{Unsigncrypt}}$: When a signcryption δ, identity of a sender is FID_A, and identity of a receiver is FID_B as input, the message M will be restored, when δ is available.

$\mathbb{A}_I$ can access all the above oracles, while $\mathbb{A}_{II}$ can access all of them except $H_{\mathrm{Replace}.PK}$ and H_d, because $\mathbb{A}_{II}$ owns the system master key s, $\mathbb{A}_{II}$ can forge partial private key γ; meanwhile, $\mathbb{A}_I$ and $\mathbb{A}_{II}$ can suppose $H_I = \{H_{PK}, H_d, H_{\mathrm{Replace}.PK}, H_{SK}, H_{\mathrm{Signcrypt}}, H_{\mathrm{Unsigncrypt}}\}$ and $H_{II} = \{H_{PK}, H_{SK}, H_{\mathrm{Signcrypt}}, H_{\mathrm{Unsigncrypt}}\}$, respectively. We prove our CLSC scheme from two aspects: confidentiality and unforgeability.

4.1. Confidentiality. This property is considered as the indistinguishability under chosen-ciphertext attack (IND-CCA). In this section, the security proof is proved by some games between adversaries ($\mathbb{A}_I$ or $\mathbb{A}_{II}$) and a challenger $\mathbb{C}$.

Game 1: The game interactions between an adversary $\mathbb{A}$ and a challenger $\mathbb{C}$ are as follows:

(i) Setup: $\mathbb{C}$ inputs a security parameter λ, a common parameter pp and α are generated, of which α is kept as a secret.

(ii) Phase 1 queries: $\mathbb{A}_I$ sends bounded queries in polynomial time to the oracles H_I, and the $\mathbb{C}$ responds to the queries passing through these oracle models.

(iii) Challenge: $\mathbb{A}_I$ sends two equal length messages m_0 and m_1 to challenger $\mathbb{C}$ with FID_A^* and FID_B^* as identifiers. A bit $\gamma \in \{0, 1\}$ is randomly selected by $\mathbb{C}$, through which $\mathrm{Signcrption}(PP, M, \mathrm{FID}_A^*, \mathrm{FID}_B^*, SK_A^*, PK_B^*)$ is implemented by $\mathbb{C}$ and δ is sent to $\mathbb{A}_I$.

(iv) Phase 2 queries: $\mathbb{A}_I$ sends bounded queries in polynomial time to the oracle H_I, and the $\mathbb{C}$ responds to the queries passing through these oracle models.

(v) Guess: $\mathbb{A}_I$ outputs a guess of γ, which is γ^*.

It is said that $\mathbb{A}_I$ wins game 1, if $\gamma^* = \gamma$ and the following conditions are established:

(1) SK_A^* cannot be extracted by $\mathbb{A}_I$ at any point

(2) S_A^* cannot be extracted by $\mathbb{A}_I$, if $\mathbb{A}_I$ has replaced PK_A^* with PK_A' before accepting the challenge

(3) In phase 2 queries, $\mathbb{A}_I$ is unable to perform unsigncryption query on δ^* under FID_A^* or FID_B^*, and signcryption FID_B^*, PK_A^*, or PK_B^* has been replaced after the challenge is issued.

Game 2: The game interactions between an adversary $\mathbb{A}$ and a challenger $\mathbb{C}$: the challenge steps are the same as those of game 1.

(i) Setup: $\mathbb{C}$ inputs a security parameter λ, and a common parameter pp and α are generated. $\mathbb{C}$ sends parameter pp and α to $\mathbb{A}_{II}$.

(ii) Phase 1 queries: $\mathbb{A}_{II}$ sends bounded queries in polynomial time to the oracle H_{II}, and $\mathbb{C}$ responds to the queries passing through these oracle models.

(iii) Challenge: $\mathbb{A}_{II}$ sends two equal length messages m_0 and m_1 to challenger $\mathbb{C}$ with FID_A^* and FID_B^* as identifiers. A bit $\gamma \in \{0, 1\}$ is randomly selected by $\mathbb{C}$, through which $\mathrm{Signcryption}(PP, M, \mathrm{FID}_A^*, \mathrm{FID}_B^*, SK_A^*, PK_B^*)$ is implemented, and then, δ is sent to $\mathbb{A}_{II}$.

(iv) Phase 2 queries: $\mathbb{A}_{II}$ sends bounded queries in polynomial time to the oracle H_{II}, and $\mathbb{C}$ responds to the queries passing through these oracle models.

(v) Guess: $\mathbb{A}_{II}$ outputs a guess γ^* of γ.

It is said that $\mathbb{A}_{II}$ wins game 2 if $\gamma^* = \gamma$ and the following conditions are hold:

(1) $\mathbb{A}_{II}$ cannot extract SK_A^* at any point. Because the secret value x_i cannot be obtained by $\mathbb{A}_{II}$, $\mathbb{A}_{II}$ solves x_i as ECDLP problem.

(2) In phase 2 queries, $\mathbb{A}_{II}$ is unable to perform an unsigncryption query on δ^* under FID_A^* or FID_B^*.

If the probability $\mathrm{Adv}(\mathbb{A}) = 2 * |\Pr[\mathbb{A} - 1/2]|$ is negligible, we say that the scheme is IND-CCA safe. We know that $\mathbb{A}_I$ can access to all of the oracles, while $\mathbb{A}_{II}$ can access to all of them except $H_{\mathrm{Replace}.PK}$ and H_d.

$\mathbb{A}_I$ sends bounded queries in polynomial time to the oracle H_I making a signcryption query $H_{\mathrm{Signcrypt}}$ but cannot win δ under FID_A^* or FID_B^*. The key generation process is $Q_A^* - R_A^* = u_A^* x_A^* P$, $Q_B^* - R_B^* = u_B^* x_B^* P$, and $Y = u_B^* x_B^* u_A^* x_A^* P$. It is still difficult to solve Y, which is an ECDHP problem.

$\mathbb{A}_{II}$ sends bounded queries in polynomial time to the oracle H_{II}, making a public key query H_{PK}, but H_{II} cannot

be used to obtain x_i^*; thus, $\mathbb{A}_{II}$ cannot obtain PK_i, and solving x_i^* is an ECDLP problem.

The probability for $\mathbb{A}_I$ and $\mathbb{A}_{II}$ to win game 1 and game 2 is negligible.

4.2. Unforgeability. This property is considered as the existential unforgeability against the chosen message attack (EUF-CMA). In this section, the security proof is proved through some games between adversaries ($\mathbb{A}_I$or$\mathbb{A}_{II}$) and a challenger $\mathbb{C}$.

Game 3: The game interactions between an adversary $\mathbb{A}$ and a challenger $\mathbb{C}$ are as follows:

(i) Setup: $\mathbb{C}$ inputs a security parameter λ, a common parameter pp and α are generated, and α is kept as a secret.

(ii) Phase 1 queries: $\mathbb{A}_I$ sends bounded queries in polynomial time to the oracle H_I, and $\mathbb{C}$ responds to the queries passing through these oracle models.

(iii) Forgery: $\mathbb{A}_I$ forges the message M^* and signcryption $\delta^* = (T^*, \tau^*, C^*)$ from the sender V_A^* to the receiver V_B^*.

If the decryption output is M^* and the following conditions are met, it is said that $\mathbb{A}_I$ wins game 3.

(1) $\mathbb{A}_I$ cannot extract SK_A^* at any point

(2) $\mathbb{A}_I$ cannot extract SK_i^* for any pseudonym FID_i, if PK_i^* has been replaced

(3) $\mathbb{A}_I$ cannot extract x_A^*

(4) $\mathbb{A}_I$ cannot make a signcryption query on M^* under FID_A^* or FID_B^*

Game 4: The game interactions between an adversary $\mathbb{A}$ and a challenger $\mathbb{C}$: the challenge steps are the same those of as game 3.

(i) Setup: $\mathbb{C}$ inputs a security parameter λ, and a common parameter pp and α are generated. $\mathbb{C}$ sends parameter pp and α to $\mathbb{A}_{II}$.

(ii) Queries: $\mathbb{A}_{II}$ sends bounded queries in polynomial time to the oracle H_{II}, and the $\mathbb{C}$ responds to the queries passing through these oracle models.

(iii) Forgery: $\mathbb{A}_{II}$ creates a forged message m^* or signcryption $\delta^* = (T^*, \tau^*, C^*)$ from the sender V_A^* to the receiver V_B^*.

If the decryption output is M^* and the following conditions are met, it is said that $\mathbb{A}_{II}$ wins game 4.

(1) $\mathbb{A}_{II}$ cannot extract SK_A^* at any point

(2) $\mathbb{A}_{II}$ cannot make a signcryption query on M^* under FID_A^* or FID_B^*

If it is negligible $\mathbb{A}_I$ or $\mathbb{A}_{II}$ to win game 3 and game 4 $(\mathrm{AdvSig}_{\epsilon,A}^{\mathrm{CMA}}(k) \le \mathrm{negl}(k)$, we say that the scheme is EUF-CMA safe. Note that $\mathbb{A}_I$ has access to all of the mentioned oracles, while $\mathbb{A}_{II}$ has access to all of them except $H_{\mathrm{Replace}.PK}$ and H_d.

$\mathbb{A}_I$ executes public key replacement queries from $H_{\mathrm{Replace}.PK}$, which can replace the public key with $PK_A' = (R_A, Q_A')$, $PK_B' = (R_B, Q_B')$, signcryption queries from $H_{\mathrm{Signcrypt}}$, and unsigncryption queries from $H_{\mathrm{Unsigncryption}}$; $\mathbb{A}_I$ randomly selects $t^* \in Z_q^*$, $x_A^* \in Z_q^*$, and $x_B^* \in Z_q^*$, which is used to $T^* = t^*P = (T_x, T_y)$, $r^* = T_x \bmod q$, $v_A^* = H_3(\mathrm{FID}_A^*, m, h_A^*, PK_A', T)$, $Q_A' = x_A^*P - h_A^*P_{\mathrm{pub}}$, and $Q_B' = x_B^*P - h_B^*P_{\mathrm{pub}}$, which are forged, so as to signcrypt the message m^*. Then, signcryption $\delta^* = (T^*, \tau^*, C^*)$ is forged, V_B receives δ^*, and feasibility verification is conducted:

$$\begin{aligned}\tau^*T^* &= t_A^{*-1}(v_A^* + r^*x_A^*)t_A^*P \\ &= (v_A^* + r^*x_A^*)P \\ &= v^*P + r^*\left(Q_A' \quad + h_A^*P_{\mathrm{pub}}\right).\end{aligned} \tag{12}$$

If it is only a signature algorithm without signcryption, the adversary can still forge a signature and pass the authentication by signing before encryption or encrypting before signature, which is the same as Du et al. [26].

$$\begin{aligned}Y' &= u_A^*x_A^*(Q_B' - R_B) \\ &= u_Ax_A\left(x_B^*P - h_B^*P_{\mathrm{pub}} - R_B\right),\end{aligned} \tag{13}$$

$$\begin{aligned}Y^* &= u_B^*x_B^*(Q_A' - R_A) \\ &= u_Bx_B\left(x_A^*P - h_A^*P_{\mathrm{pub}} - R_A\right).\end{aligned} \tag{14}$$

According to formulas (13) and (14), it is known that $Y^* \neq Y'$, so $w^* \neq w'$, the adversary $\mathbb{A}_I$ cannot pass the encryption consistency verification. Public key replacement fails. $\mathbb{A}_{II}$ cannot execute query partial private key from H_d; thus, γ is forged to replace x_A^*, and $t' \in Z_q^*$ is selected to forge $\delta^* = (T^*, \tau^*, C^*)$, where $T^* = t'P$, $\tau^* = t'^{-1}(v_A + r(S_A + u_A'\gamma)) \bmod q$, and $C^* = m^* \oplus w$, in which $P_A' = \gamma P$ and $u_A' = H_2(\mathrm{FID}_A, P_A')$, and V_B gets δ^*; then, a feasibility verification is done.

$$\begin{aligned}\tau^*T^* &= \left(t'^{-1}(v + r(S_A + u_A'\gamma))\right)t'P \bmod q \\ &= (v' + r(r_A + h_As + u_A'\gamma)) \\ &= P \\ &= v'P + r\left(R_A + h_AP_{\mathrm{pub}} + u_A'P_A\right),.\end{aligned} \tag{15}$$

$\mathbb{A}_{II}$ cannot replace any public key. It is known that $Q_A \neq R_A + h_AP_A$; thus, $\tau^*T^* \neq vP + r(Q_A + h_AP_{\mathrm{pub}})$. The output will be INVALID, and V_B discards the ciphertext.

The probability of $\mathbb{A}_I$ and $\mathbb{A}_{II}$ to win game 3 and game 4 is negligible.

5. Security Analysis

5.1. Forward Security. If the system master key s is omitted, it is calculated due to the difficulty of ECDLP, it is still difficult to calculates r_i and x_i, and (PK_i, SK_i) remains unknown. Therefore, it is guaranteed that the past signcryption information will not be disclosed, because of the randomness of r_i and x_i. When the system master key is omitted, the new values will immediately replace it. The key

Table 2: Run time of the different encryption operations.

Symbol	Operation	Parameter	Runtime (ms)
T_{em}	Elliptic curve point multiplication	$x \cdot P(P \in G, x \in z_q^*)$	0.341
T_{in}	Inverse mode	$t^{-1} \bmod q(t \in z_q^*, q \in z_q^*)$	0.029
T_{ea}	Elliptic curve point plus	$P + Q(P \in G, Q \in G)$	0.002
T_{bp}	Time required for the bilinear pairing	$e(\overline{S}, \overline{T})(\overline{S} \in G_1, \overline{T} \in G_1)$	4.669
T_{pm}	Pairing multiplication operation	$\overline{x} \cdot \overline{P}(\overline{x} \in z_q^*, \overline{P} \in G)$	0.788
T_{pa}	Pairing addition	$\overline{S} + \overline{T}(\overline{S} \in G_1, \overline{S} \in G_1)$	0.002
T_{mtp}	MapToPoint hash function	H_1: $0, 1^* \longrightarrow G_1$	0.145
T_e	Modular exponentiation	$g^* \bmod n$	1.915

update is realized, and these actions further confirm the security of the communication [32].

5.2. Traceability. The ciphertext should contain relevant information about the vehicle identity. In the scheme, TA can be used to calculate $\mathrm{RID}_i = F_i \oplus H_0(sZ_i)$ using the system master key s, which queries whether RID_i is listed in the vehicle identity. It seems that only the trusted authority TA can track the vehicle according to the relevant information. In addition, the IoV requires an extremely high real-time nature. The ciphertext contains timestamp information, which can also prevent replay attacks. Because ciphertext $C = M \oplus w$; $w = H_4(\mathrm{FID}_A, \mathrm{FID}_B, Y)$, here we can use the pseudonym of the vehicle $\mathrm{FID}_i = (\mathrm{FID}_{i1}, \mathrm{FID}_{i2}, T_i)$, making the ciphertext contains timestamp information.

5.3. Anonymous. Pseudonyms are used in V2V and V2I communications to protect the true identity of the vehicle. The pseudonym of the vehicle consists of three parts: $\mathrm{FID}_i = (\mathrm{FID}_{i1}, \mathrm{FID}_{i2}, T_i)$, where FID_{i1} is generated by the false identity F_i of the vehicle, $\mathrm{FID}_{i1} = F_i \oplus H_0(K_j \xi_i \| T_i)$, $F_i = \mathrm{RID}_i \oplus H_0(z_i P_{\mathrm{pub}})$, $\mathrm{FID}_{i2} = P_j$, and T_i is the timestamp to ensure the anonymity of the vehicle. It is necessary to protect the identity information RID_i of the vehicle when the pseudonym information is disclosed. According to the irreversibility of a hash function and the difficulty of ECDLP, the attacker cannot calculate z_i, ξ_i, or k_i in polynomial time, so the RID_i of the vehicle cannot be obtained. In addition, vehicles carry different pseudonyms in different RSU communication ranges and timestamps; that is, the pseudonym information of the vehicle changes with position and time, which makes the generation process of a pseudonym a one-way trapdoor function.

5.4. Unforgeable. The unforgeability of the CLSC scheme is proven in the unforgeability section using a (existential unforgeability against selected message attacks, EUF-CMA) security model. The signature ciphertext forged by an attacker does not satisfy the encryption consistency or convey the attacker's intentions.

6. Performance Evaluation

Computational cost, communication cost, and safety analysis are analyzed in this section compared with other relevant schemes [33–38]. The schemes selected for comparison are certificateless signcryption, which can be applied to the IoV.

The computational cost mainly depends on the amount of signcryption and unsigncryption algorithms, which can be measured based on the number of execution times of statistical elliptic curve scalar multiplication, elliptic curve scalar addition, bilinear pairing, and mapping to point operation. The computational cost of XOR operation on Z_q^* is too small to make comparison. The operation results are listed in Table 2. The experimental system environment is as follows:

CPU: Intel core i7-6700@3.40 GHz; RAM: 8 GB;

OS: Ubuntu 16.04;

Library: MIRACL, a public C++cryptographic library; [https://github.com/miracl/MIRACL/archive/master.zip].

Under the same operating environment, our scheme costs 1.397 ms, Kasyoka et al.'s scheme [33] costs 1.705 ms, Karati et al.'s scheme [34] costs 2.424 ms based no pairing, Karati et al.'s scheme [35] costs 18.913 ms based on bilinear pairing, He et al.'s [36] scheme costs 2.05 ms, and Seo et al.'s [38] scheme costs 3.41 ms. Compared with the other schemes [33–36, 38], our scheme in this paper decreases by 18.06%, 42.37%, 92.61%, 31.85%, and 59.03%, respectively.

Communication cost is measured by the length of a single ciphertext. In the bilinear pairing operation scheme, the length of $|G_1|$ is 1024 bit, and that of $|G_2|$ is the same. To provide the security schemes of the same level for a scheme based on the elliptic curve, q is the prime number and the length of $|Z_q^*|$ is 160 bit. The additive cyclic group with q order generation for point P on a nonsingular elliptic curve is G, and the length of $|G|$ is 320 bit.

The superiority of this scheme is illustrated by comparing the computation and communication overhead of a single ciphertext, which is statistically analyzed in Table 3.

In the comparative analysis of communication cost, the length of a single ciphertext is used as the unit of comparison, which is 640 bit in our scheme, slightly higher than that of Kasyoka et al.'s [33] and Seo et al.'s [38] and is lower than that of Karati et al.'s [35] and He et al.'s [36] bilinear pairing scheme, the same as no pairing scheme of Karati et al. [34].

Table 3: Performance comparison of different signcryption schemes.

Scheme	Calculate cost			Communication cost	
	Signcryption	Unsigncryption	Runtime	Signcryptext	Length
[33]	$2T_{em}$	$3T_{em}$	1.705 s	$3\|Z_q^*\|$	480 bit
[34]	$3T_{em} + 2T_{ea} + T_{in}$	$4T_{em} + 2T_{ea}$	2.424 s	$2\|Z_q^*\| + \|G\|$	640 bit
[35]	$3T_e$	$2T_e + 2T_{bp}$	18.913 s	$4\|G_1\| + \|Z_q^*\|$	4256 bit
[36]	$3T_{em}$	$3T_{em} + 2T_{ea}$	2.05 s	$3\|G\| + \|Z_q^*\|$	1120 bit
[38]	$3T_{em}$	$7T_{em}$	3.41 s	$3\|Z_q^*\|$	480 bit
Our CLSC	$T_{in} + T_{em}$	$2T_{ea} + 3T_{em}$	1.397 s	$2\|Z_q^*\| + \|G\|$	640 bit

Table 4: Safety comparison.

Scheme	Confidentiality	Unforgeability	Forward security	Anonymous
[33]	False	True	False	False
[34]	False	False	False	False
[35]	True	False	False	False
[36]	False	True	False	True
[37]	False	True	False	False
[38]	True	True	False	False
Our CLSC	True	True	True	True

Our CLSC scheme is designed according to a certificateless signcryption model and relies on ECDSA, which depends on the difficulty of pseudonyms generation. In this section, the security of the algorithm is compared and with that of similar schemes and is then analyzed. The result is in Table 4.

7. Conclusion

In this paper, we construct a reliable certificateless signcryption scheme without bilinearity, where a pseudonym mechanism is also designed to protect the privacy of vehicles. We use certificateless signcryption technology to implement the scheme, which can secure vehicular communication with a low computation overhead. Performance analysis demonstrates that the scheme proposed by us can be used to reduce computational and communication cost compared with other related schemes. Security proofs and analyses show that the scheme proposed by us can be used to avoid replacement public key attacks, and ensure the satisfaction of the security of IND-CCA as well as EUF-CMA. Other requirements on security including perfect forward secrecy, anonymity, traceability, and resistance of replay attacks can also be ensured.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the funding project for Top Talent Cultivation in Colleges and Universities in Anhui Province (gxgnfx2020178) and the Natural Science Research Project of Colleges and Universities in Anhui Province (KJ2018A0944).

References

[1] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 1, pp. 1654–1667, 2020.

[2] W. Qi, B. Landfeldt, Q. Song, L. Guo, and A. Jamalipour, "Traffic differentiated clustering routing in DSRC and C-V2X hybrid vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, 2020.

[3] C. Song, M. Y. Zhang, W. P. Peng, Z. Z. Liu, Z. P. Jia, and X. X. Yan, "Research on anonymous authentication scheme in VANET," *Journal of Chinese Computer Systems*, vol. 39, no. 5, pp. 899–903, 2018.

[4] P. Kamat, A. Baliga, and W. Trappe, "An Identity-Based Security Framework for VANETs," in *Proceedings of the International Workshop on Vehicular Ad Hoc Networks*, January 2006.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the CRYPTO 84 on Advances in Proceedings of CRYPTO 84 on Advances in Cryptology*, Santa Barabara, California, USA, 1985.

[6] S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2017.

[7] 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 Transactions on Dependable and Secure Computing*, vol. 18, 2019.

[8] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs-an efficient and privacy-preserving

cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[9] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[10] S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 452–473, Taipei, Taiwan, 2003.

[11] J. K. Liu, M. H. Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model," *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, pp. 273–283, Springer, Berlin, Germany, 2007.

[12] K. A. Shim, "A new certificateless signature scheme provably secure in the standard model," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1421–1430, 2019.

[13] W. Yang, S. Wang, W. Wu, and Y. Mu, "Top-level secure certificateless signature against malicious-but-passive KGC," *IEEE Access*, vol. 7, Article ID 112870, 2019.

[14] G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, and D. V. R. K. Reddy, "Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1641–1645, 2020.

[15] Q. Mei, X. Hu, J. H. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in IoV," *IEEE Systems Journal*, vol. 15, pp. 1–12, 2020.

[16] I. Ali, T. Lawrence, and F. G. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *Journal of Systems Architecture*, vol. 103, Article ID 101692, 2020.

[17] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security-ASIACCS*, pp. 369–372, Tokyo, Japan, March 2008.

[18] Y. Zheng, "Digital Signcryption or How to Achieve Cost(-signature & Encryption)<<cost (Signature)+cost (encryption)," in *Proceedings of the Annual International Cryptology Conference*, pp. 165–179, Berlin, Germany, May 1997.

[19] P. S. L. M. Barreto, A. M. Deusajute, E. De, S. Cruz, and R. R. D. Silva, "Toward Efficient Certiicateless Signcryption from (And without) Bilinear Pairings [EB/OL]," 2008, https://pdfs.semanticscholar.org/c42d/307a94023543067d9668b2fc9442d443070a.pdf.

[20] C. A. O. Suzhen, X. Lang, X. Liu, and F. Wang, "New heterogeneous signcryption scheme under 5G network," *Netinfo Security*, vol. 18, no. 11, pp. 33–39, 2018.

[21] F. G. Li, M. Shirase, and T. Takagi, "Certificateless hybrid signcryption," *Mathematical and Computer Modelling*, vol. 57, no. 3-4, pp. 324–343, 2013.

[22] Z. Liu, Y. Hu, X. Zhang, and H. Ma, "Certificateless signcryption scheme in the standard model," *Information Sciences*, vol. 180, no. 3, pp. 452–464, 2010.

[23] C. Zhou, W. Zhou, and X. Dong, "Provable certificateless generalized signcryption scheme," *Designs, Codes and Cryptography*, vol. 71, no. 2, pp. 331–346, 2014.

[24] M. Luo, M. Tu, and J. Xu, "A security communication model based on certificateless online/offline signcryption for Internet of Things," *Security and Communication Networks*, vol. 7, no. 10, pp. 1560–1569, 2013.

[25] H. F. Yu and B. Yang, "Provably secure certificateless hybrid signcryption," *Chinese Journal of Computers*, vol. 38, no. 4, pp. 804–813, 2015, in Chinese with English abstract.

[26] H. Du, Q. Wen, S. Zhang, and M. Gao, "A new provably secure certificateless signature scheme for Internet of Things," *Ad Hoc Networks*, vol. 100, Article ID 102074, 2020.

[27] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[28] L. Wei, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "A lightweight and conditional privacy-preserving authenticated key agreement scheme with multi-TA model for fog-based VANETs," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2021.

[29] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1810–1824, 2021.

[30] G. Itkis and L. Reyzin, "Forward-secure signatures with optimal signing and verifying," *Advances in Cryptology - CRYPTO 2001*, Springer, vol. 2139, pp. 332–354, Santa Barbara, CA, USA, 2001.

[31] R. Parvin, S. Willy, and D. Mohammad, "Efficient certificateless signcryption in the standard model: revisiting Luo and wan's scheme from wireless personal communications," *The Computer Journal*, vol. 62, no. 8, 2018.

[32] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Transactions on Information Forensics and Security*, vol. 16, 2020.

[33] P. Kasyoka, M. Kimwele, and S. M. Angolo, "Cryptanalysis of a pairing-free certificateless signcryption scheme," *ICT Express*, vol. 7, no. 2, pp. 200–204, 2021.

[34] A. Karati, C. I. Fan, and J. J. Huang, "An efficient pairing-free certificateless signcryption without secure channel communication during secret key issuance ☆," *Procedia Computer Science*, vol. 171, pp. 110–119, 2020.

[35] A. Karati, C. I. Fan, and R. H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 6, Article ID 10431, 2019.

[36] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[37] X. Jia, D. He, Q. Liu, and K. K. R. Choo, "An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment," *Ad Hoc Networks*, vol. 71, pp. 78–87, 2018.

[38] S. H. Seo, J. Won, and E. Bertino, "pCLSC-TKEM: a pairing-free certificateless signcryption-tag key encapsulation mechanism for a privacy-preserving IoT," *Transactions on Data Privacy*, vol. 9, no. 2, pp. 101–130, 2016.