Certificateless Aggregate Signature Scheme with Conditional Privacy Protection in Vehicle Networking

Xiaohui Ding¹, Suzhen Cao¹*, Fengge Dou¹, Jiajia Ma¹ and Caifen Wang²

¹College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China
²Big Data and Internet College, Shenzhen University of Technology, Shenzhen 518118, China
Email: 2405968216@qq.com; 576342353@qq.com

Abstract. Real-time road navigation information update in vehicle networking plays an extremely important role in safe driving and alleviating traffic congestion, but how to protect user privacy from leakage is a major challenge when updating real-time navigation information. In order to solve this problem effectively, a certificateless aggregate signature scheme with real-time navigation information update function is proposed, which is suitable for vehicle networking. In the scheme, when the navigation company needs to access the data, the fog node aggregates the signature message of the vehicle broadcast and uploads it to the trusted center, and then feeds it back to the navigation company after batch verification by the trusted center. The trusted center generates temporary pseudonyms for vehicle users, realizes the anonymity of user identity, and meets the requirements of conditional privacy protection. The aggregate signature technology is used to reduce the computing and communication overhead. Finally, based on the discrete logarithm difficulty problem in the elliptic curve, it is proved that the scheme satisfies the existence and cannot be forged under the adaptive selection message attack. The results of numerical analysis show that the scheme has some advantages in terms of computational cost.

Keywords. Navigation information update; certificateless cryptosystem; aggregate signature; no bilinear pair; conditional privacy protection.

1. Introduction

With the rapid development of sensor technology and artificial intelligence technology, traditional cars have been combined with information technology to derive a more safe and intelligent driving environment-vehicle networking (Internet of vehicles, VANETs [1]). VANETs is an important part of smart city, which provides data support for the update of real-time road navigation information. Effective navigation information can help drivers make choices more timely and accurately, thus reducing the incidence of traffic accidents, It plays a very important role in alleviating traffic congestion, safe driving and so on [2].

In order to update the real-time road navigation information and obtain the traffic status of the corresponding road section timely and effectively, some schemes [3-4] have been proposed in recent years, in which vehicle users agree to upload their collected road condition information to the navigation company, but this also increases the risk of user privacy disclosure. In the efficient identity-based conditional privacy protection authentication in vehicle networking scheme proposed in reference [5], the privacy protection is realized by generating pseudonyms for vehicle users, which solves the risk of
privacy disclosure of vehicle users' identity. In the process of registration, the trusted center (Trusted-Authority, TA) generates pseudonyms for vehicle users. Vehicle users can use pseudonyms to communicate with each other to protect their privacy, but when they break the law, TA can restore their true identity through their pseudonyms and achieve conditional privacy protection.

In addition, if the authenticity of the information in the vehicle networking environment cannot be guaranteed, it will lead to serious communication security problems. VANETs often use message signature technology to realize the legitimacy and authenticity of messages. At the same time, in order to reduce the communication overhead in VANETs, some scholars have proposed an aggregate signature scheme [6]. Aggregate signature technology can compress the signature messages of multiple users into a signature message for processing, so as to improve the authentication efficiency of messages, which is very suitable for VANETs communication environment. In reference [7], an aggregate signature scheme based on PKI is proposed, but the management and maintenance of certificates will cause great overhead, so it is not suitable for VANETs. Based on elliptic curve cryptosystem and general one-way hash function, an effective identity-based conditional privacy protection authentication scheme in VANETs is proposed in reference [8]. Although it solves the problem of certificate management, it has the problem of key escrow. A malicious key generation center can easily impersonate a user to sign, which brings a serious security threat to the system. Using certificateless cryptosystem to construct signature scheme [9-10] can solve the problem of key escrow. A certificate-free aggregate signature scheme in VANETs is proposed in references [11-14]. The key generation center only generates part of the user's private key, and the user randomly selects a secret value and part of the private key to form his own complete private key to ensure the security of the signature. However, the scheme proposed in reference [14] involves bilinear pairing operation, which not only increases the difficulty of calculation, but also brings great communication burden to the VANETs communication environment. In order to solve this problem, references [15-16] proposed a certificateless aggregate signature scheme without bilinear pairs for VANETs communication environment, and constructed a lighter aggregate signature scheme based on elliptic curve discrete logarithm problem, which greatly improved the computational efficiency. Unfortunately, the scheme proposed in reference [16] cannot resist class $A_{II}$ adversary attacks.

Based on the above situation, this paper proposes a secure and effective aggregate signature scheme based on certificateless cryptosystem. The main work is as follows:

- Certificateless cryptosystem can effectively solve not only the problem of certificate management in PKI cryptosystem, but also the problem of key escrow in identity-based cryptosystem. Therefore, based on the certificateless cryptosystem, this paper proposes a secure and efficient real-time road navigation information update scheme suitable for VANETs environment, which can not only ensure security, but also effectively reduce the communication burden of VANETs environment.
- The conditional privacy protection of vehicle user information is realized by generating temporary pseudonyms for vehicle users. Users do not have to worry about divulging their privacy in the process of communication. When users have illegal activities, TA can restore the true identity of users through pseudonyms and track them.
- An efficient and secure aggregate signature scheme is constructed based on the elliptic curve discrete logarithm difficulty problem. The scheme does not involve bilinear pairing operation in the construction process, so it has the advantage of lightweight, and is more suitable for the computing needs of fast response and low delay in VANETs. It can greatly shorten the signature time of the client, reduce the computational overhead and improve the application efficiency.
- The scheme of this paper realizes the confidentiality, integrity, reliability, identity authentication and non-repudiation of data, and gives strict security proof. The experimental numerical analysis shows that the scheme has obvious efficiency advantages.
2. Preliminary Knowledge

2.1. Elliptic Curve
Let the set of all points and an infinity point $O$ on equation $y^2 = x^3 + ax + b \mod p$ be called an elliptic curve $E_p(a,b)$. Where $a,b,x,y$ is all on $E_p(a,b)$ and $p$ is a large prime. Under a given operation, all the points in the set can form an Abel group, denoted as $G$, and the algorithm is as follows:

- Suppose $p$ is a point on $E_p(a,b)$, and the point of infinity is $O$, then $p + O = p$;
- Suppose $p$ is a point on $E_p(a,b)$ and its additive inverse is $Q = -p$, then $Q + p = O$;
- Double point operation: $np = p + p + \ldots + p$, where $n \in Z_q^*$.

2.2. Difficult Problems
Elliptic curve discrete logarithm problem (ECDLP): Suppose $G$ is an additive cyclic group, $P$ is the generator of the group $G$, and the order of $G$ is $q$, $Q \in G_p$. Given $P$ and $Q$, it is difficult to find the integer $a$ that satisfies $ap = Q$.

3. System Model of Scheme
In the scheme of safe and efficient road condition navigation information update system in this paper, the navigation company sends the road condition information task that needs to be collected to TA, after receiving the task, TA will send the information to the vehicle users in the range through the fog node. The vehicle users in the range will collect the corresponding information according to the task after receiving the task, and then send the corresponding information to the fog node after the collection is completed. After receiving the signature message from the vehicle user, the fog node will authenticate the legality of the signature message, and after verifying the legality, it will aggregate the signature message and send it to the trustworthy center TA. After receiving the message, TA will authenticate the signed message in batches, and if the message is legal, it will return the message to the navigation company, otherwise it will be discarded and the corresponding illegal users will be investigated. The system model, shown in figure 1, consists of five entities:

- Navigation company: the navigation company needs a lot of real-time information to update the navigation information dynamically, but the navigation company itself does not have this ability, so it sends the corresponding tasks to the trusted center TA, and then updates the corresponding navigation information according to the information fed back by TA.
- Trusted center TA: trusted center TA is considered to be completely credible and is generally served by government agencies. In the scheme of this paper, TA is mainly responsible for the registration of vehicles and fog nodes. At the same time, in order to protect the privacy of vehicles, false identities will be generated for vehicles in the process of registration, but when a vehicle violates the law, TA can also obtain his real identity from his false identity and investigate his corresponding responsibility. In addition, the trusted center will authenticate the aggregate signature messages sent by the fog node in batches, and send them to the navigation company after the authentication is passed.
- Key Generation Center (KGC): KGC is considered to be semi-trusted and is mainly responsible for system parameter establishment and key generation. When it receives the vehicle pseudo-identity information sent by the trusted center, it will execute the key generation algorithm to generate a part of the private key for the vehicle user.
- Fog nodes: fog nodes are generally distributed on both sides of the road, which are used to broadcast task information issued by TA and collect messages signed by vehicle users. Fog nodes are registered in TA. After collecting the signature message of the vehicle in the range, it will first verify the validity of the message, if the legitimate fog node will aggregate it, and send the aggregated message to the trusted center TA.
Vehicle user: after receiving the task of the fog node broadcast, the vehicle user will sign the collected real-time road condition information and send it to the fog node in the range.

Figure 1. system model diagram.

4. Description of the Scheme

- System establishment algorithm: Key generation center KGC establishes an elliptic curve $E_p(a,b) : y^2 = x^3 + ax + b \mod p$. Where $p$ is a big prime, $a,b \in F_p$. A point $P$ on the elliptic curve is selected as the generator of the group $G$, and the order of $G$ is $q$. Set $s \in Z_q^*$ is the master key of the system, then the master public key is $P_k = s \cdot p$. Five secure hash functions $h_1,h_2,h_3,h_4,h_5 : \{0,1\}^* \rightarrow Z_q^*$ are selected as the hash function of the system. Select the current time $t_i$ and use the calculated value of the function $f(t_i)$ as the current timestamp. Finally, KGC exposes the system parameter: $\text{paras} = \{E_p(a,b),G,p,q,P_k,h_1,h_2,h_3,h_4,h_5,f(t_i)\}$.

- Fog node registration phase: The fog node executes the algorithm to complete the registration. The fog node selects its own secret value $R_i \in Z_q^*$ and calculates its public key $P_{kr} = R_i \cdot p$. And broadcast its public key, then send its own public key and identity information $ID_R$ to TA through a secure channel.

- Vehicle registration stage: The vehicle needs to be registered at the trusted center. In order to achieve conditional privacy protection, TA will generate a false identity for the vehicle. When the vehicle uses the false identity for communication, it will not disclose its real identity information, but when the vehicle has illegal behavior, TA can restore its true identity through its false identity and investigate the corresponding responsibility of the vehicle. Let the real identity of the vehicle be $ID_v$, select the current time as $t_i$, and use the function $f(t_i)$ to calculate the current timestamp. TA generates
a false identity $VID_i = h_i(ID_i, f(t_i))$ for it. TA saves $(ID_i, f(t_i), VID_i)$ and then sends $VID_i$ to KGC to generate part of the private key.

- Partial private key generation algorithm: The key generation center executes the algorithm to generate a partial private key for the vehicle user. The key generation center KGC inputs the system parameter $paras$, the system master key $s$, and the false identity $VID_i$ of the vehicle. Then randomly select $a_i \in Z_q^+$, and calculate $A_i = a_i \cdot p$, $h_{n_i} = h_2 (A_i || P_k || f(t_i))$, $SV_i = a_i + h_{n_i} \cdot s \mod q$. And send $(A_i, SV_i)$ to $VID_i$ as part of its private key.

- User private key generation algorithm: Vehicle users randomly select $b, r_1, r_2 \in Z_q^+$, Select the current time as $t_i$ and use the function $f(t_i)$ to calculate the current timestamp. Calculate $SK_{n_1} = h_2(r_1 || f(t_i) || P_k)$, and $SK_{n_2} = h_2(r_2 || f(t_i) || P_k)$ means the user's private key is $SK_i = b(SK_{n_1} + SK_{n_2})$. The public key is $PK_i = SK_i \cdot p$. The user saves his private key and makes the public key.

- Kana generation algorithm: In order to ensure the timeliness of the scheme, TA executes this algorithm to generate temporary pseudonyms for the vehicle. Messages signed with this pseudonym are considered valid only within the appropriate time frame. When the vehicle leaves the appropriate section of the road or exceeds the corresponding time range, the temporary pseudonym will be revoked. TA selects the current time as $t_i$ and uses the function $f(t_i)$ to calculate the current timestamp. Calculate $ID_i = VID_i \oplus h_i(PK_k || PK_i || f(t_i))$. The temporary pseudonym of the vehicle is $F_i = (ID_i, f(t_i))$.

- Task distribution: The navigation company sends the road sections that need to collect information to the trusted center, and the trusted center sends the corresponding tasks to the fog nodes of the corresponding road sections, and the fog nodes will broadcast the tasks after receiving the tasks. Vehicles that meet the task requirements will sign the corresponding information and send it to the fog node, and the fog node will aggregate the signed messages after authentication and send them to the trust center.

- Data collection and upload:

  (1) Signature algorithm: The vehicle user executes the signature algorithm to sign the message $m_i$ collected by himself. The user randomly selects $c_i \in Z_q^+$, $C_i = c_i \cdot p$. Calculate $h_i = h_2(m_i, F_i, PK_i, A_i, C_i)$, $h_j = h_3(m_j, A_j, F_j, PK_j, C_j)$, $Q_i = c_i + h_j SK_i + h_j SV_i \mod q$. Then the sign is $\sigma_i = (C_i, Q_i)$, and broadcast the signature and message $m_i$.

  (2) Fog node aggregation signature phase: After receiving the signature messages from $n$ vehicle users, the fog node will first verify whether each vehicle user's signature message is legal, for legal signature messages the fog node will aggregate them, for illegal signature messages, the fog node will discard them and report them to TA for illegal tracking. First of all, the fog node calculates the $h_i = h_2(m_i, F_i, PK_i, A_i, C_i)$, $h_j = h_3(m_j, A_j, F_j, C_j, PK_j)$, $h_{n_i} = h_2(A_i || P_k || f(t_i))$ for each single message. Verify that equation $Q_i P = C_i + h_i \cdot A_i + h_j \cdot h_{n_i} \cdot P_k + h_j \cdot PK_i$ is valid, and if so, accept the signed message, otherwise it will be discarded. The $n$ signature messages $\{(m_i, \sigma_i = (C_i, Q_i)) | i = 1, \ldots, n\}$ with successful verification are aggregated. Calculate $Q = \sum_{i=1}^{n} Q_i$, output the aggregate signature $\sigma = (C_i, Q, Q)$, and send the aggregated signature message to the trusted center for verification.

  (3) Trusted center batch authentication phase: After receiving the aggregate signature, the trusted center carries out batch verification through the following equation. If
$$QP = \sum_{i=1}^{n} C_j + \sum_{i=1}^{n} h_i \cdot A_i + (\sum_{i=1}^{n} h_i \cdot h_{n_i}) \cdot P_k + \sum_{i=1}^{n} h_j \cdot PK_i$$

is valid, it accepts the message and feeds it back to the navigation company. Otherwise, the message is discarded and the illegal users are tracked down.

Navigation information update: after receiving the message sent by the trusted center, the navigation company will update the navigation information of the corresponding road section in time, which can greatly alleviate the traffic pressure and reduce the incidence of accidents.

5. Safety Analysis

5.1. Correctness Analysis

Verify the correctness of a single signature:

Verify that equation $Q \cdot p = C_j + h_h \cdot A_i + h_i \cdot h_{n_i} \cdot P_k + h_j \cdot PK_i$ is correct.

Similarly, the correctness of the aggregate signature can be obtained by verifying the following equations:

$$Qp = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n} h_i \cdot A_i + (\sum_{i=1}^{n} h_i \cdot h_{n_i}) \cdot P_k + \sum_{i=1}^{n} h_j \cdot PK_i$$

5.2. Security Proof

The aggregate signature scheme in this paper is based on the certificateless cryptosystem. According to the security model proposed in reference [17], the security of this scheme considers two different adversaries, the first common adversary $A_I$ and the second super adversary $A_{II}$.

Theorem 1: In the random prediction model, if there is an ordinary adversary $A_I$ who can win the game with a non-negligible probability $\epsilon$ in polynomial time, then there must be a challenger who can solve the ECDLP problem with the following advantages:

$$\epsilon^* \geq (1 - \frac{q_{h_3}}{q})^n(1 - \frac{1}{q_{cu}})^n(q_{h_4} - \frac{q_{h_5}}{q}) \epsilon$$

where $q_{h_3}, q_{h_4}, q_{h_5}$ represents the corresponding number of hash prediction machine queries, $q_{cu}$ represents the number of user prediction machine queries, and $q_k$ represents the number of partial private key queries of the user.

Proof: Assuming that an ordinary adversary $A_I$ can win the game with the non-negligible advantage $\epsilon$, that is, successfully forge the valid signature of the target user $VID_i$, then we think that the challenger $C$ who interacts with it can successfully solve the ECDLP problem. $C$ and $A_I$ interact with each other according to the following steps.

- Initialization phase: Challenger $executes$ the algorithm to build the system, and makes $Q = P_k$, challenger disclose the system parameters, and establish and maintain the following four lists: $L_1$ list $(VID, A, P_k, T_h)$, $L_2$ list $(VID, PK_i, T_{h_i})$, $L_3$ list $(VID, m, F_i, SK_i, A)$, $L_4$ list $(VID, m, F_i, SK_i, A, T_{h_i}, T_{h_i}, C, Q)$. 

Proof complete!
• Prophecy machine query phase: in this stage, the first type of ordinary adversary and the challenger carry on the prophecy machine interaction.
  • \( h_{i} \) Prophecy machine query: The ordinary adversary \( A_{i} \) asks with \( VID \), and if \( VID \) already exists in the \( L_{1} \) list, \( T_{h_{i}} \) is returned to the adversary \( A_{i} \). If it does not exist, the challenger performs a partial private key prediction machine query, select \( a \in Z_{q}^{*} \) at random, calculate \( A = a \cdot p \), \( T_{h_{i}} = h_{2}(A \parallel P_{K} \parallel f(t_{i})) \), and return \( T_{h_{i}} \) to adversary \( A_{i} \).
  • \( h_{i} \) Prophecy machine query: The ordinary adversary \( A_{i} \) asks with \( VID \), and if \( VID \) already exists in the \( L_{2} \) list, \( T_{h_{i}} \) is returned to the adversary \( A_{i} \). If it does not exist, the challenger performs a partial private key prediction machine query, Select \( b, r_{1}, r_{2} \in Z_{q}^{*} \) at random, calculate \( SK_{1} = h_{3}(r_{1} \parallel f(t_{i}) \parallel P_{K}) \), \( SK_{2} = h_{3}(r_{2} \parallel f(t_{i}) \parallel P_{K}) \), \( SK = b(SK_{1} + SK_{2}) \), \( T_{h_{i}} = SK \cdot p \), and return \( T_{h_{i}} \) to adversary \( A_{i} \).
  • \( h_{i} \) Prophecy machine query: The ordinary adversary \( A_{i} \) asks with \( VID \), and if \( VID \) already exists in the \( L_{3} \) list, \( T_{h_{i}} \) is returned to the adversary \( A_{i} \). If it does not exist, the challenger performs the user secret value prediction machine query and part of the private key prediction machine query. Select \( c \in Z_{q}^{*} \) at random, calculate \( C = c \cdot p \), \( T_{h_{i}} = h_{4}(m, F, PK, A, C) \), and return \( T_{h_{i}} \) to adversary \( A_{i} \).
  • \( h_{i} \) Prophecy machine query: The ordinary adversary \( A_{i} \) asks with \( VID \), and if \( VID \) already exists in the \( L_{4} \) list, \( T_{h_{i}} \) is returned to the adversary \( A_{i} \). If it does not exist, the challenger performs the user secret value prediction machine query and part of the private key prediction machine query. calculate \( T_{h_{i}} = h_{4}(m, F, PK, A, C) \), and return \( T_{h_{i}} \) to adversary \( A_{i} \).
  • User creates prophecy machine query: The opponent \( A_{j} \) queries the challenger with \( VID \), and the challenger queries the \( L_{5} \) list. If the tuple does not exist in the list, do the following: When \( VID = VID_{m} \), the challenger randomly selects \( a \), \( T_{h_{i}} \in Z_{q}^{*} \), and calculates \( A = a \cdot p \), selects \( b, r_{1}, r_{2} \in Z_{q}^{*} \), calculates \( SK_{1} = h_{3}(r_{1} \parallel f(t_{i}) \parallel P_{K}) \), \( SK_{2} = h_{3}(r_{2} \parallel f(t_{i}) \parallel P_{K}) \), \( SK = b(SK_{1} + SK_{2}) \), \( PK = SK \cdot p \), \( SV \perp \). When \( VID \neq VID_{m} \), the challenger randomly selects \( SV, SK, a, T_{h_{i}} \in Z_{q}^{*} \), and calculates \( A = a \cdot p \), \( A = SK \cdot p - T_{h_{i}} \cdot Q \). Then add it to the appropriate list. If there is a corresponding tuple, the challenger queries the \( L_{5} \) list, if there is a corresponding \( (VID, A, T_{h_{i}}) \), verify whether it satisfies \( h_{2}(A, Q) \rightarrow T_{h_{i}} \), if not, the challenger ends the game, otherwise returns user information.
  • User secret value prediction machine query: the ordinary adversary \( A_{i} \) queries with \( VID \), the challenger queries the \( L_{5} \) list, and returns \( PK, SK \) to the adversary \( A_{i} \) if the corresponding tuple already exists in the \( L_{5} \) list. If it does not exist, the challenger randomly selects \( b, r_{1}, r_{2} \in Z_{q}^{*} \), calculates \( SK_{1} = h_{3}(r_{1} \parallel f(t_{i}) \parallel P_{K}) \), \( SK_{2} = h_{3}(r_{2} \parallel f(t_{i}) \parallel P_{K}) \), \( SK = b(SK_{1} + SK_{2}) \), and returns \( PK, SK \) to the opponent.
  • Partial private key prediction machine query: In a valid polynomial time, Challenger performs a maximum of \( q_{0} \) partial private key queries. The opponent asks with \( VID \), and when \( VID = VID_{m} \), the challenger outputs \( \perp \) and terminates the game. When \( VID \neq VID_{m} \), the challenger queries the \( L_{5} \) list. If the corresponding tuple already exists in the \( L_{5} \) list, the challenger returns \( (A, SV) \) to \( A_{i} \). If there is no corresponding tuple, the challenger randomly selects \( a \), \( SV \in Z_{q}^{*} \), and calculates \( A = a \cdot p \). Then return \( (A, SV) \) to \( A_{i} \).
  • Public key prediction machine query: The opponent queries with \( VID \), and the challenger queries
the $L_3$ list. If the corresponding tuple already exists in the $L_3$ list, the challenger returns $(A, PK)$ to $A_i$.

- Signature prophecy machine query: When the challenger asks with $(m_i, A_i, F_i, \text{VID})$, the challenger randomly selects $Q_i, h_i, h'_i \in Z_q$ , $T_{h_i} = h_i(A \parallel P_k \parallel f(t_i))$, and adds $\{A, T_{h_i}\}$ to the $L_1$ list. Make $C_i = Q_iP - h_iA - h'_iT_{h_i} \cdot P_k - T_{h_i} \cdot PK_i$. Insert $(m_i, C_i, Q_i, A_i)$ into $L_3L_4$ list.

- Output stage: Finally, the adversary $A$ outputs a forged signature of $(VID, A, m)$, at this time, if $VID \neq V ID_m$, the challenger declares failure, otherwise, the challenger finds the following signature message from the signature prophecy machine: $(m_i, \sigma_i = (A_i, Q_i, F_i, C_i, PK_i)$. If the challenger wins the game, there will be:

$$Q_iP = C_i + h_iA + h'_iT_{h_i} \cdot P_k + T_{h_i} \cdot PK_i$$

(1)

The adversary can reconstruct a new valid signature $(m_i, \sigma'_i = (A_i, Q'_i, F_i, C'_i, PK_i)$ with different $Q_i, h'_i$ in polynomial time, that is, the following equation holds:

$$Q'_iP = C'_i + h'_iA + h'_iT_{h_i} \cdot P_k + T_{h_i} \cdot PK'_i$$

(2)

According to equations (1) and (2), Challenger $C$ can calculate:

$$(Q_i - Q'_i) \cdot P = (h_i - h'_i)T_{h_i} \cdot s \cdot P$$

(3)

By equation (3) the challenger can solve $s = \frac{(Q_i - Q'_i)}{(h_i - h'_i)T_{h_i}} \mod q$. That is, the challenger solved the ECDLP problem.

Finally, we calculate the advantages of Challenger $C$ in solving ECDLP difficult problems. If Challenger can successfully solve ECDLP problems, it should meet the following two situations at the same time:

$E_1$: Challenger $C$ never stops the game.

$E_2$: $Q'_i$ is a legal signature for message $(VID_m, m)$.

So, the challenger's probability of winning is:

$$\varepsilon^* = pr[E_1 \land E_2] = pr[E_1]pr[E_1 \mid E_2]$$

(4)

Among them, $pr[E_1 \mid E_2] = \varepsilon$

Through the analysis and calculation of the game process:

$$pr[E_1] = (1 - \frac{q_{h2}}{q} \cdot \frac{q_{h4}}{q}) \cdot \frac{1}{q} \cdot (1 - \frac{q_{h5}}{q}) \cdot \frac{1}{q} \cdot (1 - \frac{q_{h5}}{q}) \cdot \frac{1}{q} \cdot \frac{1}{q}$$

(5)

Therefore, we can draw the following conclusion from equations (4) and (5):

$$\varepsilon^* \geq (1 - \frac{q_{h2}}{q} \cdot \frac{q_{h4}}{q}) \cdot \frac{1}{q} \cdot (1 - \frac{q_{h5}}{q}) \cdot \frac{1}{q} \cdot (1 - \frac{q_{h5}}{q}) \cdot \frac{1}{q} \cdot \frac{1}{q} \cdot \varepsilon$$

Obviously, if Challenger $C$ can successfully forge a signature with advantage $\varepsilon$, then the challenger can solve the ECDLP problem. However, in the random prophecy model, the ECDLP problem is a difficult problem, that is to say, the opponent’s advantage does not exist. That is to say, the scheme in this paper can resist the forgery attack of adversary. Proof complete.
Theorem 2: In the random prediction model, if there is a super adversary $A_{II}$ in polynomial time that can win the game with a non-negligible probability $\varepsilon$, then there must be a challenger who can solve the ECDLP problem with the following advantages:

$$\varepsilon^* \geq (1 - \frac{q_{h2}}{q}) \varepsilon (1 - \frac{1}{q_{cu}}) \varepsilon (1 - \frac{1}{q_{cu}}) \varepsilon (1 - \frac{q_{h3}}{q}) (1 - \frac{q_{h4}}{q}) (1 - \frac{q_{h5}}{q}) \frac{1}{q_{cu}}$$

where $q_{h2}$ $q_{h3}$ $q_{h4}$ $q_{h5}$ represents the corresponding number of hash prediction machine queries, $q_{cu}$ represents the number of user prediction machine queries, and $q_{c}$ represents the number of partial private key queries of the user, $q_{m}$ represents the number of user secret value queries.

It has been proved that the scheme in this paper can resist the forgery attack of super adversary $A_{II}$, and the scheme is secure. The proof process is similar to Theorem 1, and the space is limited. I will not repeat it here.

6. Performance Analysis

6.1. Performance Comparison of Schemes

This part mainly analyzes and compares the main performance of the scheme and the competitive scheme. Table 1 is the description of the symbols used. As shown in table 2 the scheme proposed in reference [6] does not have bilinear pairings and can not resist class $A_{I}$ adversary attacks. In reference [16], a lighter cryptographic scheme is constructed by using elliptic curve, but it can not resist malicious KGC attacks. Although the certificateless aggregate signature scheme proposed in reference [14] meets the security requirements, it has a great computational overhead and will cause a great burden of communication in the VANETs environment. The scheme in this paper not only meets all the security requirements, but also uses elliptic curve to construct a lighter certificateless aggregate signature scheme, which is more suitable for VANETs communication environment.

| $T_{bp}$ | Bilinear pairing operation |
| $T_{bm}$ | Bilinear midpoint multiplication |
| $T_{ba}$ | Addition operation in bilinear alignment |
| $T_{cu}$ | Point multiplication of elliptic curve |
| $T_{ca}$ | Addition operation in elliptic curve |
| $T_{h}$ | Hash operation |

| Table 1. symbol description. |
| Scheme | Scheme [6] | Scheme [16] | Scheme [14] | Ours scheme |
|------------------|-------------|-------------|-------------|-------------|
| Confidentiality  | √           | √           | √           | √           |
| Anonymity        | √           | √           | √           | √           |
| Unlinkability    | √           | √           | √           | √           |
| No bilinear pair.| ×           | √           | ×           | √           |
| Resist class $A_{I}$ adversaries | × | √ | × | √ |
| Resist class $A_{II}$ adversaries | √ | × | √ | √ |

6.2. Comparison of Computational Costs of Schemes
As shown in table 3, the total computational cost of the certificateless aggregate signature scheme proposed in reference [14] is $5T_{em} + 3T_{ba} + 4T_{h}$ in the signature algorithm part, $4T_{lp} + 2T_{lm} + T_{ba} + 4T_{h}$ in the verification algorithm part and $4T_{lp} + 7nT_{lm} + nT_{ba} + 4nT_{h}$ in the aggregate signature algorithm part.

In the same way, the total computational cost of the scheme proposed in reference [6] and reference [16] can be obtained. In the scheme of this paper, the total computational cost of signature algorithm is $2T_{lp} + T_{ba} + T_{h}$, the total computational cost of verification algorithm is $3T_{lp} + 3T_{ba} + 3T_{h}$, and the total cost of aggregate signature algorithm is $(3n+2)T_{em} + 3nT_{ba} + 3nT_{h}$. It can be seen that because the certificateless aggregate signature scheme is constructed by using elliptic curve, the complex bilinear pairing operation is avoided. This scheme has a great advantage over the certificateless aggregate signature scheme proposed in references [6, 14] in terms of computational cost.

### Table 3. Scheme calculation overhead.

| Scheme         | Signature algorithm   | Verification algorithm | Aggregate signature algorithm |
|----------------|-----------------------|------------------------|------------------------------|
| Reference [6]  | $2T_{im} + T_{ba} + T_{h}$ | $3T_{lp} + T_{lm} + T_{ba} + 2T_{h}$ | $3T_{lp} + nT_{lm} + nT_{ba} + 2nT_{h}$ |
| Reference [16] | $T_{em} + T_{ea} + T_{h}$ | $3T_{em} + 2T_{ea} + 2T_{h}$ | $(n+2)T_{em} + (n+2)T_{ea} + 2nT_{h}$ |
| Reference [14] | $5T_{im} + 3T_{ba} + 4T_{h}$ | $4T_{lp} + 2T_{lm} + T_{ba} + 4T_{h}$ | $4T_{lp} + 7nT_{lm} + nT_{ba} + 4nT_{h}$ |
| Ours scheme    | $T_{em} + 2T_{h}$      | $5T_{em} + 3T_{ea} + 3T_{h}$ | $(3n+2)T_{em} + 3nT_{ea} + 3nT_{h}$ |

In order to compare the computational efficiency of the scheme more clearly, a simulation experiment is carried out in a memory environment with Intel Core i5-7500 processor, 3.0GHz frequency and 8GB. As shown in figures 2 and 3, the computational efficiency of the scheme proposed in this paper is compared with that of references [6, 14, 16]. The results show that the scheme proposed in this paper has obvious advantages over the scheme proposed in references [6, 14] in terms of signature algorithm and verification algorithm, and is basically the same as that in reference [16]. However, the scheme proposed in reference [16] can not resist class II adversary attacks, so its security is not as good as that of this scheme. In addition, this scheme uses aggregate signature technology, which further reduces the computing overhead, so that it can meet the VANETs environment with high communication and computing overhead.

**Figure 2.** Time-consuming signature algorithm.

**Figure 3.** Time-consuming verification algorithm.

7. Conclusions
Aiming at the problem of security and privacy in the updating of road navigation information in VANETs, a certificateless aggregate signature scheme with conditional privacy protection based on certificateless cryptosystem is proposed, and the security of the scheme is expressed by strict security proof. The conditional privacy protection of vehicle users is realized by generating temporary pseudonyms. The bilinear pairing operation is not used in the construction process of the scheme, and the aggregate signature technology is used to greatly reduce the computational cost of the scheme. Through the performance analysis and comparison with other schemes, this scheme has obvious advantages over the competitive schemes in terms of security and computational efficiency, and is suitable for VANETs application environment.

Acknowledgments
This research was funded by the National Natural Science Foundation of China (Grant No.61662071 and 61662069).

References
[1] Alessandrini A, Campagna A, Site P D, et al. 2015 Automated vehicles and the rethinking of mobility and cities Transportation Research Procedia 5 145-160.
[2] Lai C Z, Zhang M and Zheng D 2019 A safe and efficient map updating scheme for driverless vehicles Computer Research and Development 56 (10) 2277-86.
[3] Lke D, Forest H, Aman R, et al. 2018 Generative street addresses from satellite imagery ISPRS International Journal of Geo-Information 7 (3) 84.
[4] Demir I, et al. 2018 Deep Globe 2018: A challenge to parse the earth through satellite images IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (Salt Lake City) UT pp 172-17209, doi: 10.1109/CVPRW.2018.00031.
[5] He D, Zeadally S, Xu B, et al. 2015 An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks IEEE Transactions on Information Forensics & Security 10 (12) 2681-91.
[6] Horng S J, Tzeng S F, Huang P H, et al. 2015 An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks Information Sciences: An International Journal 317 48-66.
[7] Zhou T and Xu J 2011 Provable secure authentication protocol with anonymity for roaming service in global mobility networks Computer Networks 55 (1) 205-213.
[8] Ali I, Lawrence T and Li F 2020 An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs Journal of Systems Architecture 103 (C).
[9] Zhang X Y, Xu Y and Cui J 2016 Anonymous authentication protocol based on no certificate signature in vehicle network Computer Engineering 42 (003) 18-21.
[10] Zuo L M, Zhou Q and Chen L L 2019 A certificated safe and efficient short signature scheme without certificate Computer Engineering 45 (06) 193-198.
[11] Zhao Y, Hou Y, Wang L, et al 2019 An efficient certificateless aggregate signature scheme for the internet of vehicles Transactions on Emerging Telecommunications Technologies (1).
[12] Xu Z, He D, Kumar N, et al. 2020 Efficient certificateless aggregate signature scheme for performing secure routing in VANETs Security and Communication Networks (2) 1-12.
[13] Xu G, et al. 2020 A security-enhanced certificateless aggregate signature authentication protocol for In VANETs IEEE Network 34 (2) 22-29 doi: 10.1109/MNET.001.1900035.
[14] Zhao N, ZHANG G and Gu X H 2020 Privacy protection certificateless aggregate signature scheme in VANET Computer Engineering 046 (001) 114-120,128.
[15] Kamil I A and Ogundoyin S O 2018 An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks Journal of Information Security and Applications 44 (FEB.) 184-200.
[16] Cui J, Zhang J, Zhong H, Shi R and Xu Y 2018 An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks Information Sciences 451-452.

[17] Jia X, He D, Liu Q, et al. 2018 An efficient provably-secure certificateless signature scheme for internet-of-things deployment Ad Hoc Networks 71 (MAR.) 78-87.