Journal of Computers Vol. 33 No. 2, April 2022, pp. 177-188
doi: 10.53106/199115992022043302016

Conditional Privacy Protection Scheme based on Blockchain and Ring Signcryption in VANETs

Nan Cui[*], Haibing Mu

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, 100044, China
{20120031, hbmu}@bjtu.edu.cn

Received: 7 January 2022; Revised: 1 March 2022; Accepted: 3 March 2022

Abstract. As the infrastructure of intelligent transportation systems, Vehicular Ad hoc Networks (VANETs) improve the efficiency of transportation. Meanwhile, key management and privacy leakage of users in VANETs are two vital security aspects. It is extremely important to perform these actions promptly and efficiently. Based on the idea of batch authentication and ring signcryption, a conditional privacy protection scheme of anonymous multi-receiver is proposed in this paper. On the one hand, the scheme with ring list selection has an optional privacy level. On the other hand, the blockchain prevents the single point of failure problem in key management and shares the public keys of vehicles promptly in Road Side Units (RSUs). Finally, experiments show that the proposed scheme has higher efficiency with certain security as the security analysis shows.

Keywords: ring signcryption, key management, privacy protection, Vehicular Ad hoc Networks (VANETs)

1 Introduction

VANET (Vehicular Ad hoc Network) is a promising vehicular communication infrastructure. In a typical scenario of VANETs, each vehicle broadcasts traffic-related information, such as its speed, position, and road condition. To ensure that the VANETs can provide safe services, traditional security technologies have been widely studied and applied in security protection, such as identity authentication of vehicles, access control and privacy protection. In the safety message broadcast by the vehicle, the traffic-related information is directly exposed. So, if the vehicle is not processed and protected, the attacker is likely to infer the identity, behavior pattern, health status, home address, and other private information of the vehicle user based on the monitored message, which is unacceptable [1-3].

To tackle privacy during the communication in VANETs, there are existing kinds of proposals such as pseudonyms-based approaches [4, 5], group signature-based approaches [6, 7], and ring signature-based approaches [8]. Compared to pseudonym-based approaches, ring signature-based approaches have a higher level of privacy. Compared to group signature-based approaches, ring signature-based approaches have equality of members. Ring signature-based schemes for VANETs need not keep the trusted third party online all the time, which is more flexible in practice. Moreover, due to the time-sensitive and frequent dynamic topology of VANETs, the ring signature-based approach is a suitable way whose generation does not require setup messaging. However, ring signature-based approaches relies on trusted third authority, which usually has the problem of centralization of key management. The centralized management mode has great risks. E.g., the failure of the centralized authority may result in the loss of all vehicles' key; attacks on the centralized trusted authority may result in keys being tampered with. Based on this, there is an urgent need for a secure distributed key management method.

Blockchain [9] is a synchronized and distributed ledger that stores a list of blocks. Central managers are removed from the blockchain structure, and the public ledger is maintained by all the network participants instead. Messages are broadcast to authenticate nodes in the network. With the help of this simplified structure, information propagation among security domains can be accelerated since the information is directly sent to the destination rather than passing the messages through central managers. Moreover, the distributed structure of the blockchain network performs better robustness under the single point of failure. Therefore, it is suitable to provide a distributed key management method by using the features of blockchain technology.

Based on the above analysis, we present a conditional privacy protection scheme of anonymous multi-receiver for VANETs based on blockchain. The main contributions of this work are listed as follows. Firstly, we propose anonymous multi-receiver ring signcryption based on the idea of batch authentication. The optional ring membership on RSUs provides the enhanced privacy protection. Secondly, the blockchain-based key management

[*] Corresponding Author

technology solves the single point of failure and enables RSUs to reach consensus to quickly obtain the public keys for vehicles. The RSUs construct the ring list by sharing the public key stored in the blockchain, which ensures the security of the public key and improves fairness. Thirdly, we construct a conditional privacy protection scheme for blockchain-based VANETs based on ring signcryption. And the scheme has the properties of unforgeability, anonymity, traceability, and confidentiality.

The remainder of this paper is organized as follows. Section 2 introduces the related work. Section 3 presents the system model in detail and gives the implementation process of the scheme. In Section 4, the security of the scheme is analyzed. The performance analysis is shown in Section 5. The last section concludes this paper.

2 Related Work

In the simple process of vehicle communication, the identity information and location information of vehicles are easily obtained by malicious attackers. Many privacy-preserving schemes with ring signature have been proposed to address such issues. Mundheet al. [10] applied a lattice-based ring signature to address message authentication in VANETs. However, its solution lacks conditional privacy because it cannot track malicious vehicles. Hence, to make the honest users unconditionally untraceable while enabling the trusted authority to uncover the misbehaving or malicious users in the VANETs, a lot of research schemes have been proposed. Zeng et al. [11] proposed an anonymous ring signature scheme, which does not depend on any fully trusted authority during the tracing phase. Cui et al. [12] gave a solution that satisfies the traceability, but the length of the signature is related to the number of ring members. Liu et al. [13] proposed a hybrid scheme, which employs ring signatures in VANETs with batch verification mode to audit ring members efficiently. However, messages were not protected in this scheme.

Ring signcryption combines ring signature and encryption with low compution and communication costs. More importantly, ring signcryption realizes the confidentiality and message authentication at the same time and realizes the full anonymity of the signcrypter. Cai et al. [14] proposed a novel conditional privacy protection scheme based on ring signcryption, which utilizes the salient features of identity-based cryptosystems and ring signature to achieve conditional privacy. However, it only supports one-to-one communication. Lai et al. [15] proposed a scheme based on certificateless ring signcryption technique, which can achieve anonymous authentication and secure communication. In addition, the scheme can provide tracking function of the suspicious vehicle when disputes occur.

In addition, to ensure the legitimacy and confidentiality of vehicles in the privacy protection schemes, key management is indispensable. To optimize the efficiency of a centralized key management scheme, blockchain is introduced into VANETs to store and distribute keys. The blockchain-based scheme has tamper-proof and distributed characteristics, which can ensure the integrity and authenticity of the keys. Lasla et al. [16] proposed a lightweight blockchain-based authentication approach to replace certificate authentication, using blockchain technology to track each vehicle's certificate (valid or revoked) in a distributed immutable ledger. Ao et al. [17] gave a secure identity authentication scheme based on blockchain and identity-based cryptography, which avoids complex certificate management and has low system complexity. Table 1 summarizes the existing surveys on privacy protection in VANET and discusses the enhancements in our paper. The circles in Table 1 indicate the direction of focus in the existing surveys.

Table 1. Existing surveys on privacy protection in VANET

Paper	Confidentiality	Key generation security	One-to-many communication	Conditional Privacy Protection	Optional privacy protection
[10]	○		○		
[11]			○	○	
[12]			○	○	
[13]			○	○	○
[14]	○			○	
[15]	○			○	
[16]		○	○		
[17]		○	○		
[18]	○		○		
This paper	○	○	○	○	○

Aiming at the problems above, a privacy protection scheme of vehicles for VANETs based on blockchain is proposed. Batch authentication is used in the anonymous multi-receiver ring signcryption algorithm, which reduces the computing and communication costs. The conditional privacy protection scheme of anonymous multi-receiver can protect the receiver's privacy and prevent the sender's deceptive behavior by having the fairness of decryption, in response to the problems of receiver's identity leakage and unfairness of decryption. The multi-receiver signing scheme can securely send the same message to multiple receivers with only one signing operation, which is more effective and practical than the traditional one-to-one approach [18]. It can also simplify key management and ease the traffic pressure on VANETs, distributed generation and storage of keys with blockchain are used to solve the problem of single point failure and update the ring list of RSUs quickly and efficiently.

3 The Proposed Scheme

There are three entities in our proposed scheme: 1) TRC; 2) RSUs; and 3) On board Units (OBUs). The system model is illustrated in Fig. 1.

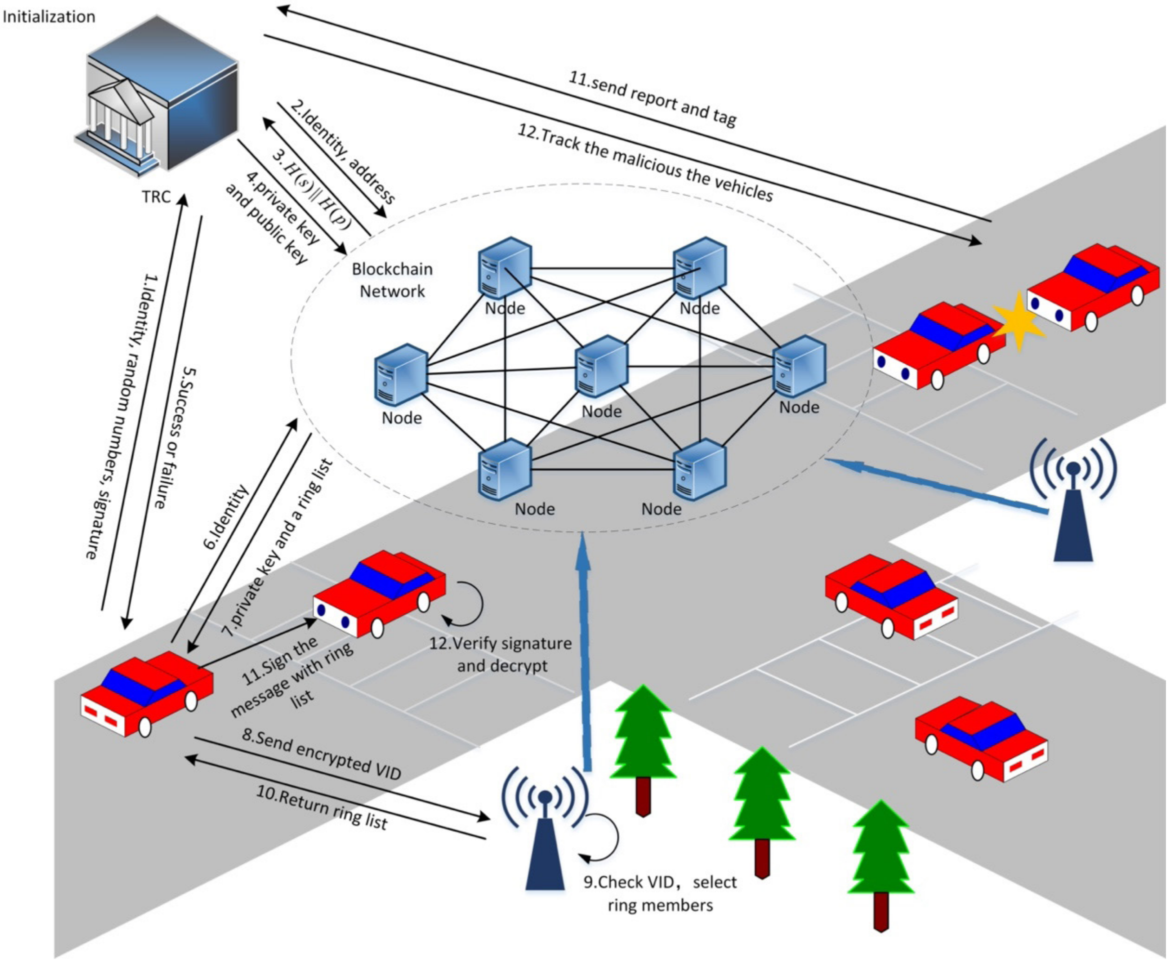
Initialization
TRC
11.send report and tag
12.Track the malicious the vehicles
2.Identity, address
3.$H(s)||H(p)$
4.private key and public key
1.Identity, random numbers, signature
5.Success or failure
Blockchain Network
Node
Node
Node
Node
Node
Node
Node
6.Identity
7.private key and a ring list
11.Sign the message with ring list
12.Verify signature and decrypt
8.Send encrypted VID
10.Return ring list
9.Check VID， select ring members

Fig. 1. Our proposed scheme

TRC： TRC is completely credible and responsible for the registration of all communication entities, including RSUs and vehicles. In addition, it generates the public key for vehicles for an ID-base cryptosystem.

RSUs： The blockchain network is a P2P network built by all RSUs deployed in the same vehicle management area. In the blockchain network, for RSUs that need pre-deploying, TRC first generates public-private key pairs for them, the public keys of RSUs are added to the blockchain and the private keys are secretly stored locally in RSUs. The smart contract is used to realize the automated registration of vehicle private keys and the effective and secure sharing of vehicle public keys. Moreover, the smart contract mainly includes three storage functions and three query functions.

The first storage function is used to store the master key's hash and the system parameters' hash, the second storage function is used to store the private key for vehicles, and the third storage function is used to store the public key of vehicles. The first query function is used for RSUs to obtain the master key's hash and the system parameters' hash, the second query function is used for the vehicles to obtain the private key, and the third query function is used for the RSUs to obtain a ring list of vehicles.

OBUs： Each vehicle is assumed to be equipped with a powerful OBU that is a tamper-proof device (TPD). An OBU can transmit essential messages to RSUs and other vehicles'OBUs as well as verify received messages. The vehicles are in a distributed operation, corresponding to the completely distributed characteristics of blockchain, and the blockchain network is constructed by RSUs.

We divide the whole process into seven phases: initialization, key generation, ring list selection, signcryption, verify, decrypt and trace. After the initialization of TRC server, each vehicle is assumed to get the public key from the TRC server, obtain the private key and an initial ring list from the blockchain. Once a vehicle enters a certain region, it obtains a new ring list from the local RSUs. Then the vehicle can sign messages by identity-based ring signcryption from the ring list. Other vehicles can verify and decrypt locally by using the public parameters preloaded in OBUs. Relevant notations are listed in Table 2.

Table 2. Explanation of notations

Notations	Explanation
$s,H(s)$	The secret key of TRC server and its hash.
$params,H(p)$	public parameters and its hash.
VID_s	Public key of vehicle s.
VSK_s	Private key of vehicle s.
RID_j	Public key of RSU j.
RSK_j	Private key of RSU j.
$K_{s\text{-}j}$	A shared secret key between vehicle s and RSU j.
L	The set of legitimate vehicles on the RSUs.
n_1	The number of vehicles in the ring.
k	The overlapped set size under attacks, where $2 \leq k \leq n1$.
m	The number of vehicles in L.
$Enc_{K_{s-j}}(\cdot)$	A symmetric encryption algorithm.
$Dec_{K_{s-j}}(\cdot)$	The timestamp for signcryption.
T_b	The traceable tag fosigncryption.
tag	A symmetric hash-based message authentication code.
$HMAC_{K_{j-i}}(\cdot)$	The set of legitimate vehicles after ring selection.
$L^{'}$	The receivers of ring signcryption.

Based on the system model of Fig. 1 and the implementation process of the above scheme, we give a sequence diagram of the whole scheme as shown in Fig. 2.

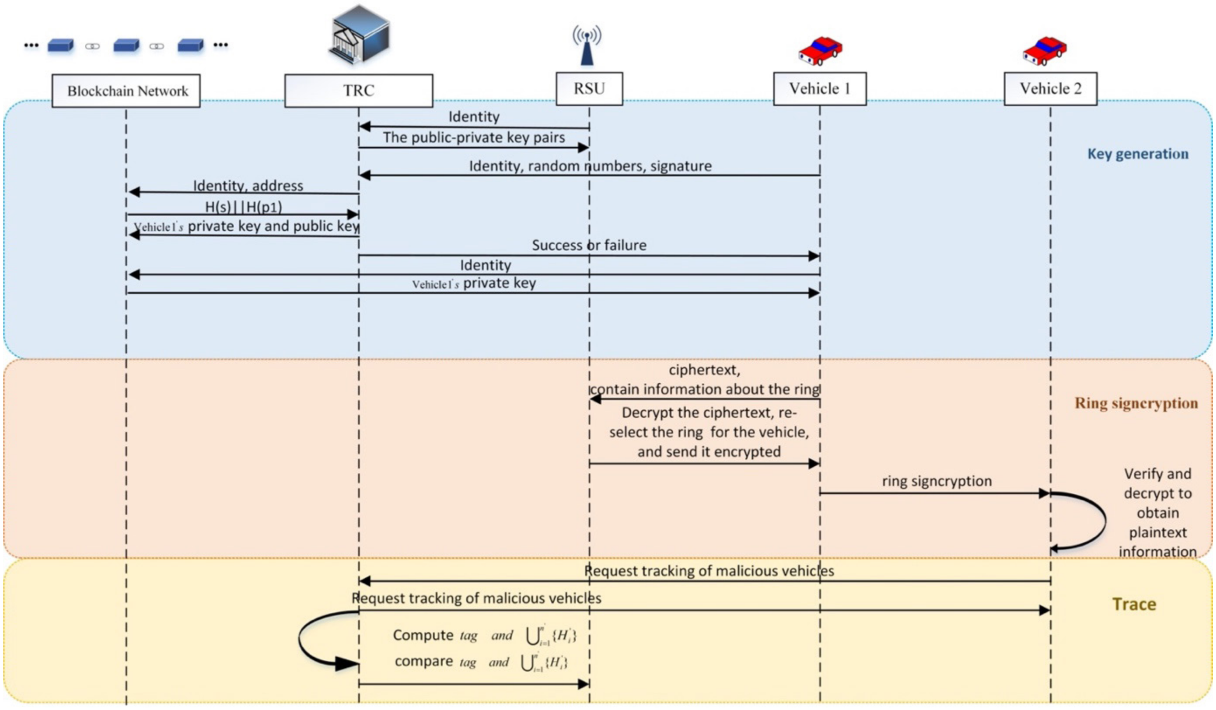
Blockchain Network
TRC
RSU
Vehicle 1
Vehicle 2
Identity
The public-private key pairs
Identity, random numbers, signature
Identity, address
H(s)||H(p1)
Vehicle1's private key and public key
Success or failure
Identity
Vehicle1's private key
Key generation
ciphertext,
contain information about the ring
Decrypt the ciphertext, re-select the ring for the vehicle, and send it encrypted
ring signcryption
Verify and decrypt to obtain plaintext information
Ring signcryption
Request tracking of malicious vehicles
Request tracking of malicious vehicles
Compute tag and $\bigcup_{i=1}^{n'}\{H_i'\}$
compare tag and $\bigcup_{i=1}^{n'}\{H_i'\}$
Trace

Fig. 2. Scheme sequence diagram of privacy protection

3.1 Initialization

In the beginning, the TRC server selects the master secret key $s \in_R \mathbb{Z}_q^*$ randomly. Let G_1, G_2, be two cyclic groups of the same prime order q. Pairing operation $e(P, Q)$,where $P, Q \in G_1$, $\hat{e}: G_1 \times G_1 \rightarrow G_2$. And $PK_1 = s \cdot P$, $PK_2 = s \cdot Q$, randomly select $P_0 \in G_1$, calculate $g{=}\hat{e}(PK_1, P_0)$. H_1, H_2, H_3, H_4 and H are five cryptographic hash function where H_1:$\{0,1\}^* \rightarrow G_1$, H_2:$\{0,1\}^* \rightarrow G_2$, H_3:$G_2 \rightarrow \{0, 1\}^\lambda$, H_4: $\{0,1\}^\lambda \times G_1 \rightarrow \mathbb{Z}_q^*$, H: $\{0,1\}^* \rightarrow \mathbb{Z}_q^*$, and outputs params as $P = < G_1, G_2, P, Q, PK_1, PK_2, q, \hat{e}, H_1, H_2, H_3, H_4, H>$, writes the results as $H(s)$ and $H(p)$, interacts $H(s)$ and $H(p)$ with smart contract and stores on the blockchain.

3.2 Key Generation

There are two types of packets generated by the vehicles, which are initiation packets (IAP) and ring list update request packets (RURP).

IAP is a type of packet sent from a vehicle to the TRC server. IAP contains the public key of a vehicle, a random number R_{ex} which is generated by the vehicle, signature Sn_{ex} which is signed with the private key of its Ethereum account and PK_{eth} (public key of its Ethereum account), whose purpose is to get the vehicle's private key and a ring list.

RURP is a type of packet sent from a vehicle to the RSU. RURP contains the identity of the vehicle, the number of vehicles in the ring n_1, the overlapped set size under attacks k and the set of legitimate vehicles in the ring L, whose purpose is to get a new ring list L'.

The vehicles respectively authenticate their identity to the TRC server and obtain their private key.

1) The Ethereum blockchain is jointly maintained by all RSUs. Our proposed scheme implements decentralized key generation and ring list selection through the deployment of smart contracts on Ethereum blockchain. The RSUs are completely credible. For RSU j, identity is ID_j, public key is $RID_j = H_2(ID_j)$, private key is $RSK_j = s \cdot RID_j$.

2) The real identity of the vehicle s is ID_s and the public key $VID_s = H_1(ID_s)$ is calculated and published. Then the vehicle s sends the $IAP = (VID_s, R_{ex}, Sn_{ex}, PK_{eth})$ to the TRC server.

3) The TRC server decrypts Sn_{ex} with PK_{eth} to get R'_{ex}, compares Rex and $R'ex$. If they are equal, the TRC server gets the Ethereum account address Ad_s through PK_{eth}. If not, the TRC server sends an error message to the vehicle s.

4) The TRC server interacts with the smart contract to check whether the identity ID_s or Ethereum account address Ad_s is registered. If registered, the TRC server returns a rejected message to the vehicle s. If unregistered, the TRC server interacts with the smart contract again to obtain $H(s)$ and $H(p)$, computes the hash of s and *params* stored by itself (If they are different, the TRC server issues a warning message. If they are the same, the TRC server calculates $VSK_s = s \cdot VID_s$ (VSK_s is the private key of the vehicle s). Finally, the TRC server sends an extract-succeed message to the vehicle s , and interacts with smart contract and stores VSK_s and VID_s on the blockchain.

5) After receiving success message, the vehicle s interacts with the smart contract and sends ID_s to the smart contract. The smart contract determines whether the vehicle s is the owner of ID_s by the Ethereum account address calling the contract. After the verification is successful, the smart contract returns the private key to the vehicle s.

3. 3 Ring Selection

When vehicle s receives RID_j which is broadcasted by RSU j, it will request the ring list L from RSU j by sending its encrypted public key VID_s. After that, the RSU will select ring members, and then return a new ring list $L^{'}$ for the valid vehicle s.

1) The vehicle s chooses $r \in_R Z_q^*$ randomly and computes $g = \hat{e}\ (PK_1, RID_j)$. Then, sends its ciphertext $C = (rP, VID_s \oplus H(g^r))$to RSU j.

2) The RSU j receives the ciphertext C and computes $VID_s = VID_s \oplus H(g^r) \oplus H(\hat{e}(rP, RSK_j))$. Then, it saves the VID_s to the ring member list L_{RSU_j} , and computes a shared secret key $K_{j\text{-}s} = \hat{e}(VID_s, RSK_j)$.

3) The vehicle s computes a shared secret key $K_{s\text{-}j} = \hat{e}(\ VSK_s, RID_j)$ and ciphertext $C' = Enc_{K_{s-j}}(RURP)$. Then, it sends C' to RSU j.

4) The RSU j recovers $RURP = (n_1 \| k \| L)$.

a) Check the number of vehicles m in L_{RSU_j}.

b) Determine the ring size n, where $n < m$;

c) Keep k ring members including himself/herself in the ring L, and discard the left $n_1 - k$ ring members of L. Note that these $n_1 - k$ ring members cannot be used in ring $L^{'}$;

d) Select $n - k$ new ring members from the ring L, together with the remained k members chosen from ring L to form the new ring $L^{'}$;

Then, it computes ciphertext $C^* = Enc_{K_{j-s}}(n \| L^{'})$, $\Sigma = HMAC_{K_{j-s}}(C^* \| t_d)$, and finally sends $(C^*, \sum, t_d)$ to the vehicle.

5) After the vehicle s receives the ciphertext C^*, it checks the message authentication code Σ and recovers n || $L^{'} = Dec_{K_{s-j}}(C^*)$.

3.4 Signcrypt

For a vehicle s holding a ring list $L^{'}$ with an unexpired t_d, it could use ring signcryption to communicate with other vehicles. The vehicle s is the real sender. $L^* = \{ID_1^*, ID_2^*, \cdots, ID_p^*\}$ is the vehicle s's choice of p recipients.

1) Choose $ui \in Z_q^*$ randomly, $i \in \{1, 2, ..., n\} \backslash \{\mathrm{s}\}$. And compute $R_i = u_i P$, choose $u_s \in Z_q^*$ randomly. Choose $\alpha_i \in Z_q^*$ randomly, $i \in \{1, 2, ..., n\}$, and compute $\alpha = \sum_{i=1}^{n} \alpha_j$, $U = \alpha P$, $\sigma = g^\alpha$, $W = H_3(\sigma) \oplus M$.

2) Compute $h_i = H_4(W, R_i) + H(tag \| T_b)$, $i \in \{1, 2, ..., n\} \backslash \{s\}$. Let $R_s = u_s VID_s - \sum_{i=1, i \neq s}^{n} (R_i + h_i VID_i)$, $R = \{R_1, R_2, ..., R_n)$ .Compute $tag = e(H_1(ID_s \| T_b), PK_1)$, $V = (u_s + h_s) \cdot VSK_s$, $h_s = H_4\ (W, R_s) + H\ (tag \| T_b)$.

3) $x_j = H(ID_j')$, $y_j = \alpha(P_0 + VID_j')$, $j = 1, 2, ..., p$. Get n pairs of numbers (x_1, y_1), (x_2, y_2),..., (x_n, y_n), and construct a Lagrangian Function $F_j(x)$ such that x_j is a solution to $F_j(x) = y_j$.

4) For $j \in \{1, 2, ..., p\}$, compute $f_j(x) = \prod_{1 \le j \neq j' \le p} \frac{x - x_j'}{x_j - x_j'} = a_{j,1} + a_{j,2}x + \cdots + a_{j,p}x^{p-1}$, among them $a_{j,1}$, $a_{j,2}$, ..., $a_{j,p}$

ϵZ_q. Compute $T_j = \sum_{j'=1}^{p} a_{j',j} y_{j'}$, $J'_j = \sum_{j'=1}^{p} a_{j',j} J_{j'}$, among them $J_j = \alpha\alpha_j^{-1} PK_1$. Let $T = \{T_1, T_2, ..., T_n\}$, $J = \{J'_1, J'_2, \cdots, J'_n\}$. Finally, add the timestamp T_b for the message.

5) The ciphertext is $C' = <U, V, W, T, R, L', J, T_b, tag>$.

3.5 Verify

Upon received C', the receiver first checks the timestamp T_b to determine whether the message is still valid. Our proposed scheme supports single verification and batch verification.

Single verification:

1) Compute $K = \sum_{i=1}^{n}(R_i + h_i VID_i),\ h_i = H_4(W, R_i) + H(tag \parallel T_b),\ i \in \{1,2,\cdots,n\}.$.

2) Judge $e(V, Q) = e(K, PK_2)$

Batch verification:

1) Given η messages and corresponding ciphertexts. Compute $V' = \sum_{i=1}^{\eta} V_i$, $K' = \sum_{i=1}^{\eta} \sum_{j=1}(R_{ij} + h_{ij} VID_{ij})$.

2) Judge $e(V', Q) = e(K', PK_2)$

3.6 Decrypt

After the message is verified, the receiver can decrypt the message by computing.

1) Compute $\delta_j = T_1 + x_j T_2 + \cdots + (x_j^{n-1} \bmod q) T_n,\ v_j = J'_1 + x_j J'_2 + \cdots + (x_j^{n-1} \bmod q) J'_n$,

2) Compute $\sigma' = \frac{e(v_j, \delta_j)}{e(U, d'_j)}$, $M = H_3(\sigma') \oplus W$. M is the decrypted message.

3.7 Trace

Within the jurisdiction of TRC, when the vehicle s finds a disputed message, it will report to TRC. Then, it calculates $tag' = tag^{1/s}$, $H'_i = e(H_i(ID_i \parallel t), P)$, $\forall i \in \{1, 2, ... n'\}$. By comparing tag' and $\cup_{i=1}^{n'}\{H'_i\}$, the TRC server will find out the signer's true identity ID.

4 Security Analysis

4.1 Correctness

$$K_{s-j} = \hat{e}(VSK_s, RID_j) = e\hat{}(VID_s, RID_j)^s = \hat{e}(VID_s, RSK_j) = K_{s-j} \tag{1}$$

$$\begin{aligned} \delta_j = T_1 + x_j T_2 + \cdots + x_j^{n-1} T_n = \left(a_{1,1}\alpha_1(P_0 + Q'_1) + \cdots + a_{n,1}\alpha_n(P_0 + Q'_n)\right) + \left(x_j a_{1,2}\alpha_1(P_0 + \right. \\ \left. Q'_1) + \cdots + x_j a_{n,2}\alpha_n(P_0 + Q'_n)\right) + \cdots + \left(x_j^{j-1} a_{1,j}\alpha_1(P_0 + Q'_1) + \cdots + x_j^{j-1} a_{n,j}\alpha_n(P_0 + Q'_n)\right) + \\ \cdots \left(x_j^{n-1} a_{1,n}\alpha_1(P_0 + Q'_1) + \cdots + x_j^{n-1} a_{n,n}\alpha_n(P_0 + Q'_n)\right) = (a_{1,1} + a_{1,2}x_j + \cdots + a_{1,n}x_j^{n-1})\alpha_1(P_0 + Q'_1) + \\ (a_{2,1} + a_{2,2}x_j + \cdots + a_{2,n}x_j^{n-1})\alpha_2(P_0 + Q'_2) + \cdots + (a_{j,1} + a_{j,2}x_j + \cdots + a_{j,n}x_j^{n-1})\alpha_j(P_0 + Q'_j) + \cdots + \\ (a_{n,1} + a_{n,2}x_j + \cdots + a_{n,n}x_j^{n-1})\alpha_n(P_0 + Q'_n) = \alpha_j(P_0 + Q'_j) \end{aligned} \tag{2}$$

$$\begin{aligned} v_j = J_1' + x_j J_2' + \cdots + x_j^{n-1} J_j' + \cdots + x_j^{n-1} J_n' = \left(a_{1,1}J_1 + \cdots + a_{n,1}J_n\right) + \left(x_j a_{1,2}J_1 + \cdots + \right. \\ \left. x_j a_{n,2}J_n\right) + \cdots + \left(x_j^{j-1} a_{1,j}J_1 + \cdots + x_j^{j-1} a_{n,j}J_n\right) + \cdots \left(x_j^{n-1} a_{1,n}J_1 + \cdots + x_j^{n-1} a_{n,n}J_n\right) == \\ \left(a_{1,1} + a_{1,2}x_j + \cdots + a_{1,n}x_j^{n-1}\right)J_1 + \left(a_{2,1} + a_{2,2}x_j + \cdots + a_{2,n}x_j^{n-1}\right)J_2 + \cdots + \left(a_{j,1} + a_{j,2}x_j + \cdots + \right. \\ \left. a_{j,n}x_j^{n-1}\right)J_j + \cdots + \left(a_{n,1} + a_{n,2}x_j + \cdots + a_{n,n}x_j^{n-1}\right)J_n = J_j \end{aligned} \quad \textbf{(3)}$$

$$\sigma' = \frac{e(v_j,\delta_j)}{e(U,d_j')} = \frac{e(J_j,\alpha_j(P_0+Q_j'))}{e(\alpha P,sQ_j')} = \frac{e(\alpha\alpha_j^{-1},\alpha_j(P_0+Q_j'))}{e(\alpha P,sQ_j')} = \frac{e(PK_1,\alpha P_0)\cdot e(PK_1,\alpha Q_j')}{e(sP,\alpha Q_j')} = e(PK_1,P_0)^{\alpha} = g^{\alpha} = \sigma \quad \textbf{(4)}$$

As result, $K_{s\text{-}j} = K_{s\text{-}j}$ and $M = H_3(\sigma') \oplus W = H_3(\sigma') \oplus H3(\sigma) \oplus M = M$. Thus, it can be verified that M is indeed the message sent by the vehicle s .

4.2 Unforgeability

If an attacker wants to forge a message transmitted by another vehicle that is used to encrypt the ring signcryption, the attacker needs to obtain the real private key of that vehicle. However, obtaining the private keys of other vehicles from $V = (u_s + h_s)$. VSK_s is an elliptic curve discrete logarithm problem.

4.3 Anonymity

When a vehicle in a ring list sends a message through ring signcryption to another vehicle, the message receiver cannot determine the real identity of the message signer, so the anonymity of the message sender is kept. From the ciphertext perspective, any member of the ring is indistinguishable from each other and can act as a signer on behalf of all members of the ring. Even if the worst case is that the private keys of all members of the ring are compromised, the probability of an attacker guessing the right signer from the ring is no more than $1/n$, and if the attackers come from inside the ring, the probability of successful guessing is no more than $1/\ (n-1)$, so this scheme satisfies unconditional anonymity.

4.4 Against Replay Attack

Since in our scheme, each message contains a timestamp. Once the vehicles discover that the message is out of date, the message will be discarded before being verified. Unless an attacker can tamper with the content of a message and forge a valid signature, an opponent will not be able to perform a replay attack. Based on the above analysis, it is almost impossible for an attacker to carry out a replay attack.

4.5 Confidentiality

Messages transmitted between vehicles are confidential, and attackers cannot determine the real content of messages during transmission. This is because in the process of message transmissions σ, W, and other security factors required to encrypt the message are randomly selected. Hence the attacker cannot obtain the transmitted messages from the W, which is the Elliptic Curve Discrete Logarithm Problem.

4.6 Traceability

When the recipient verifies that a message cannot be successfully recovered, or finds the message in dispute, the disputed report and *tag* will be sent to the authority TRC. When the TRC server receives the disputed message reports for a message sender *IDs*, it will compare tag' and $\cup_{i=1}^{n'}\{H_i'\}$. If a solution i is found, then the TRC server successfully uncovers that the identity of the disputed sender (a potential malicious attacker) is $s = i$, and hence it publishes i on the revocation list and punishes it with certain measures.

5 Performance Analysis

To show the performance advantages of this protocol, the JPBC (Java Pairing-Based Cryptography Library) is used in the actual environment of Intel I7, 64 GB memory using Java language implementation. In this paper, we compare the computation cost and communication cost respectively.

5.1 Computation Cost

Using a comparative approach, the computational overhead of the scheme in this paper are compared with those of [11], and [14]. All three schemes are ring signature schemes based on the bilinear pairing, which are more comparable. We evaluate the computation cost for vehicle-to-message signcryption, and at the same time evaluate the computation overhead for the vehicle after receiving the signcrypted message and verifying it. When the vehicle receives the message, it needs to verify the message. Assuming that the size of the ring in the three schemes is certain, compare the variation of the verification time with the number of messages. When the ring size is 5, with the increase of messages, the change of the validation time of the four schemes is shown in Fig. 3. Fig. 3 shows that with the increase of the number of signcryptions, the calculated amount of the scheme in [11] varies most, the calculated amount of our scheme and the scheme in [14] is nearly equal, while our scheme in batch mode is the least.

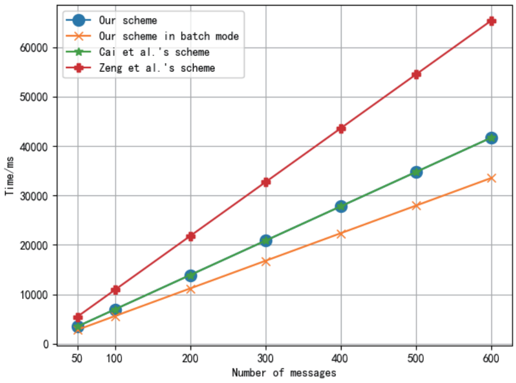

Fig. 3. The computation cost of verification with respect to messages

When a vehicle receives a message for verification, the computation time for verification is related to the size of the ring in the ring signature and the number of messages. Fig. 4 compares the variation of the time for the vehicle to verify a message with the size of the ring in the ring signature for the three schemes when the number of messages is certain. Because of the wide distribution and large number of vehicles in practical use, this paper sets the number of ring numbers from $n = 4$ to $n = 12$, calculates the operation time of different schemes under different number of ring members, and the experimental results are shown in Fig. 4. Fig. 4 shows that with the increase of the number of vehicles, the calculated amount of the scheme in [11] varies most, the calculated amount of the scheme in [14] varies is moderate, the calculated amount of the scheme in this paper is lower than the scheme in [11] and [14], while the calculated cost of the scheme in this paper with ring selection is the least.

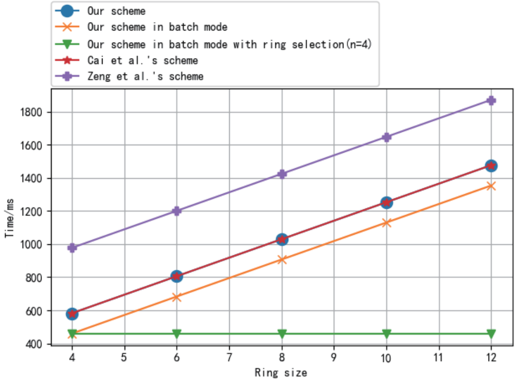

Fig. 4. The computation cost of verification with respect to ring size

In addition to the computation cost of authentication time, the computation cost of encryption time is equally important. As the number of recipients increases, the change of signature time of the three schemes is shown in Fig. 5. In the scheme [11, 14], the number of signcryptions is equal to the number of recipients. While in our scheme, the number of recipients is much more than the number of signcryptions. That is because our scheme is based on anonymous multi-receiver and can send messages to multiple recipients only by constructing ciphertext once. The time of our proposed scheme is minimal.

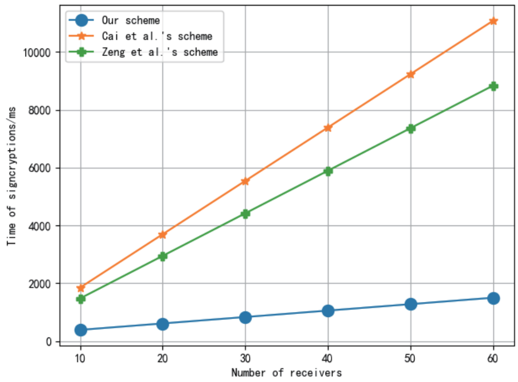

Fig. 5. The computation cost of signcryption with respect to recipients

It is widely assumed [11, 14], that OBUs have limited computation capacity. However, Fig. 3 shows the computation cost of the ring signcryption depends on the number of ring members. We argue that privacy level can be changed with ring selection in our scheme, ring size 5 can achieve a certain level of privacy protection. Based on the benchmark, the number of receivers is 10, and the computation cost for each RSU and OBU is shown in Fig. 6.

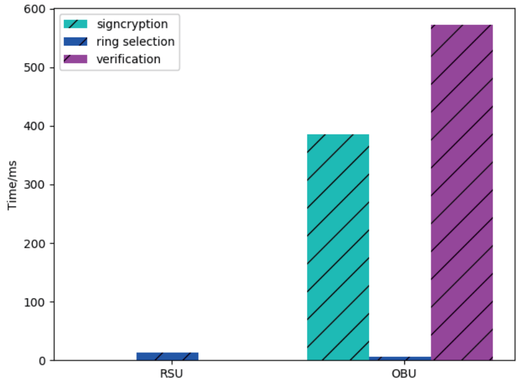

Fig. 6. The computation cost for each RSU and OBU

5.2 Communication Cost

In the proposed scheme, the communication cost is determined by the size of the ciphertext length, which is mainly due to batch verification and unsigncryption. For our proposed scheme, we use a bilinear pairing ê: G1 × G1 → G2 to achieve the security level of 80 bits. Then let the sizes of the general hash function's output and timestamp be 20 bytes and 4 bytes, let the sizes of the user's identity, the length of the elements in the Z_q^* and the message be 20 bytes, 20bytes and 30bytes.

The communication cost of the three schemes is shown in Fig. 7. As the number of ring size and recipients increases greatly, the communication overhead of [10, 16] increases greatly, this paper's scheme grows slowly, indicating multi-receiver signcryption can safely send the same message to multiple receivers through a single signcryption operation, which is more efficient and practical than the traditional one-to-one mode. In the case of many vehicles, the communication cost in [10, 16] is huge, and that in this paper is much smaller than the above two schemes. In short, this scheme is suitable for VANETs.

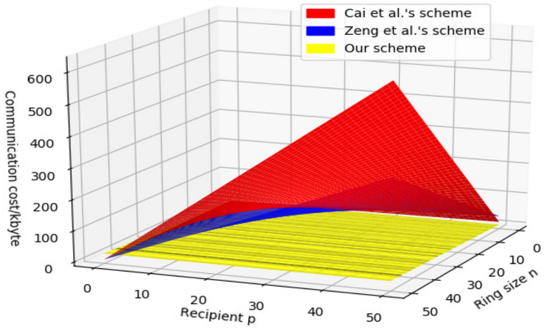

Fig. 7. Comparison of communication cost

6 Conclusion

From the methodological viewpoint, we proposed a new conditional privacy protection scheme of anonymous multi-receiver based on blockchain and ring signcryption. The scheme is suitable for scenarios where a single vehicle communicates anonymously to multiple vehicles. When an anonymous vehicle sends a signcrypted message, multiple anonymous recipients can receive the signcryption, enabling one-to-many communication. At the same time, the scheme supports conditional privacy protection, which protects the real identity information of the vehicle during communication and allows TRC to trace the real identity information of the vehicles under certain circumstances. Moreover, the scheme has an optional privacy level to protect the location and identity privacy of vehicles efficiently. And the scheme utilizes the blockchain to solve the single point failure and shares the public key of vehicles promptly, which contributes to the formation of the ring list. In the future, our work will focus on system efficiency and autonomous tracking of trusted vehicles.

Acknowledgement

The authors may express their acknowledgement and the financial support project number here.

References

[1] X. Kong, F. Xia, Z. Ning, A. Rahim, Y. Cai, Z. Gao, J. Ma, Mobility Dataset Generation for Vehicular Social Networks Based on Floating Car Data, IEEE Transactions on Vehicular Technology 67(5)(2018) 3874-3886.

[2] X. Liu, H. Huang, F. Xiao, Z. Ma, A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs, IEEE Internet of Things Journal 7(5)(2020) 4101-4112.

[3] L. Zhang, Q. Wu, J, Domingo-Ferrer, B, Qin, C. Hu, Distributed Aggregate Privacy-Preserving Authentication in VANETs, IEEE Transactions on Intelligent Transportation Systems 18(3)(2017) 516-526.

[4] A. Boualouache, S.M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks, IEEE Communications Surveys & Tutorials 20(1)(2018) 770-790.

[5] J. Yang, J. Deng, T. Xiang, B. Tang, A Chebyshev Polynomial-Based Conditional Privacy-Preserving Authentication and Group-Key Agreement Scheme for VANET, Nonlinear Dynamics 106(3)(2021) 2655-2666.

[6] S.K.H. Islam, M.S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, M.K.C. Reddy, A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs, Future Generation Computer Systems 84(2018) 216-227.

[7] J. Zhang, J. Cui, H. Zhong, Z. Chen, 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 18(2)(2021) 722-735.

[8] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang, H. Zhang, Lattice-Based Double-Authentication-Preventing Ring Signature for Security and Privacy in Vehicular Ad-Hoc Networks, Tsinghua Science and Technology 24(5)(2019) 575-584.

[9] V.K. M., R. Koduri, S. Nandyala, M. Manalikandy, Secure Vehicular Communication Using Blockchain Technology, WCX SAE World Congress Experience, AE Technical Paper 2020-01-0722, 2020.

[10]P. Mundhe, V.K. Yadav, S. Verma, S. Venkatesan, Efficient Lattice-Based Ring Signature for Message Authentication in VANETs, IEEE Systems Journal 14(4)(2020) 5463-5474.

[11]S.K. Zeng, Y. Huang, X.W. Liu, Privacy-preserving Communication for VANETs with Conditionally Anonymous Ring Signature, International Journal of Network Security 17(2)(2015) 135-141.

[12]Y. Cui, L. Cao, X. Zhang, G. Zeng, Ring Signature Based on Lattice and VANET Privacy Preservation, Chinese Journal of Computation 42(5)(2019) 980-992.

[13]F. Liu, Q. Wang, IBRS: An Efficient Identity-based Batch Verification Scheme for VANETs Based on Ring Signature, in: Proc. 2019 IEEE Vehicular Networking Conference (VNC), 2019.

[14]Y. Cai, H. Zhang, Y. Fang, A Conditional Privacy Protection Scheme Based on Ring Signcryption for Vehicular Ad Hoc Networks, IEEE Internet of Things Journal 8(1)(2021) 647-656.

[15]C. Lai, G. Li, D. Zheng, SPSC: A secure and privacy-preserving autonomous platoon setup and communication scheme, Transactions on Emerging Telecommunications Technologies 32(9)(2020) e3982.

[16]N. Lasla, M. Younis, W. Znaidi, D.B. Arbia, Efficient Distributed Admission and Revocation Using Blockchain for Cooperative ITS, in: Proc. IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2018.

[17]W. Ao, S. Fu, C. Zhang, Y. Huang, F. Xia, A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography, in: Proc. 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET) IEEE, 2019.

[18]Y. Ming, X. Yu, X. Shen, Efficient Anonymous Certificate-Based Multi-Message and Multi-Receiver Signcryption Scheme for Healthcare Internet of Things, IEEE Access 8(2020) 153561-153576.