A New Certificateless Signcryption Scheme for Securing Internet of Vehicles

Beibei Cui (cuibei3@163.com)
Anhui University Longhe Campus: Anhui University
Lu Wei
Anhui University Longhe Campus: Anhui University
Wei He
Anhui Water conservancy Technical college

Research Article

Keywords: Elliptic Curve, Certificateless signcryption, Pseudonym, Timestamp mechanism

Posted Date: January 28th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1272183/v1

A New Certificateless Signcryption Scheme for Securing Internet of Vehicles

First Beibei Cui[1,2*], Second Lu Wei[2,3†] and Third Wei He[3,4†]

[1*]Department of Electronic Information ,Huishang Vocational College, Zipeng Road, Hefei, 230039, Anhui, China.
[2]The Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, JiuLong Road, Hefei, 230039, Anhui, China.
[3]School of Computer Science and Technology, Anhui University, JiuLong Road, Hefei, 230039, Anhui, China.
[4]School of mechanical and automotive engineering, Anhui Water Conservancy Technical College, No. 18, Hema road, Feidong County, Hefei City, Anhui Province, Hefei, 231603, Anhui, China.

*Corresponding author(s). E-mail(s): cuibei3@163.com;
Contributing authors:
Great$_h$e@163.com; dreamer$_w$eilu@163.com;
†These authors contributed equally to this work.

Abstract

The application of digital signature technology on the Internet of Vehicles (IoV) is affected by its network and communication environment, which requires low transmission delay, power consumption, and high-security requirement. To the best of our knowledge, a well-designed solution that uses signcryption technology has not been proposed in the IoV research area. Motivated by the fact, a certificateless signcryption scheme based on Elliptic Curve Digital Signature Algorithm, which also considers pseudonym and timestamp mechanism, has been designed in this paper. We prove that our proposed scheme can be reduced to solving the difficulty of the Computational Diffie-Hellman problem under the standard model, show that the scheme meets both security and efficiency requirements, and provides a comparative analysis with the state-of-the-art schemes in terms of security analysis, computational cost, and communication cost, demonstrating that our proposed scheme is suitable to be deployed in the IoV environment.

Keywords: Elliptic Curve; Certificateless signcryption; Pseudonym; Timestamp mechanism

1 Introduction

In the 5g era, Internet of vehicles (IoV) has developed rapidly. To meet the needs of research and application, IoV can be divided into vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), and vehicle and network(V2N) communication. They are exchange data using wired or wireless communication and store the data in the cloud environment[1].

There are security problems such as counterfeiting, tampering, and forgery[2] in all links of IoV. Anonymous authentication is the key factor to solve the problem of information security and privacy protection, it is a research hotspot in recent years. Kamat et al.[3] proposed a security framework for VANETs based on Identity-Based Cryptography (IBC). IBC was first proposed by Shamir [4] as early as 1984, the idea of an identity-based cryptosystem in which arbitrary strings can act as public keys. For example, Zhang et al.[5] proposed to use fingerprint information as identity authentication. Cui et al.[17] applied the privacy protection of edge computing used in VANETs. Raya et al.[6] proposed a conditional anonymity scheme, which requires a third-party trusted organization to store the correspondence between all vehicles and anonymous certificates. When the authority is not authorized, it may deliberately disclose vehicle privacy information, forge and tamper with legal vehicle identity. To solve this problem, Tzeng et al.[7] introduces the identity-based public-key cryptosystem into the Internet of vehicles and designs an identity-based public-key cryptosystem authentication scheme. The user's private key is generated by the third-party private key generator (PKG). However, if the third-party private key generation center is dishonest or malicious, it can forge the signature of any user, which has the problem of key escrow. Therefore, Al-Riyami et al.[8] put forward the concept of key generator center(KGC), pointing out that the generation of any effective signature based on obtaining the secret value of OBU and partial keys distributed by KGC at the same time. In 2007, Liu et al.[9] proposed a certificateless signature scheme. Compared with the traditional certificate-based signature scheme, the key is no longer simply determined by CA. Shim[10] designed a new certificateless signature scheme and analyzed the security of the scheme based on Computational Diffie Hellman (CDH), but Yang et al.[11] considered that the scheme is vulnerable to malicious but passive KGC attacks. In 2020, Thumbur et al.[12] proposed a certificateless signature scheme without bilinear pairing, saying that the scheme can be deployed in source constrained IoV. Mei et al.[13] proposed a certificate-less signature aggregation scheme with conditional privacy protection based on bilinear pairing. The scheme realizes complete aggregation and can be proved to be secure under the random oracle model. Ali et al.[14] designed an identity-based message authentication scheme without bilinear

pairing for V2V secure communication. When vehicles apply to the trusted authority (TA) for registration, the TA generated pseudonyms and keys for them to protect privacy in the communication process.

Barbosa et al.[15] proposed the definition form of certificateless signcryption (CLSC), their scheme introduced signcryption. Signcryption was originally proposed by Zheng[16] for the first time, which can transmit signature and encryption simultaneously. Signcryption can improve efficiency in processing time, broadband occupation, and key management. But Barbosa's scheme was pointed out to be vulnerable to malicious passive KGC attacks. Barreto et al.[18] proposed a certificateless signcryption scheme for bilinear pairs. In 2018, CAO et al.[19] proposed a signcryption scheme with privacy protection function. TA and PKG generated pseudonyms and keys of vehicles respectively. Schemes in literature[19] and literature[20] bilinear pairing operation adopted in the same way, which had low computational efficiency. At present, many scholars have studied signcryption technology[21–24], but no systematic scheme formed. Du et al.[25] put forward a certificateless signature scheme based on elliptic curve cryptosystemc but exist a replacement key attack. We improve Du et al's scheme, propose a certificateless signcryption scheme based on an elliptic curve, and the scheme is applied to the privacy protection of the IoV. The main contributions of this paper are as follows:

2 Results

- The ECC cryptography is used to construct pseudonyms, the traditional tamper-proof device(TPD) and password(PWD) are abandoned, the pseudonym is generated through the intermediate variable false identity and timestamp. So the scheme has strong privacy protection capability.
- Combining certificateless and signcryption theory, anonymous is introduced in the scheme. Key generation is related to RSUs, OBU, and KGC; the IBC algorithm is improved. Thus, the security of the key is enhanced.
- Computational cost decreased at least 18% compared with other relevant schemes. The scheme satisfies the security of IND-CCA and EUF-CMA that makes the IoV system have forward security, anonymity, traceability, and can avoid replay attacks.

3 Elliptic curve

If q is a large prime, it satisfies $q >= 2^{160}$, Z_q includes all solutions in the finite domain F_q elliptic curve $E : y^2 = x^3 + ax + b \bmod q$, let $E(Z_q)$ denote 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 $4a^3 + 27b^2 \neq 0$, O is called the point at infinity.

- Elliptic Curve Digital Signature Algorithm(ECDSA) is mainly used to create a digital signature for data and verify its authenticity without destroying

security. Take a random integer k, Calculate the point $P = kG$, Calculate the number $r = x_p \bmod q$, where $r = x_p$ is the x coordinate of P. Calculate $s = k^{-1}(z + rd_A) \bmod q$, z is the hash truncation of message M.

- Elliptic curve discrete logarithmic problem (ECDLP), selecting additive cyclic group G with order of the large prime q, P is any generator of additive cyclic group G. It is know $P, aP \in G$, but it's unknown $a \in Z_q^*$, any probabilistic polynomial-time algorithm is difficult to compute the advantage in the a, looking for advantages in solution $Pr[a|P, aP \in G]$ is considered negligible.
- Computational Diffie-Hellman(CDH) problem, selecting additive cyclic group G with order of the large prime q, P is any generator of additive cyclic group G. It is known that $P, aP, bP \in G$, but it's unknown $a, b \in Z_q^*$, any probabilistic polynomial time algorithm is difficult to compute the advantage in the abP, finding the solution $Pr[abP|P, aP, bP \in G]$ is considered negligible.

4 System Overview

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

Onboard Unit (OBU): Vehicles equipped with OBU are intelligent and can exchange information and data with roadside units and 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.

Roadside Units (RSUs): RSUs deploy along with urban roads. They are mainly composed of a wireless communication interface and local data preprocessing unit. The roadside units are deployed according to specific rules. Therefore, the vehicle can access the roadside units. All RSUs equipment should wire to the intelligent transportation information data center.

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

Key Generation Center (KGC): KGC is responsible for two-way communication with TA to generate partial public/private keys for legitimate OBU and RSUs.

The model as been shown in Figure 1.

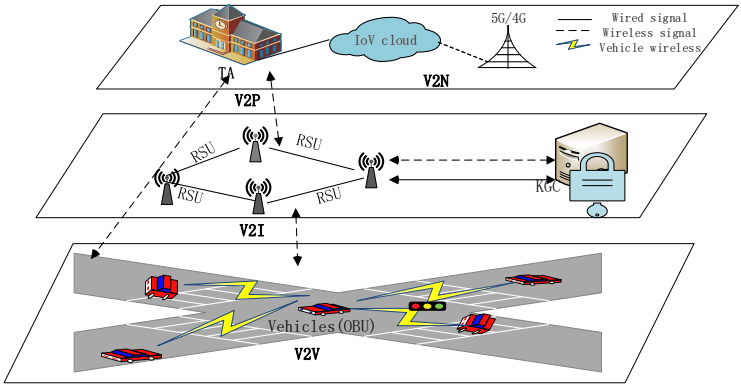

Fig. 1 System structure diagram of the IoV.

4.1 Scheme

The scheme is designed for IoV communication, avoids the problem of key escrow, the pseudonym mechanism is adopted to protect the real identity of both sides of the communication, ensures the confidentiality of the identity and the traceability of vehicles.

First, to eliminate the impact of replacing the public key in our scheme. The system-master-key is added to the pseudonym generation formula to enhance the difficulty of the attacker's forgery signature, making the s cannot be bypassed. It can be seen that in the Du et al'scheme [25], 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 table1 and the flow chart of the algorithm is shown in figure 2. The algorithm steps are as follows:

Table 1 Parameter Description Table.

line	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, 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, 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, Decryption key
V_A, V_B	Vehicle of data sender, Vehicle of data receiver
$\mathbb{A}_{\mathrm{I}}, \mathbb{A}_{\mathrm{II}}$	Type-I and Type-II adversaries

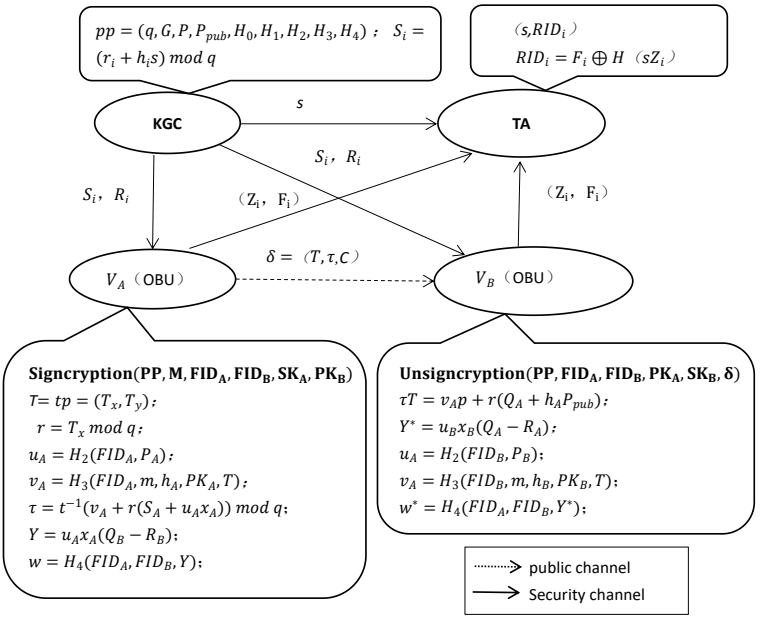

Fig. 2 The CLSC of our scheme.

4.2 Algorithm

The certificateless signcryption scheme based on ECDSA, comprises five players: KGC, TA, RSU, the sender of vehicle (V_A), and the receiver of vehicle(V_B). OBU and RSU pass TA for two-way authentication[26]. We divide the whole scheme into six algorithms as follows:

4.2.1 Initialization

The KGC selects the five collision-resistant Hash functions:

$H_0 : \{0,1\}^* \to Z_q^*$;
$H_1 : \{0,1\}^* \times G \to Z_q^*$;
$H_2 : \{0,1\}^* \times G \times G \to Z_q^*$;
$H_3 : \{0,1\}^* \times Z_q^* \times G \times G \to Z_q^*$;
$H_4 : \{0,1\}^* \times G \times G \to Z_q^*$.

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

4.2.2 Registration

The OBU executes the algorithm, OBU random selection $z_i \in Z_i^*$, calculates the negotiation key[27] $Z_i = z_i P$, generates false identity $F_i = RID \oplus H_0(z_i P_{pub})$, then sends (Z_i, F_i) to TA. The algorithm is executed by TA, TA receives the message (Z_i, F_i) from OBU. TA calculates $RID_i = F_i \oplus H_0(sZ_i)$, queries whether the vehicle identity list containing RID_i. If not, TA terminates the algorithm and determines it as an illegal OBU. RSU set identity as P_j, randomly selected $k_i \in Z_q^*$ as its private key, RSU calculate the negotiation key $K_i = k_i P$, the public key $K_j = k_i P_{pub}$, and sents (P_j, K_i) to TA, TA calcuates $\mathbb{K}_j = sK_i$ and forwards $(P_j, \mathbb{K}_j)$ to the legitimate OBU.

4.2.3 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 the RSU, it receives K_j from the RSU broadcast. The OBU checks the RSU's public key, if $K_j \notin (P_j, \mathbb{K}_j)$, the RSU is illegal, the algorithm is not executed. Otherwise, the 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 $FID_{i1} = F_i \oplus H_0(K_j \xi_i \,||\, T_i)$, $FID_{i2} = P_j$, the OBU sets the pseudonym of the vehicle $FID_i = (FID_{i1}, FID_{i2}, T_i)$.

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.

4.2.4 Key generation

- **Secret-Value:** OBU chooses a random $x_i \in Z_q^*$ as the secret value.
- **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, calculates partial public key $R_i = r_i P$, partial private key $S_i = (r_i + h_i s) \bmod q$, which $h_i = H_1(FID_i, R_i)$. KGC via secure channel sends $(S_i, R_i)$to OBU.
- **Public-key-extract:** OBU calculates $P_i = x_i P, u_i = H_2(FID_i, P_i)$, $Q_i = R_i + u_i P_i$ then generates the public key is $PK_i = (R_i, Q_i)$.
- **Private-key-extract:** OBU checks whether the $S_i P = R_i + h_i P_{pub}$ is established. If it established, it will be accepted. If not, it will be rejected. Generates the private key $SK_i = (S_i, x_i)$. Proof of correctness: $S_i P = (r_i + h_i s)P = R_i + h_i P_{pub}$.

4.2.5 Signcrption

V_A is the sender of OBU, V_B is the receiver of OBU, V_A takes message M, FID_A, FID_B, PP, SK_A and PK_B as input, and produces signcryptext δ. The algorithm is as follows:

- $T = tP = (T_x, T_y)$, T_x, T_y are the x coordinate value and y coordinate value of point T.
- $\tau = t^{-1}(v_A + r(S_A + u_A x_A)) \bmod q$.
  Where
  $h_A = H_1(FID_A, R_A)$;
  $v_A = H_3(FID_A, m, h_A, PK_A, T)$;
  $r = T_x \bmod q$;
  $u_A = H_2(FID_A, P_A)$;
- $C = M \oplus w$.
  Where
  $Y = u_A x_A(Q_B - R_B)$;
  $w = H_4(FID_A, FID_B, Y)$.

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

4.2.6 Unsigncryption

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

- $w^* = H_4(FID_A, FID_B, Y^*)$;
- $Y^* = u_B x_B(Q_A - R_A)$;
- $u_B = H_2(FID_B, P_B)$.

V_B executes $M = C \oplus w^*$.

5 Correctness

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

- 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.
  $\tau T = t^{-1}(v_A + r(S_A + u_A x_A))tp \bmod q$
  $= (v_A + r(r_A + h_A s + u_A x_A))P$
  $= v_A P + r(R_A + u_A P_A + h_A P_{pub})$
  $= v_A P + r(Q_A + h_A P_{pub})$.
- Consistency of encryption and decryption, if $Y^* = Y$ is true, $w^* = w$ must be true, $M = C \oplus w^* = M \oplus w \oplus w^*$ must be established.
  $Y = u_A x_A(Q_B - R_B)$; $Q_B - R_B = u_B P_B = u_B x_B P$; $Y = u_A x_A u_B x_B P$;
  $Y^* = u_B x_B(Q_A - R_A)$; $Q_A - R_A = u_A P_A = u_A x_A P$; $Y^* = u_B x_B u_A x_A P$;
  $Y^* = Y$; $w^* = w$;
  $M = C \oplus w^* = M \oplus w \oplus w^* = M \oplus w \oplus w$.

6 Security proof

To prove the security of our scheme, two types of adversaries are considered[28]. These security requirements are described via some games between an adversary ($\mathbb{A}_{\mathrm{I}}$ or $\mathbb{A}_{\mathrm{II}}$) and a challenger $\mathbb{C}$. Adversaries can be divided into two cases: one is that the adversary $\mathbb{A}_{\mathrm{I}}$ is a malicious user attacker. The adversary $\mathbb{A}_{\mathrm{I}}$ does not know the system master key s, but can replace the public key of any user; the second type of adversary $\mathbb{A}_{\mathrm{II}}$ is a malicious KGC attacker. This type of attacker knows the master key s but cannot replace any public keys. In our CLSC scheme, the adversaries may access the following oracles:

- H_{PK}. FID_i is entered as an identifier, a public-key PK_i matching FID_i will be returned.
- H_d. FID_i is entered as an identifier, a partial-private key S_i will be returned.
- $H_{Replace.PK}$. 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.
- 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.
- $H_{Signcrypt}$. When there are a message M, identity of a sender FID_A, and identity of a receiver FID_B as input, An available signcryption δ on M will be returned.
- $H_{Unsigncrypt}$. When a signcryption δ, identity of a sender FID_A, and identity of a receiver FID_B are given, the message M will be restored, when δ is available.

$\mathbb{A}_{\mathrm{I}}$ can access all the above oracles, while $\mathbb{A}_{\mathrm{II}}$ can access all of them except $H_{Replace.PK}$ and H_d, becuase $\mathbb{A}_{\mathrm{II}}$ owns system-master-key s, can forge partial-private key γ, $\mathbb{A}_{\mathrm{I}}$ and $\mathbb{A}_{\mathrm{II}}$ can suppose

$H_{\mathrm{I}} = \{H_{PK}, H_d, H_{Replace.PK}, H_{SK}, H_{Signcrypt}, H_{Unsigncrypt}\}$ and $H_{\mathrm{II}} = \{H_{PK}, H_{SK}, H_{Signcrypt}, H_{Unsigncrypt}\}$, respectively.

We will prove this scheme from two aspects: confidentiality and unforgeability.

6.1 Confidentiality

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

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

- **Setup.** $\mathbb{C}$ enters a security parameter λ, a common parameter pp and α are generated, α is kept as secret.
- **Phase 1 Queries.** $\mathbb{A}_{\mathrm{I}}$ sends bounded queries in polynomial time to the oracles in the H_{I}, the $\mathbb{C}$ responses to these queries pass through these oracle models.
- **Challenge.** $\mathbb{A}_{\mathrm{I}}$ sends two equal length messages m_0 and m_1 to Challenger $\mathbb{C}$ with FID_A^* and FID_B^* as identifiers. $\mathbb{C}$ selects a bit $\gamma \in \{0,1\}$ randomly, implements $Signcrption(PP, M, FID_A^*, FID_B^*, SK_A^*, PK_B^*)$ then $\mathbb{C}$ sends δ to $\mathbb{A}_{\mathrm{I}}$.
- **Phase 2 Queries.**$\mathbb{A}_{\mathrm{I}}$ send bounded queries in polynomial time to the oracle H_{I}, the $\mathbb{C}$ responses to these queries pass through these oracle models.
- **Guess.** $\mathbb{A}_{\mathrm{I}}$ outputs a guess of γ is γ^*.

It is said that $\mathbb{A}_{\mathrm{I}}$ wins Game 1 if $\gamma^* = \gamma$ and the following conditions established:

a. $\mathbb{A}_{\mathrm{I}}$ can't extract SK_A^*, at any point.
b. $\mathbb{A}_{\mathrm{I}}$ can't extract S_A^*, if $\mathbb{A}_{\mathrm{I}}$ has replaced PK_A^* with PK'_A before accepting the challenge.
c. In Phase 2 queries,$\mathbb{A}_{\mathrm{I}}$ is unable to perform unsigncryption query on δ^* under FID_A^* or FID_B^*, used to signcryption M_γ, PK_A^* or PK_B^* has been replaced after the challenge was issued.

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

- **Setup.** $\mathbb{C}$ enters a security parameter λ, a common parameter pp and α are generated. $\mathbb{C}$ sends parameter pp and α to $\mathbb{A}_{\mathrm{II}}$.
- **Phase 1 Queries.** $\mathbb{A}_{\mathrm{II}}$ sends bounded queries in polynomial time to the oracles in the H_{II}, the $\mathbb{C}$ responses to these queries pass through these oracle models.
- **Challenge.** $\mathbb{A}_{\mathrm{II}}$ sends two equal length messages m_0 and m_1 to Challenger $\mathbb{C}$ with FID_A^* and FID_B^* as identifiers. $\mathbb{C}$ selects a bit $\gamma \in \{0,1\}$ randomly, implements $Signcrption(PP, M, FID_A^*, FID_B^*, SK_A^*, PK_B^*)$ then $\mathbb{C}$ sends δ to $\mathbb{A}_{\mathrm{II}}$.

- **Phase 2 Queries.** $\mathbb{A}_{\mathrm{II}}$ sends bounded queries in polynomial time to the oracle H_{II}, the $\mathbb{C}$ responses to these queries pass through these oracle models.
- **Guess.** $\mathbb{A}_{\mathrm{II}}$ outputs a guess γ^* of γ.

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

a. $\mathbb{A}_{\mathrm{II}}$ can't extract SK_A^* at any point. Because the secret value x_i can't be obtained by $\mathbb{A}_{\mathrm{II}}$, adversary solves x_i as ECDLP problem.
b. In Phase 2 queries, $\mathbb{A}_{\mathrm{II}}$ is unable to perform an unsigncryption query on δ^* under FID_A^* or FID_B^*.

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

$\mathbb{A}_{\mathrm{I}}$ sends bounded queries in polynomial time to the oracles in the H_{I} make a signcryption query $H_{Signcrypt}$ but cannot win δ under FID_A^* and FID_B^*. even if $\mathbb{A}_{\mathrm{I}}$ known key generation process $Q_A^* - R_A^* = u_A^* x_A^* P$, $Q_B^* - R_B^* = u_B^* x_B^* P$, $Y = u_B^* x_B^* u_A^* x_A^* P$. Solving Y is still difficult, it is the CDH problem.

$\mathbb{A}_{\mathrm{II}}$ sends bounded queries in polynomial time to the oracles in the H_{II} make an public-key query H_{PK}, but H_{II} cannot obtain x_i^*, thus cannot obtain PK_i. Solving x_i^* is ECDLP problem.

$Adv(\mathbb{A})$ the probability of winning game 1 and game 2 is negligible.

6.2 Unforgeability

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

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

- **Setup.** $\mathbb{C}$ enters a security parameter λ, a common parameter pp and α are generated, α is kept as secret.
- **Phase 1 Queries.** $\mathbb{A}_{\mathrm{I}}$ sends bounded queries in polynomial time to the oracles in the H_{I}, the $\mathbb{C}$ responses to these queries pass through these oracle models.
- **Forgery.** $\mathbb{A}_{\mathrm{I}}$ forges the message M^* and signcryption $\delta^* = (T^*, \tau^*, C^*)$ from the send V_A^* to the receiver V_B^*.

$\mathbb{A}_{\mathrm{I}}$ wins Game 3 if $Unsigncrption(PP, FID_A^*, FID_B^*, PK_A^*, SK_B^*, \delta)$ output M^* and the following conditions hold:

a. $\mathbb{A}_{\mathrm{I}}$ can't extract SK_A^* at any point.
b. $\mathbb{A}_{\mathrm{I}}$ can't extract SK_i^* for any pseudonym FID_i, if PK_i^* has been replaced.
c. $\mathbb{A}_{\mathrm{I}}$ cannot extract x_A^*.
d. $\mathbb{A}_{\mathrm{I}}$ can't make a signcryption query on M^* under FID_A^* and FID_B^*.

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

- **Setup.** $\mathbb{C}$ enters a security parameter λ, a common parameter pp and α are generated. $\mathbb{C}$ sends parameter pp and α to $\mathbb{A}_{\mathrm{II}}$.
- **Queries.** $\mathbb{A}_{\mathrm{II}}$ sends bounded queries in polynomial time to the oracles in the H_{II}, the $\mathbb{C}$ responses to these queries pass through these oracle models.
- **Forgery.** $\mathbb{A}_{\mathrm{II}}$ creates a forged message m^* or signcryption $\delta^* = (T^*, \tau^*, C^*)$ from the send V_A^* to the receiver V_B^*.

It is said that $\mathbb{A}_{\mathrm{II}}$ wins Game 4 if the output of $Unsigncrption(PP, FID_A^*, FID_B^*, PK_A^*, SK_B^*, \delta)$ is M^* and the following conditions hold:

a. $\mathbb{A}_{\mathrm{II}}$ can't extract SK_A^* at any point.
b. $\mathbb{A}_{\mathrm{II}}$ can't make a signcryption query on M^* under FID_A^* and FID_B^* .

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

$\mathbb{A}_{\mathrm{I}}$ executes public key replacement queries from $H_{Replace.PK}$, can replace the public key with $PK'_A = (R_A, Q'_A)$, $PK'_B = (R_B, Q'_B)$, signcryption queries from $H_{Signcrypt}$ and unsigncryption queries from $H_{Unsigncryption}$, $\mathbb{A}_{\mathrm{I}}$ random selects $t^* \in Z_q^*$, $x_A^* \in Z_q^*$, $x_B^* \in Z_q^*$ computes $T^* = t^*P = (T_x, T_y)$, $r^* = T_x \bmod q$, $v_A^* = H_3(FID_A^*, m, h_A^*, PK'_A, T)$, forged $Q'_A = x_A^*P - h_A^*P_{pub}$, $Q'_B = x_B^*P - h_B^*P_{pub}$; to signcrypt the message m^*. Then forged signcryption $\delta^* = (T^*, \tau^*, C^*)$, V_B receives δ^* and conducts feasibility verification:

$\tau^*T^* = t_A^{*-1}(v_A^* + r^*x_A^*)t_A^*P = (v_A^* + r^*x_A^*)P = v^*P + r^*(Q'_A + h_A^*P_{pub})$;

$Y' = u_A^*x_A^*(Q'_B - R_B) = u_Ax_A(x_B^*P - h_B^*P_{pub} - R_B)$;

$Y^* = u_B^*x_B^*(Q'_A - R_A) = u_Bx_B(x_A^*P - h_A^*P_{pub} - R_A)$;

Because $Y^* \neq Y'$; $w^* \neq w'$, so $m' = C^* \oplus w^* = m^* \oplus w \oplus w^* \neq m^*$. $\mathbb{A}_{\mathrm{I}}$ challenge failure.

$\mathbb{A}_{\mathrm{II}}$ cannot execute query partial-private key from H_d; thus, forged γ replace x_A^*, select $t' \in Z_q^*$, forged $\delta^* = (T^*, \tau^*, C^*)$; $T^* = t'P$; $\tau^* = t'^{-1}(v_A + r(S_A + u'_A\gamma)) \bmod q$; which $P'_A = \gamma P$; $u'_A = H_2(FID_A, P'_A)$; V_B get δ^* then feasibility verification.

$\tau^*T^* = (t'^{-1}(v + r(S_A + u'_A\gamma)))t'P \bmod q$;

$= (v' + r(r_A + h_As + u'_A\gamma))P$;

$= v'P + r(R_A + h_AP_{pub} + u'_AP_A)$;

for $\mathbb{A}_{\mathrm{II}}$ cannot replace any public keys, thus $Q_A \neq R_A + h_AP_A$; $\tau^*T^* \neq vP + r(Q_A + h_AP_{pub})$. We know if the equation does not hold, output INVALID, V_B discard ciphertext.

$Adv(\mathbb{A})$ the probability of winning game 3 and game 4 is negligible.

7 Performance evaluation

This section analyzes the present scheme from security, computational cost, and communication cost. It is compared with other relevant schemes [30–35].

Table 2 Run time of the different encryption operations.

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

These schemes selected for comparison are certificateless signcryption and can be applied to the IoV.

The computational cost mainly depends on the amount of computation of signcryption algorithm and verification calculation for decryption. It can be measured by 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 small, so that no comparison. The operation results are in table 2. The experimental system environment:CPU:

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

OS:Ubuntu16.04;

Library: MIRACL, a public C++cryptographic library;

[https://github.com/miracl/MIRACL/archive/master.zip].

Communication cost is measured by the length of a single ciphertext. In the bilinear pairing operation scheme, the length of $|G_1|$ is 1024 bits, the length of $|G_2|$ is the same as $|G_1|$. To provide the same level of security scheme, for the scheme based on the elliptic curve, q is the prime number, the length of $|Z_q^*|$ is 160 bits. The additive cyclic group with q order generation for point P on a nonsingular elliptic curve is G, the length of $|G|$ is 320 bits. Our scheme is designed according to the certificateless signcryption model, relies on ECDSA, and depends on the difficulty of pseudonym generation. This section will compare and analyze the security of the algorithm with similar schemes. The result is in table 3. The superiority of this scheme is illustrated by comparing the calculation cost and communication cost of a single ciphertext, which is statistically analyzed in table 4. Under the same operating environment, our scheme costs 1.397ms, Kasyoka et al's scheme[30] costs 1.705ms, Karati et al's scheme[31] based no pairing costs 2.424ms, Karati et al's scheme[32] based on bilinear pairing costs 18.913ms, He et al's[33] costs 2.05ms and Seo et al's[35] costs 3.41ms. Compared with the other schemes [30–33] and [35]. Our scheme in this paper increases by 18.06%, 42.37%, 92.61%, 31.85% and 59.03% respectively.

Table 3 safety comparison.

Scheme	Confidentiality	Unforgeability	Forward security	Anonymous
[30]	false	true	false	false
[31]	false	false	false	false
[32]	true	false	false	false
[33]	false	true	false	true
[34]	false	true	false	false
[35]	true	true	false	false
Our-CLSC	true	true	true	true

Table 4 performance comparison of different signcryption schemes.

Scheme	Calculate cost			Communication cost	
	Signcryption	Unsigncryption	Runtime	signcryptext	Length
[30]	$2T_{em}$	$3T_{em}$	1.705	$3\|Z_q^*\|$	480
[31]	$3T_{em} + 2T_{ea} + T_{in}$	$4T_{em} + 2T_{ea}$	2.424	$2\|Z_q^*\| + \|G\|$	640
[32]	$3T_e$	$2T_e + 2T_{bp}$	18.913	$4\|G_1\| + \|Z_q^*\|$	4256
[33]	$3T_{em}$	$3T_{em} + 2T_{ea}$	2.05	$3\|G\| + \|Z_q^*\|$	1120
[35]	$3T_{em}$	$7T_{em}$	3.41	$3\|Z_q^*\|$	480
Our-CLSC	$T_{in} + T_{em}$	$2T_{ea} + 3T_{em}$	1.397	$2\|Z_q^*\| + \|G\|$	640

In the comparative analysis of communication cost, the length of a single ciphertext is used as the unit of comparison. The length of the ciphertext in our scheme is 640bits, which is slightly higher than Kasyoka et al's[30] and Seo et al's[35], lower than Karati et al's bilinear pairing scheme[32] and He et al's[33], the same as no pairing scheme of Karati et al.[31].

8 Security analysis

8.1 Forward security

If the system master key s was leaked, it is calculated due to the difficulty of ECDLP, calculates r_i, x_i still difficult, (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, x_i. When the system master key is leaked, the new values will immediately replace for them. The key update is realized, these actions further confirm the security of the communication[29].

8.2 Traceability

The ciphertext should contain relevant information about the identity of the vehicle. In the scheme, the TA can calculate $RID_i = F_i \oplus H_0(sZ_i)$ by using the system master key s, which queries whether RID_i is in the vehicle identity list. It seems that only the trusted authority TA can track the vehicle according to this relevant information. In addition, the Internet of vehicles requires an extremely high real-time nature, and the ciphertext contains timestamp information, which can also prevent replay attacks. Because ciphertext

$C = M \oplus w$; $w = H_4(FID_A, FID_B, Y)$, here we can use the pseudonym of the vehicle $FID_i = (FID_{i1}, FID_{i2}, T_i)$ making the ciphertext contains timestamp information.

8.3 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 $FID_i = (FID_{i1}, FID_{i2}, T_i)$ where FID_{i1} is generated by the false identity F_i of the vehicle $FID_{i1} = F_i \oplus H_0(K_j \xi_i T_i)$, $F_i = RID_i \oplus H_0(z_i P_{pub})$, $FID_{i2} = P_j$, 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 and k_i in polynomial time, so he cannot obtain the RID_i of the vehicle. In addition, vehicles carry different pseudonyms in different RSU communication ranges and different timestamps, that is, the vehicle pseudonym information changes with position and time, which makes the generation process of a pseudonym is the trapdoor one-way function.

9 Conclusion

In this paper, we constructed a reliable certificateless signcryption scheme without bilinear, where a pseudonym mechanism was also designed to protect the privacy of vehicles. We use certificateless signcryption technology to implement the scheme, which can secure vehicular communications with a low computational overhead. Performance analysis demonstrates that our proposed scheme reduces computational cost and communication cost compared with other related schemes. Security proves and analysis shows that our proposed scheme can avoid replacement public-key attacks, satisfy the security of IND-CCA and EUF-CMA, and other security requirements including perfect forward secrecy, anonymity, traceability, and resistance of replay attacks.

Supplementary information. c If your article has accompanying supplementary file/s please state so here.

Authors reporting data from electrophoretic gels and blots should supply the full unprocessed scans for key as part of their Supplementary information. This may be requested by the editorial team/s if it is missing.

Please refer to Journal-level guidance for any specific requirements.

Declarations

- Authors' contributions. This paper is completed by all authors. Beibei.C. is responsible for proposing the idea of the paper, Beibei.C. checks whether the idea is feasible and gives some suggestions to improve this idea. Beibei.C.

is responsible for writing this paper, and the security analysis is completed by Beibei.C. Lu. Wei. is responsible for the performance analysis and comparison. Finally, the language of the paper is improved by Wei.H.

- Funding. In part by the funding project for top talent cultivation in Colleges and Universities of Anhui Province under Grant gxgnfx2020178, in part by the Natural Science Foundation of Anhui Province under Grant KJ2018A0944.
- acknowledgments. The authors thank the Associate Editor and the anonymous reviewers for their useful comments and suggestions which helped us improve the quality and presentation of this paper.
- Conflict of interest. The authors declare no conflict of interest.

If any of the sections are not relevant to your manuscript, please include the heading and write 'Not applicable' for that section.

References

[1] Cui J, Zhang X, Zhong H, et al. Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment [J]. IEEE Transactions on Information Forensics and Security, 2020, 15(1): 1654-1667.

[2] Song C, Zhang M Y, Peng W P, et al. Research on anonymous authentication scheme in VANET[J]. Journal of Chinese Computer Systems,2018, 39(5): 899-903.

[3] Kamat P, Baliga A, Trappe W. An identity-based security framework For VANETs[C]// International Workshop on Vehicular Ad Hoc Networks. ACM, 2006.

[4] A.Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in Proceedings of CRYPTO 84 on Advances in cryptology 1985.

[5] Zhang J, Cui J, Zhong H, et al. PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-preserving Authentication Scheme in Vehicular Ad-hoc Networks[J]. IEEE Transactions on Dependable and Secure Computing, 2019:1-1.

[6] Raya M, Hubaux J P. Securing vehicular ad hoc networks [J]. Journal of Computer Security, 2007, 15(1): 39-68.

[7] Tzeng S F, Horng S J, Li T, et al. Enhancing security and privacy for identity-based batch verification scheme in VANETs[J]. IEEE Transactions on Vehicular Technology, 2017, 66(4): 3235-3248.

[8] Al-Riyami S, Paterson K G. Certificateless public key cryptography [C] //International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2003: 452-473.

[9] Liu J K, Au M H, Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model [C]//Proceedings of the 2nd ACM symposium on Information, computer and communications security. Springer, Berlin, Heidelberg, 2007: 273-283.

[10] Shim K A. A new certificateless signature scheme provably secure in the standard model[J].IEEE Systems Journal, 2018, 13(2): 1421-1430.

[11] Yang W, Wang S, Wu W, et al. Top-Level secure certificateless signature against malicious-but-passive KGC[J]. IEEE Access, 2019, 7: 112870-112878.

[12] Thumbur G, Rao G S, Reddy P V, et al. Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices[J]. IEEE Communications Letters, 2020, 24(8): 1641-1645.

[13] Mei Q,Xiong Hu, Chen J H, et al. Efficient certificateless aggregate signature with conditional privacy preservation in IoV[J]. IEEE System Journal, 2020: 1-12.

[14] Ali I, Lawrence T, Li F G. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs[J]. Journal of Systems Architecture, 2020, 103: 101692-101705.

[15] Barbosa M, Farshim P. Certificateless signcryption. In ACM Symposium on Information, Computer and Communications Security-ASIACCS 2008: 369-372.

[16] Zheng Y. Digital signcryption or how to achieve cost(signature & encryption)¡¡cost (signature)+cost (encryption)[C]//Annual international cryptology conference. Springer, Berlin, Heidelberg, 1997: 165-179.

[17] Cui J, Wei L, Zhong H, et al. Edge Computing in VANETs-An Efficient and Privacy-Preserving Cooperative Downloading Scheme[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(6):1191-1204.

[18] Barreto P, Deusajute A, Cruz E, et al. Toward efficient certiicateless signcryption from (and without) bilinear pairings [EB/OL].(2008)

[19] Suzhen CAO,Xiaoli LANG, Xiangzhen LIU, et al. New Heterogeneous Signcryption Scheme under 5G Network[J].Netinfo Security, 2018, 18(11): 33-39.

[20] Li FG, Masaaki S, Tsuyoshi T. Certificateless hybrid signcryption. Mathematical and Computer Modelling 2013, 57(3-4):324–343. [doi: 10.1016/j.mcm.2012.06.011]

[21] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3): 452-464.

[22] Zhou C, Zhou W, Dong X. Provable certificateless generalized signcryption scheme [J]. Designs, Codes and cryptography, 2014, 71(2):331-346.

[23] Luo M, Tu M, Xu J. A security communication model based on certificateless online/offline signcryption for Internet of Things. Security & Communication Networks, 2013,7(10):1560–1569.

[24] Yu HF, Yang B. Provably secure certificateless hybrid signcryption. Chinese Journal of Computers, 2015, 38(4):804–813 (in Chinese with English abstract).

[25] Du H, Wen Q, Zhang S, et al. A new provably secure certificateless signature for Internet of Things[J]. Ad Hoc Networks, 2020, 100: 102074-102084.

[26] Wei L, Cui J, Zhong H, et al. Proven Secure Tree-based Authenticated Key Agreement for Securing V2V and V2I Communications in VANETs[J]. IEEE Transactions on Mobile Computing, 2021, PP(99):1-1.

[27] J Zhang, Zhong H, J Cui, et al. SMAKA: Secure Many-to-Many Authentication and Key Agreement Scheme for Vehicular Networks[J]. IEEE Transactions on Information Forensics and Security, 2020, PP(99):1-1.

[28] Parvin R, Willy S, Mohammad D. Efficient Certificateless Signcryption in the Standard Model: Revisiting Luo and Wan's Scheme from Wireless Personal Communications (2018)[J]. The Computer Journal, 2019(8):8.

[29] Wei L, Cui J, Xu Y, et al. Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs[J]. IEEE Transactions on Information Forensics and Security, 2020, PP(99):1-1.

[30] Kasyoka P, Kimwele M, Angolo S M. Cryptanalysis of a pairing-free certificateless signcryption scheme[J], ICT Express 7, 2021, 200-204.

[31] Karati A, Fan C I, Huang J J. An efficient pairing-free certificateless signcryption without secure channel communication during secret key issuance[J]. Procedia Computer Science, 2020, 171: 110-119.

[32] Karati A, Fan C I, Hsu R, et al. Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices[J]. IEEE Internet of Things Journal: 2019, 6(6): 10431-10440.

[33] He D, Zeadally S, Xu B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[34] Jia X, He D, Liu Q, et al. An Efficient Provably-Secure Certificateless Signature Scheme for Internet-of-Things Deployment[J]. Ad Hoc Networks, 2018, 71(MAR.):78-87.

[35] Seo S H, Won J, Bertino E. pCLSC-TKEM: a Pairing-free Certificateless Signcryption-tag Key Encapsulation Mechanism for a Privacy-Preserving IoT[J]. Transactions on Data Privacy, 2016, 9(2): 101-130.