PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-preserving Authentication Scheme in Vehicular Ad-hoc Networks

Jing Zhang, Jie Cui, Hong Zhong, Zhili Chen, Lu Liu

***Abstract*—Existing security and identity-based vehicular communication protocols used in Vehicular Ad-hoc Networks (VANETs) to achieve conditional privacy-preserving mostly rely on an ideal hardware device called tamper-proof device (TPD) equipped in vehicles. Achieving fast authentication during the message verification process is usually challenging in such strategies and further they suffer performance constraints from resulting overheads. To address such challenges, this paper proposes a novel Chinese remainder theorem (CRT)-based conditional privacy-preserving authentication scheme for securing vehicular authentication. The proposed protocol only requires realistic TPDs, and eliminates the need for pre-loading the master key onto the vehicle's TPDs. Chinese remainder theorem can dynamically assist the trusted authorities (TAs) whilst generating and broadcasting new group keys to the vehicles in the network. The proposed scheme solves the leakage problem during side channel attacks, and ensures higher level of security for the entire system. In addition, the proposed scheme avoids using the bilinear pairing operation and map-to-point hash operation during the authentication process, which helps achieving faster verification even under increasing number of signature. Moreover, the security analysis shows that our proposed scheme is secure under the random oracle model and the performance analysis shows that our proposed scheme is efficient in reducing computation and communication overheads.**

***Index Terms*—Vehicular Ad-hoc Networks (VANETs), Chinese Remainder Theorem (CRT), authentication, conditional privacy-preserving, elliptic curve.**

I. Introduction

VEHICULAR Ad-hoc networks (VANETs) are a form of ad-hoc networking that encompasses vehicles as nodes for message transmission. In the VANET environment, vehicles are equipped with a module called on-board unit (OBU) which enables communication between the vehicular nodes through communication protocols such as 802.11p, 3G/4G, etc. [1]. Communication in VANETs are usually of two types such as vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. Both of these communications are carried out using the Dedicated Short Range Communications (DSRC) standard [2], [3].

A typical VANET environment consists of OBUs equipped in vehicles, roadside units (RSUs) installed alongside the roads, and trusted authorities (TAs). A system of VANET architecture is shown in Fig. 1. According to the DSRC protocol standard, each vehicle periodically broadcasts traffic related information such as location, traffic accidents records, etc., to nearby vehicles and RSUs every 100-300 milliseconds [4], [5]. RSUs can potentially aid road traffic management by transmitting messages reflecting on-road scenarios. Such messages also benefit on-road drivers by disseminating information about the driving environment.

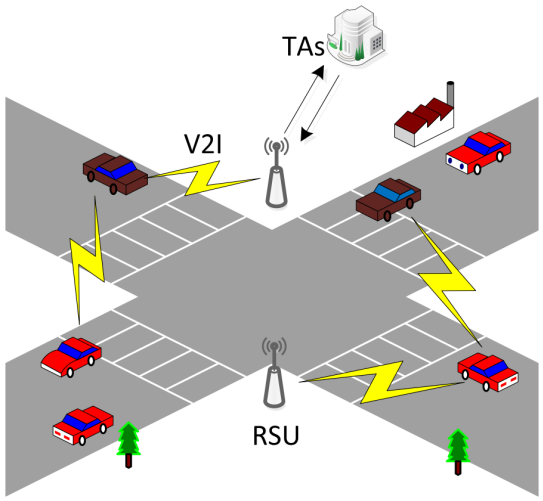


Fig. 1. A system architecture of the VANETs.

Given the fact the VANETs exploits wireless communication, obvious security and privacy vulnerabilities of wireless communication cannot be eliminated [6]–[13]. For instance, malicious vehicles in the network might broadcast wrong information to mislead and interfere normal operation of the network. Such incorrect information might mislead traffic management department with incorrect decisions. Besides, user's sensitive and private information such as their real identity and driving route etc., should be protected from attacks such as eavesdropping etc.

Moreover, authenticating user identity is one of the core requirements in VANETs in order to effectively identifying and eliminating malicious users in the network. Existing authentication schemes [14]–[26] can be broadly classified into identity management authentication schemes and message authentication schemes. Both the schemes are susceptible under adversarial environments, which can disrupt their function. It is common for a malicious user when involved in accidents

J. Zhang, J. Cui, H. Zhong and Z. Chen are with the School of Computer Science and Technology, Anhui University, Hefei 230039, China, the Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China, and the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China (e-mail: cuijie@mail.ustc.edu.cn).

L. Liu is with the School of Computing and Mathematics, University of Derby, Derby DE22 1GB, UK (e-mail: l.liu@derby.ac.uk).

to send falsified information, this should be efficiently traced by the TA. Such core requirements necessitate efficient conditional privacy and message authentication schemes as integral components of VANETs.

A. Related Work

A wide range of research works have previously addressed resolving security and privacy issues in VANETs, which can be divided into five categories. The first category exploits digital signatures based on public key infrastructure (PKI) [9], [17], [27] to ensure message integrity, authentication and non-repudiation. Recently, the Security Credential Management System (SCMS) [28] proposed by USDOT utilizes a Public Key Infrastructure (PKI) approach to support trusted and secure communications. However, each vehicle in the network requires a large number of certificates to achieve privacy. Furthermore, storing the certificates of all the participating vehicles incur higher storage costs for the TAs. Besides, the certificate verification process involving large number of nodes is usually tedious with this approach.

In order to overcome the limitations of the traditional certificate based management methods, the second category used the group signatures technology [18], [23], [29], [30]. However, the member revocation problem of this method incurs a verification and storage/transmission cost higher than most traditional schemes. Such issues restrains the performance of the group signature based schemes under extreme environment.

With the motivation of reducing the verification overheads of the group signature technology, the third category approaches exploited identity-based batch authentication protocols [19]–[22], [31]. Batch authentication strategies significantly reduces the time incurred in the authentication process. However, such schemes rely heavily on a dedicated TPD. Given one of the TPDs being compromised by malicious users, such schemes face the risk of single point of failure, leaving the entire network susceptible for privacy attacks.

The fourth category is a software based approach without involving TPDs [23]–[26], developed with the motivation of overcoming the fundamental storage issues of hardware based systems. Such software-based schemes only use two shared secrets in order to meet the security and privacy requirement. However, vehicles upon joining the RSUs require access to the shared secret parameters from the TAs. Another factor restraining the efficiencies of the software based schemes is the moving speed of the vehicular nodes, which creates high level of communication overheads.

The final category works [32]–[35] based on a trusted authority, TRA, which generates a batch of pseudo identities (pseudo-IDs) for each vehicle. These pseudo-IDs are later sent to another trusted institution called PKG via a secure channel. For a given vehicle, PKG generates a pseudo-ID corresponding to its private key and sends the pseudo-IDs/private keys to the vehicle securely. However, an increasing number of network vehicles will increase the demand for generating more pseudo-IDs. Under this scenario, both the TRA and PKG need to be added at the same time, and multiple TRAs can make the vehicle tracking and revocation process to be more complex and be detrimental for protocol extensions.

Many of the existing schemes available in the above literature are only used to provide authentication. In addition, we need to discuss some existing group key management methods for using CRT in wired and wireless networks [36]–[38]. Zheng et al. [36] introduced two centralized group key management protocols based on the CRT. By shifting more computing load onto the key server, they optimize the number of re-key broadcast message, user-side key computation and number of key storages. However, their protocols require more computation power from the key server.

Zhou and Yong [37] proposed a CRT-based static key tree structure for distributing the group key to the members of the group when group membership changes. It deal with the scenario of a pre-defined static prospective user set containing all potential customs of multicast services and concentrate on the stateless receiver case. It can reduce the key server's computation complexity for each group key distribution. However, it also increases the workload of key server by allowing the key server to find a common group key by using CRT for 'n' number of congruential equations.

Vijayakumar et al. [38] proposed a CRT-based group key management scheme that drastically reduces computation complexity of the key server. The computation complexity of key server is reduced to O(1) in this proposed algorithm. Moreover, the computation complexity of group member is also minimised by performing one modulo division operation when a user join or leave operation is performed in a multicast group.

B. Our Contribution

With the motivation of addressing the aforementioned issues, this paper proposes a CRT-based conditional privacy-preserving authentication (PA-CRT) protocol for the purpose of establishing secure communication between vehicles. The CRT-based domain key management scheme is used to generate a common domain key for each vehicle in the TA side, which has been used in many existing schemes [36]–[38]. TA uses the CRT technology to generate a domain key for vehicles in its domain. To prevent an intruder to use other vehicles secret keys, we have included an identity of each authenticated driver in the TPD issued by the TA. The driver inputs his/her fingerprint to verify that it matches the identity, each time the user uses the TPD. Important contributions of this paper are listed as follows:

- Firstly, a new PA-CRT scheme is proposed for VANETs, which eliminates the need for TPDs to store long-term system secret. With the proposed scheme, fingerprint from a corrupted vehicle will not be validated, so that the TPD is not required to proceed further. The proposed scheme also minimises the number of affected vehicles, even under the cases where the vehicles are compromised after the fingerprint validation.
- Secondly, the proposed scheme uses the Chinese remainder theorem, which greatly reduces the computational complexity of the TAs. Besides, the computation

complexity of the domain vehicles is also minimised by performing the one modulo division operation upon vehicles joining or leaving in a multicast domain.
- Thirdly, the efficiencies of the proposed protocol in satisfying the security and privacy requirements are demonstrated. Moreover, the analysis of the computation and the communication overhead shows that the proposed scheme exhibits better performance in comparison with the existing schemes.

C. Organization of The Rest Paper

The remainder of this paper is organised as follows: Section II introduces the preliminaries and background. The proposed CRT-based conditional privacy-preserving authentication (PA-CRT) scheme is described in Section III. The security analysis and performance evaluation of our scheme are presented in Section IV and V, respectively. Section VI concludes this paper.

II. Preliminaries and Background

This section briefly presents a background on cryptography including Chinese remainder theorem [36]–[38] and elliptic curve cryptosystem [39], and further describes the network model, security model and security objectives of the PA-CRT scheme for VANETs.

A. Chinese Remainder Theorem

The Chinese remainder theorem is a theorem of number theory, which states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime [36]–[38].

Let $k_1, k_2, k_3, \ldots, k_n$ be pairwise relative prime positive numbers. Let K_i^{-1} be the modular multiplicative inverse of an integer $K_i \bmod k_i$ so that the following equation is satisfied.

$$K_i K_i^{-1} \equiv 1 \,(\mathrm{mod} k_i) \tag{1}$$

where $i = 1, 2, \ldots, n$.

Let $a_1, a_2, a_3, \ldots, a_n$ be any given n positive integers. Then, CRT states that the pair of congruences,

$$X \equiv a_1 \bmod k_1, X \equiv a_2 \bmod k_2, \ldots, X \equiv a_n \bmod k_n \tag{2}$$

has a unique solution mod $\partial_g = k_1 k_2 \ldots k_i = \prod_{i=1}^{n} (k_i)$. The key server can obtain the solution with the following function.

$$X = a_1 + a_2 + \ldots + a_n \,(\bmod \partial_g) = \sum_{i=1}^{n} a_i \beta_i \gamma_i \,(\bmod \partial_g) \tag{3}$$

where $\beta_i = \frac{\partial_g}{k_i}$ and $\beta_i \gamma_i \equiv 1 \bmod k_i$.

B. Elliptic Curve Cryptosystem

Let F_p be a finite field, which is determined by a prime number p. Let a set of elliptic curve point E over F_p be defined by the equation: $y^2 = x^3 + ax + b(\mathrm{mod} p)$, where $a, b \in F_p$ and $(4a^3 + 27b^2) \bmod p \neq 0$. The main characteristics of Elliptic Curve are listed below:

- Scalar point multiplication: The scalar multiplication of E is defined as $mP = P + P + \ldots + P$ (m times) where $m \in Z_q^*$, $m > 0$.
- **Definition 1.** Elliptic Curve Discrete Logarithm problem (ECDLP): Given two random points $P, Q \in G$ on curve E, where $Q = xP$, $x \in Z_q^*$. It has been proved that calculating x from Q is difficult.
- **Definition 2.** Suppose that an algorithm A solves the ECDLP problem in group G within polynomial time, and the probability of success is defined as:

$$Succ_{A,G}^{ECDLP} = \Pr\left[A(P, xP) = x : x \in Z_q^*\right] \geq \varepsilon$$

then the ECDLP hypothesis is defined as the algorithm A in any polynomial time, and the $Succ_{A,G}^{ECDLP}$ is negligible.

C. Network Model

The two-layer network model of VANETs, has been increasingly used in the literature [19]–[22], [24]–[26], [31]–[33], as shown in Fig. 2.

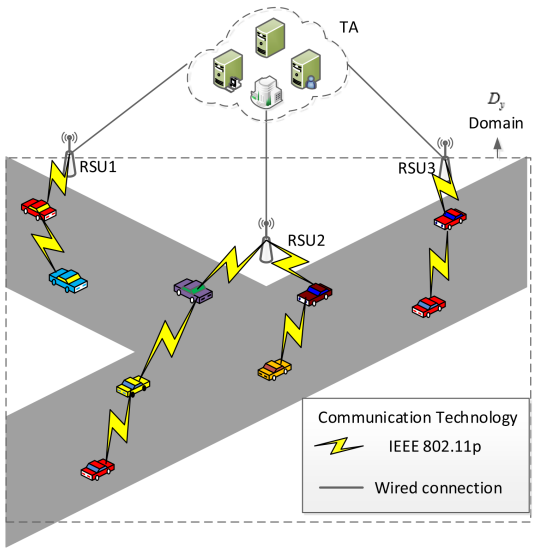


Fig. 2. Network model.

- Trusted authority (TA)[1]: The TA, trusted by RSUs and OBUs, generates the system parameters and the secret key for each vehicle and preloads them into each corresponding vehicle. TA is responsible to generate the security information for each domain. To avoid issues such as single point of failure and bottlenecks, a set of reliable servers and redundant TAs with identical functionalities and databases are installed in the network.

[1]Here TA is consist of redundant TAs and a set of reliable servers, such as registration servers, key generation server, tracing server and so on.

In our scheme, a dedicated TA is assigned for each cities in the country. When a vehicle moves from one city to another, the vehicle's credentials will be verified using the TA of the vehicle's originally registered city. This verification process will be initiated by the TA of the newly entered city. It has been assumed that TAs comprise sufficient storage capacity with a negligible probability to be compromised by an adversary [40].

- Roadside units (RSUs): The RSUs are connected to the TA with wired links whilst the vehicles are connected to TA with wireless links. The main function of RSU is tantamount to store and forward the information between the vehicle, the TA and other RSUs.
- Vehicles: Each vehicle is equipped with a realistic TPD on board units (OBU), and can communicate with other vehicles or RSUs through the DSRC protocol. Each OBU has its own real identity, pseudo identities, and a private key. Every originating message from vehicles needs to be signed before being sent to nearby vehicles or RSUs.

D. Security Model

In this subsection, we prove that the signature scheme in the PA-CRT protocol (PA-CRT_Sign scheme) is secure under the random oracle model, and the definitions are as follows:

Definition 3. The PA-CRT_Sign scheme consists of three steps including setup, sign, and verify. These setups are defined as follows:

1) $Setup(1^k)$: Given the random system security parameter k, the TA outputs public system parameters $params$, system public key P_{pub} and system master key s.
2) $Sign(ID_1, sk, m)$: Given the system's parameter $params$, signer's secret key sk, signer's identity ID_1 and the message m to be signed, it outputs the corresponding signature σ.
3) $Verify(ID_2, P_{pub}, m, \sigma)$: Given the system's parameter $params$, the system's public key P_{pub}, the pseudo-identity ID_2, the signature σ and the message m, it outputs 1 if σ is a valid signature of the message m and outputs 0 otherwise.

Definition 4: The PA-CRT_Sign scheme is secure if the probability that any adversary A could break the authentication of the PA-CRT_Sign algorithm is negligible in any polynomial time. The signature algorithm is secure against existential forgery under the adaptive-chosen-message attack.

Game: Based on the network model and the adversaries' ability, the security model for the PA-CRT scheme is defined through a game played between an adversary A and a challenger B. The game between adversary A and challenger B is defined as follows:

1) Setup: Challenger B runs the Setup step with a security parameter k to obtain the system parameters $params$, system public key P_{pub}, then it sends $(P_{pub}, params)$ to A.
2) Query: The adversary A asks the following questions to the challenger B:
   - Hash query: Adversary A requests the Hash function, challenger B returns the corresponding Hash value, and stores the Hash value.
   - Sign query: Adversary A can request the signature of a message m of its choice. Then, B returns σ to A.
3) Output: When the adversary A considers that the above process has been completed, A will return a valid signature (m^*, σ^*). If this output satisfies $Verify\,(m^*, \sigma^*) = Accept$, and m^* has not been requested to the Sign queries, the adversary A is expected to win in the Game.

E. Security Objectives

Both security and privacy are important for secure communications in VANETs. Based on the state-of-art research achievements [19]–[21], [38], [40]–[42], a secure PA-CRT scheme for VANETs should satisfy the following requirements: message integrity and authentication, identity privacy preserving, forward and backward secrecy, traceability, unlinkability and resistance to attacks. The combination of identity privacy protection and traceability represents the definition of conditional privacy.

1) Message integrity and authentication: To guarantee secure communication, the vehicle or RSU should be able to verify the integrity and validity of the received messages, and should be able to detect any modification of the received message.
2) Identity Privacy Preserving: To guarantee users' privacy, the real identity of a vehicle should be maintained anonymous to other vehicles and third-parties. Any adversary other than the TA should not be able to extract a vehicle's real identity by analysing multiple messages sent by it.
3) Perfect backward secrecy: Backward security is a technology that prevents new vehicles from accessing the communication information of the previous vehicles when the new vehicles join the group. To protect the confidentiality of messages issued in the domain, a new vehicle can join the group and update the old group key, but the old group key cannot be obtained by the newly added vehicle.
4) Perfect forward secrecy: Forward secrecy is a technology that prevents vehicles leaving the group from accessing the communication information of the currently present vehicles. Forward secrecy further guarantees that only the existing vehicles can update the existing group key, so that the modified group key cannot be accessed by the leaving vehicles.
5) Traceability: To prevent malicious vehicles from denying their liability for traffic accidents by sending false messages, the TA should have the ability to find out the real identity of a vehicle from its message in case of any misbehaviour.
6) Un-linkability: To preserve privacy, RSUs and malicious vehicles are not able to link two messages sent by the same vehicle with the same ID.

7) Resistance to attacks: To resist other known attacks, the PA-CRT scheme should be able to withstand various common attacks such as the impersonation attack, the modification attack, the replay attack and the collusion attack.

III. The Proposed Scheme

This section details our proposed PA-CRT protocol developed based on the CRT. Fig. 3 illustrates an authentication process between a single TA and a number of vehicles in PA-CRT for VANETs. This section mainly includes five phases including the system initialisation, secure domain key computation, vehicles pseudo identity generation, message signing, message verification and domain key updating. The notations used in this process are shown in Table 1.

TABLE I
Notations and Definitions Used

Notations	Definitions
TA	The trusted authority
RSU	The roadside unit
V_i	The i-th vehicle
D_y	The y-th domain
s	The master secret key of TA
P_{pub}	The public key of TA
sk	Vehicles Secret Key
k_d	Vehicles Domain Key
ET_i	The validity period length of the domain key k_d
RID	Real identity of the vehicle
ID_i	An pseudo-identity of V_i
ID_{ij}	A part of ID_i such that $ID_i = (ID_{i1}, ID_{i2})$
M_i	The message sent by V_i
T_i	The current timestamp
ΔT	The validity period of the pseudo-identity
H_1,H_2,H_3	Three secure hash functions
$\oplus$	The exclusive-OR operation
$\|\|$	The Concatenation operation

A. System Initialization

Given the public parameters $\left(p, q, E, G, Z_q^*\right)$, the TA initialises the system as per the following steps.

1) The TA selects a random number $s \in Z_q^*$ as the system secret key and computes the corresponding public key $P_{pub} = sP$;
2) The TA chooses two large prime numbers p and q, where $p > q$ and $q \leq \lceil p/4 \rceil$, p is used for defining a multiplicative group z_p^* and q is used for choosing the domain key values;
3) The TA chooses sk_i from the multiplicative group z_p^* for 'n' number of vehicles which is given to the vehicle drivers at the time of offline registration;
4) The TA calculates $\partial_g = \prod_{i=1}^{n} (sk_i)$, and $x_i = \frac{\partial_g}{sk_i}$ where $i = 1, 2, \ldots, n$;
5) Then calculates y_i such that $x_i \times y_i \equiv 1 \bmod sk_i$;
6) TA multiplies all drivers x_i and y_i values and stores them in the variables $\mathrm{var}_i = x_i \times y_i$, and calculates the value $\mu = \sum_{i}^{n} \mathrm{var}_i$;
7) TA selects four secure one-way hash functions H_i: $\{0,1\}^* \rightarrow Z_q^*$ $(i = 1, 2, 3, 4)$. Then, the system parameters will be published, which include $\left(q, G, E, P, P_{pub}, Z_q^*, H_1, H_2, H_3, H_4\right)$

B. Secure Domain Key Computation

For a vehicle V_i in the domain D_y, the VANET domain vehicles complete the registration process and obtain their corresponding domain secret keys from the TA. When TA wants to transmit information to a domain of VANET vehicles in order to support the domain communication, TA computes the domain key and multicasts it to the vehicles domain through RSU, as explained below.

1) TA chooses a random element $k_d \in Z_q^*$ as a new domain key, and computes $\gamma_d = k_d \times \mu$.
2) TA signs γ_d and ET_i using its private key sk_{TA}. It then computes $K_{pud} = k_d \cdot P$ and broadcasts the message $\{\gamma_d, K_{pud}, SIG_{sk_{TA}}(\gamma_d || ET_i)\}$ to all RSUs and vehicles in D_y, where ET_i defines the valid period of this domain key k_d.
3) On receiving the γ_d value from the TA side, an authorised vehicle can gain the new domain key k_d through a one modulo division operation $\gamma_d \bmod sk_i = k_d$.

Since $k_d < q < sk_i < p$ and $\mu \bmod sk_i = 1$, k_d gained through the above process must be equal to the value of k_d generated in Step 1). When 'i' reaches to n, TA executes the system initialisation algorithm to compute ∂_g, var_i and μ for 'm' number of drivers, where $m = n \times \delta$, where δ is a constant, which satisfies $\delta < 5$.

C. Generation of Pseudo Identity and Message Signature

Each vehicle V_i sends its real Fingerprint into TPD to activate it. If the Fingerprint is correct, TPD will generate pseudo identities and signing keys. Then, the vehicle broadcasts its pseudo identities, the message and the corresponding message signature to its nearby vehicles and RSUs. Fig. 4 depicts the message authentication procedure of the realistic TPD.

1) For generating a pseudo identity, the tamper-proof device first generates a random nonce $r_i \in Z_q^*$. Its pseudo identity ID_i contains two parts – $ID_{i,1}$ and $ID_{i,2}$ where $ID_{i,1} = r_i \cdot P$ and $ID_{i,2} = RID_i \oplus H_1(r_i \cdot \mathrm{P}_{pub})$.
2) Then, the tamper-proof device obtains the new domain key k_d through a one modulo division operation $\gamma_d \bmod sk_i = k_d$, then computes $\alpha_i = H_2(ID_i || T_i)$ and $S_i = \alpha_i \cdot k_d \bmod q$.
3) When an OBU needs to send a message M_i , it inputs M_i to the tamper-proof device, and then computes $\beta_i = H_3(ID_i || M_i || T_i)$. A message M_i is signed by calculating the signature $\sigma_i = S_i + \beta_i \cdot r_i \bmod q$.
4) V_i sends the final message $(M_i, ID_i, T_i, \sigma_i)$ to the nearby RSUs and vehicles every 100-300 ms according to the DSRC standard.

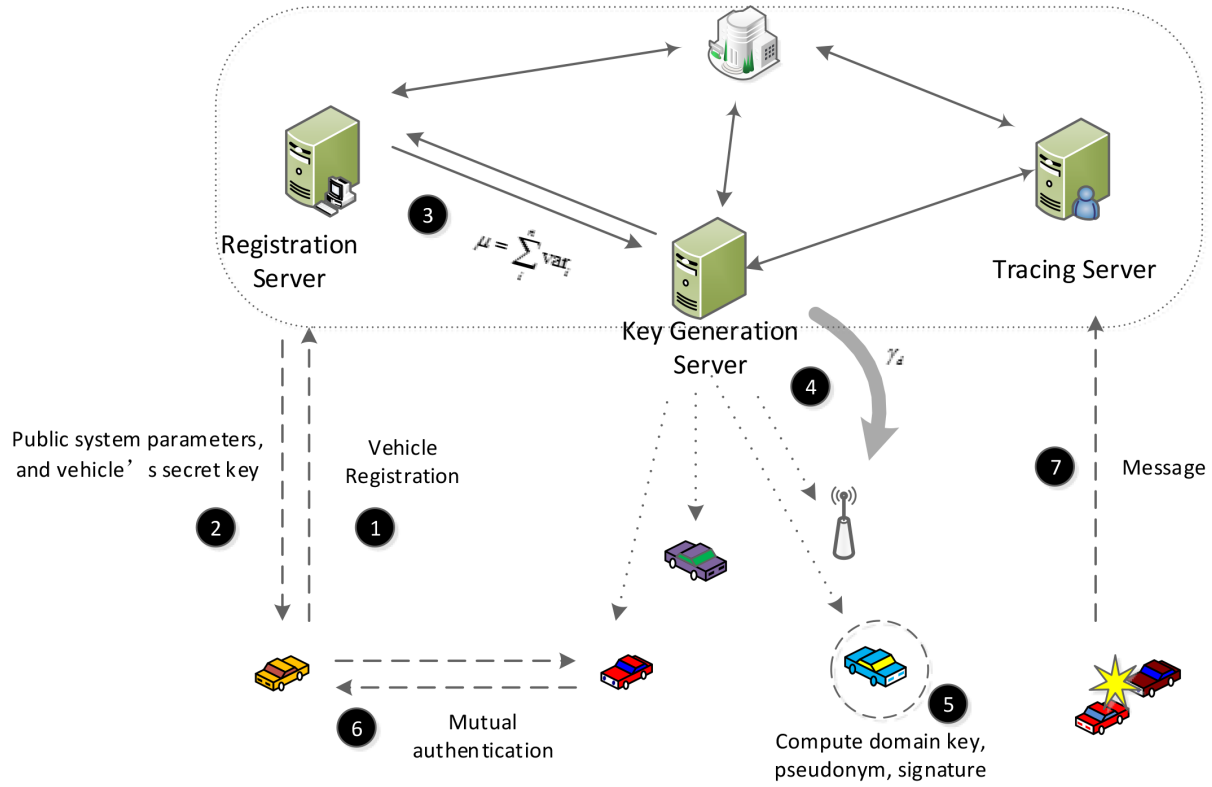


Fig. 3. An illustration of the operations in PA-CRT for VANETs.

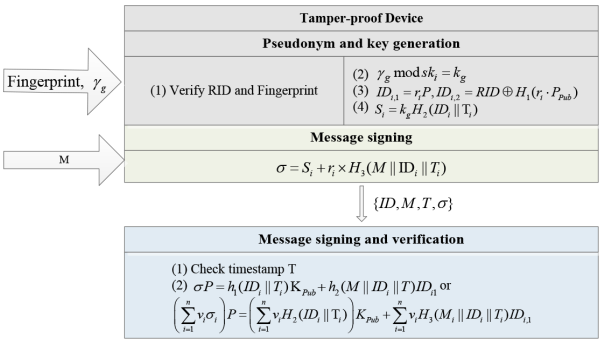


Fig. 4. The message authentication procedure.

D. Message Verification

When the verifier collects enough messages from nearby vehicles or when the verification period is expired, the verifier checks the validity of the signatures of the messages as follows.

[Authentication for One Message]

Given the final message $\{M_i, ID_i, T_i, \sigma_i\}$ sent by the vehicle V_i, the verifier uses the public parameters $\left(q, G, E, P, P_{pub}, Z_q^*, H_1, H_2, H_3\right)$ assigned by TA to execute the following steps.

1) The verifier checks the freshness of T_i. Assume that the receiving time is T. If $\Delta T \geq T - T_i$, the verifier continues; otherwise, the verifier discards the message.
2) The verifier verifies the signature of the message by checking whether the formula $\sigma_i \cdot P = \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1}$ holds true or not. If not, the verifier will rejects the message; otherwise, the message will be considered legal and unaltered.

Due to $\mathrm{P}_{pub} = s \cdot \mathrm{P}$, $ID_{i,1} = r_i \cdot P$, $ID_{i,2} = RID_i \oplus H_1\left(r_i \cdot \mathrm{P}_{pub}\right)$, $\alpha_i = H_2\left(ID_i || T_i\right)$, $S_i = \alpha_i \cdot k_d \bmod q$, $\beta_i = H_3\left(ID_i || M_i || T_i\right)$ and $\sigma_i = S_i + \beta_i \cdot r_i \bmod q$, the correctness of the verification can be ensured using the below formula.

$$\begin{aligned} \sigma_i \cdot P &= (S_i + \beta_i \cdot r_i) \cdot P \\ &= S_i \cdot P + \beta_i \cdot r_i \cdot P \\ &= \alpha_i \cdot k_d \cdot P + \beta_i \cdot ID_i \\ &= \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1} \end{aligned} \tag{4}$$

[Batch Authentication of Multiple Messages]

Assume that the verifier receives a batch of message signatures $\sigma_1, \sigma_2, \ldots, \sigma_n$ from the vehicles $V_1, V_2, \ldots, V_n$ on messages $\{M_1, ID_1, T_1, \sigma_1\}$, $\{M_2, ID_2, T_2, \sigma_2\}$,...,$\{M_n, ID_n, T_n, \sigma_n\}$. The batch authentication process is described as follows.

1) The verifier checks whether T_i of message M_i is new or not, where $i = 1, 2, ..., n$. If it is not new, the verifier discards the message M_i.
2) To ensure non-repudiation and avoid the confusion attack, the small exponent test [25] has been utilised in the batch verification phase. A vector composed of small random integers is used to investigate any modification on multiple signatures during batch verification. The verifier chooses $v = \{v_1, v_2, \ldots, v_n\}$, where v_i is randomly selected in $[1, 2^t]$, t is a very small integer which increases low computation overhead.

3) The verifier checks the following equation.

$$\left(\sum_{i=1}^{n} v_i{\cdot}\sigma_i\right)\cdot P = \left(\sum_{i=1}^{n}(v_i\cdot\alpha_i)\right)\cdot K_{pud} + \sum_{i=1}^{n}(v_i\cdot\beta_i\cdot ID_{i,1}) \quad (5)$$

If the above equation holds true, all the n messages are considered to be valid. Otherwise, some of the messages in the batch are invalid. The invalid message signature detection algorithm has been proposed in [26], detailing this algorithm is not within the scope of this paper.

Next, we analyse the correctness of the batch messages verification using equation Eq.(5). Due to $\mathrm{P}_{pub} = s\cdot\mathrm{P}$, $ID_{i,1} = r_i\cdot P$, $ID_{i,2} = RID_i \oplus H_1(r_i\cdot \mathrm{P}_{pub})$, $\alpha_i = H_2(ID_i||T_i)$, $S_i = \alpha_i\cdot k_d \bmod q$, $\beta_i = H_3(ID_i||M_i||T_i)$ and $\sigma_i = S_i + \beta_i\cdot r_i \bmod q$, we obtain

$$\begin{aligned}
&\left(\sum_{i=1}^{n} v_i{\cdot}\sigma_i\right)\cdot P = \left(\sum_{i=1}^{n} v_i{\cdot}(S_i+\beta_i\cdot r_i)\right)\cdot P\\
&= \left(\sum_{i=1}^{n} v_i{\cdot}(\alpha_i\cdot k_d+\beta_i\cdot r_i)\right)\cdot P\\
&= \sum_{i=1}^{n} v_i{\cdot}(\alpha_i\cdot k_d\cdot P+\beta_i\cdot r_i\cdot P)\\
&= \sum_{i=1}^{n}(v_i\cdot\alpha_i\cdot K_{pud}) + \sum_{i=1}^{n}(v_i\cdot\beta_i\cdot ID_{i,1})\\
&= \left(\sum_{i=1}^{n}(v_i\cdot\alpha_i)\right)\cdot K_{pud} + \sum_{i=1}^{n}(v_i\cdot\beta_i\cdot ID_{i,1})
\end{aligned} \quad (6)$$

E. Domain Key Updating

Domain key updating operation is performed when a vehicle joins or leaves the network. When a vehicle joins the VANET domain, it falls within the competence of the TA to securely communicate the new domain key to the domain members. Hence, the newly joined vehicle cannot listen the aforementioned communication and it preserves backward secrecy. Similarly, when a vehicle leaves from a domain, the TA must update the domain key in order to prevent using a new domain key for the old vehicle to ensure forward secrecy. Our proposed scheme characterises a simple domain key updating procedure when the domain membership changes. For instance, when a vehicle V_i leaves the domain, the TA has to perform the following process.

1) Subtract var_i from μ

$$\mu' = \mu - \mathrm{var}_i \quad (7)$$

2) Then, the TA must choose a new domain key k'_d and it should be multiplied by μ' to form the rekeying message as shown in (8).

$$\gamma'_d = k'_d \times \mu' \quad (8)$$

3) The domain key value of the TA broadcast update is delivered as a broadcast message. On receiving the updated domain key value, the existing vehicles in the domain can obtain k'_d by executing the modulo operation just once. From the received k'_d, vehicle V_i cannot compute the newly updated domain key k'_d since its secret key is not included in μ'.

- **Batch Leave**

When some vehicles intends to leave the domain D_y, the TA will begin to update the domain key. For instance, if the vehicles V_3, V_5, V_7 and V_9 are ready to leave the domain D_y, then TA will execute the below steps for updating the domain key.

1) Subtract var_3, var_5, var_7 and var_9 from μ

$$\mu' = \mu - (\mathrm{var}_3 + \mathrm{var}_5 + \mathrm{var}_7 + \mathrm{var}_9) \quad (9)$$

2) Then, the TA must choose a new domain key k'_d and it should be multiplied by μ' to form the rekeying message as shown in (10).

$$\gamma'_d = k'_d \times \mu' \quad (10)$$

3) The domain key value of the TA broadcast update is delivered as a broadcast message. On receiving the updated domain key value, existing vehicles in the domain obtains k'_d by excuting the modulo operation just once. From k'_d, the vehicle V_i cannot extract the newly updated domain key k'_d since its secret key is not included in μ'.

Thus, it can be concluded that, when 'n' vehicles are ready to leave the domain, the TA will execute $(\mathrm{n}-1)$ additions and one subtraction operation in order to update the domain key.

- **Batch Join**

When some vehicles intends to enter the domain D_y, the TA will perform some addition operations in order to update the domain key. For instance, if four vehicles V_3, V_5, V_7 and V_9 intends to join the domain D_y, then TA will execute the following steps to update the domain key.

1) Instead of computing x_i and y_i for all these vehicles, the TA takes the multiplied values of x_i and y_i from var_3, var_5, var_7 and var_9, which has been pre-computed in the initialisation phase.

$$\mu' = \mu + (var_3 + var_5 + var_7 + var_9) \quad (11)$$

2) Then, the TA chooses a new domain key k'_d and multiplies by μ' to form the rekeying message as shown in equation (10).
3) The domain key value of the TA broadcast update is delivered in a broadcast message. From the received γ'_d, the vehicles can obtain the newly updated domain key k'_d since var_i are included in μ' , based only on var_3, var_5, var_7 and var_9.

Thus, it can be concluded that, when 'n' vehicles try to enter the vehicle's multicast domain, the TA needs to execute 'n' additions in order to update the domain key, which cause $O(1)$ computation complexity for TA. Beyond that, the computational complexity of a multicast vehicle is also minimised by enabling every vehicle to execute the modulo division operation just once. In addition to this, the TA should only broadcast one message to the vehicles in the multicast domin.

IV. Security Proof and Analysis

This section demonstrates the efficiencies of our proposed PA-CRT scheme in satisfying the required secure requirements under the presumption that the Elliptic Curve Discrete Logarithm Problem (ECDLP) is difficult to solve.

A. Security Proof

Since the communication among the vehicular nodes and between vehicles and RSUs is based on wireless media in VANETs, the vulnerabilities of the communication channel to attackers and malicious users are always inevitable. To this end, this section demonstrates that our proposed identity-based scheme is secure against the adaptive chosen message attack.

Definition 5: A signature authentication protocol, under an adaptive selection message attack $(t, \varepsilon, q)-$ is unforgeable if no attacker (t, ε, q) is able to break it, where q is the number of H_2 hash queries to the random oracle.

Theorem 1. In the random oracle model, if an adversary A with probabilistic polynomial time executes the Game (**Definition 4**) and wins the game with the probability that the adversary cannot be ignored in the corresponding polynomial time, then the simulator with probabilistic polynomial time solve the ECDLP problem with a probability of no less than $\varepsilon' = \frac{\varepsilon}{q}$ in that polynomial time.

Proof. Suppose that the adversary A that can forge the message $(ID_i, M_i, T_i, \sigma_i)$. Now, another simulator B has been built based on A, so B characterise the ability to solve the ECDLP problem run by A as a subroutine with a noneligible probability. Given an instance sample $(G, P, Q = xP)$ of the ECDLP problem, B simulates oracles queried by A as follows.

Setup: The simulator B sets $Q = xP$ and selects a random number $r_i \in Z_q^*$ to construct a anonymous set $S_{ID} = \{ID_1, ID_2, \cdots, ID_{i^*}, \cdots, ID_n\}$, where $i^* \in \{1, 2, \cdots, n\}$.

$$ID_i = \begin{cases} ID_{1,i} = Q & if\ i = i^* \\ ID_{1,i} = r_i P & if\ i \neq i^* \end{cases} \tag{12}$$

The simulator B chooses any random number k_d, and computes its corresponding public key with $K_{pud} = k_d P$. Then B sends the public parameters $Params = (G, P, k_d P, H_1, H_2)$ and the anonymous set S_{ID} to A.

H_2 **hash query:** When the adversary A makes an H_2 query with pseudoidentity ID_i, B checks whether the tuple $\langle ID_i, T_i, \tau_{H_2}\rangle$ is already contained in the hash list L_{H_2} or not. If so, B sends $\tau_{H_2} = H_2(ID_i, T_i)$ to A. Otherwise, B chooses a random $\tau_{\mathrm{H}_2} \in Z_q^*$ and then adds $\langle ID_i, T_i, \tau_{H_2}\rangle$ into the hash listL_{H_2}. At last, B sends $\tau_{H_2} = H_2(ID_i, T_i)$ to A.

H_3 **hash query:** When adversary A makes an H_3 query with message $\langle M_i, ID_i, T_i, \tau_{\mathrm{H}_2}\rangle$, B checks whether the tuple $\langle M_i, ID_i, T_i\rangle$ is already contained in the hash list L_{H_3}. If so, B sends $\tau_{H_3} = H_3(M_i, ID_i, T_i)$ to A. Otherwise, B chooses a random $\tau_{\mathrm{H}_3} \in Z_q^*$ and then adds $\langle M_i, ID_i, T_i, \tau_{\mathrm{H}_2}\rangle$ into the hash list L_{H_3} . At last, B sends $\tau_{H_3} = H_3(M_i, ID_i, T_i)$ to A.

Sign query: When the adversary A makes a signing query on the message M_i and ID_i, B first checks the tuple value $\langle ID_i, T_i, \tau_{H_2}\rangle$ from the hash list L_{H_2}. Then, B retrieves τ_{H_2} from the tuple $\langle ID_i, T_i, \tau_{H_2}\rangle$.

If $i = i*$, B chooses three random numbers $\sigma_i, \alpha_i, \beta_i \in Z_q^*$, a random point ID_i, and calculates $ID_{i,1} = \beta_i^{-1}(\sigma_i \cdot P - \alpha_i \cdot K_{pud})$. B adds $\tau_{H_2} = H_2(ID_i, T_i)$ and $\tau_{H_3} = H_3(M_i, ID_i, T_i)$ to the list L_{H_3} and L_{H_3} respectively, then sends $(M_i, ID_i, T_i, \sigma_i)$ to A. According to the rules of the game,all responses to the Sign query are valid because $(M_i, ID_i, T_i, \sigma_i)$ has been answered in the game and can satisfy the following.

$$\begin{aligned} &\sigma_i \cdot P = \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1} \\ &= \alpha_i \cdot K_{pud} + \beta_i \cdot \left(\beta_i^{-1}(\sigma_i \cdot P - \alpha_i \cdot K_{pud})\right) \\ &= \alpha_i \cdot K_{pud} + \sigma_i \cdot P - \alpha_i \cdot K_{pud} = \sigma_i \cdot P \end{aligned} \tag{13}$$

Otherwise, if $i \neq i*$, B has a valid signature and outputs a valid signature directly.

Output: A communicates with B until A realises that the process has been completed. A outputs the message $\{M_{\mathrm{i}}, ID_{\mathrm{i}}, T_{\mathrm{i}}, \sigma_i\}$. B checks whether the equation holds true or not.

$$\sigma_i \cdot P = \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1} \tag{14}$$

If not, B will abort the process. By using the forgery lemma [43], A could output another valid message $\{M_{\mathrm{i}}, ID_{\mathrm{i}}, T_{\mathrm{i}}, \sigma_i^*\}$ within a polynomial time, if it chooses another H_2, where $\alpha_i \neq \alpha_i^*$. Hence we can get:

$$\sigma_i^* \cdot P = \alpha_i^* \cdot K_{pud} + \beta_i \cdot ID_{i,1} \tag{15}$$

According to equation (14) and (15), we can deduce the following:

$$\begin{aligned} &(\sigma_i - \sigma_i^*) \cdot P = \sigma_i \cdot P - \sigma_i^* \cdot P \\ &= \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1} - \\ &(\alpha_i^* \cdot K_{pud} + \beta_i \cdot ID_{i,1}) \\ &= (\alpha_i - \alpha_i^*) \cdot K_{pud} \\ &= (\alpha_i - \alpha_i^*) \cdot k_d \cdot P \end{aligned} \tag{16}$$

Now, B outputs $(\alpha_i - \alpha_i^*)^{-1}(\sigma_i - \sigma_i^*)$ as a solution for the given instance of the ECDLP problem. Otherwise the simulation is terminated.

Based on the above simulation, correct answer to the ECDLP problem can be ensured depending on whether the following events occur simultaneously:

- Event $E1$: Adversary A returns a valid signature forgery.
- Event $E2$: Adversary A can forge a pseudoidentity $ID_i \neq ID_{i^*}$.

Due to $\Pr[E_1] = \varepsilon$, $\Pr[E_2] = \frac{1}{q}$, we obtain

$$\Pr[E_1 E_2] = \Pr[E_1]\Pr[E_2] = \varepsilon \cdot {}^1\!/_q = {}^\varepsilon\!/_q. \tag{17}$$

Next, we show that B can solve the given instance of the ECDLP problem with advantage $Adv_B == {}^\varepsilon\!/_q$.

As a result, the simulator B calculates x in a polynomial time with an ignorable the advantage of ${}^\varepsilon\!/_q$, namely, the solution of the ECDLP problem, that is **Theorem 1** is satisfied. However, it is difficult to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) within a shorter time. Therefore, under the random oracle model, our proposed PA-CRT scheme is secure against forgery under the adaptive chosen message attack.

B. Security Analysis

This section presents an analysis on various security features of our proposed scheme.

1) Message integrity and authentication: According to the proof of security in the previous section, if the ECDLP problem is difficult to solve, then no adversary can create legitimate messages in a given polynomial time. Therefore, as long as the message and signature satisfies the equation $\sigma_i \cdot P = \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1}$, the scheme can guarantee authentication and message integrity.

2) Identity privacy preserving: Suppose that vehicle V_i broadcasts message $\langle M_i, ID_i, T_i, \sigma_i \rangle$ to other vehicles in the network, where $ID_{i1} = r_i P$, $ID_{i2} = RID_i \oplus H_1(r_i \cdot P_{pub})$. In order to retrieve V_i's real identity, the adversary must calculate $RID_i = ID_{i2} \oplus H_1(r_i \cdot s \cdot P)$. However, t_i is stored in TA, r_i is a random number, so that the adversary cannot obtain RID, due to the complexities of the Computational Diffie Hellman (CDH) problem. Thus, even if the pseudo identity ID_i is disclosed, the adversary will be unable to achieve the user's identity privacy.

3) Perfect backward secrecy: When old domain vehicles obtains the newly updated domain key k_d, adversaries might intend to access any one of the domain vehicles private key sk_i. Moreover, the private keys are randomly chosen from a large set of positive integers with respect to the multiplicative group z_p^*. Because of this property, adversary cannot compute any other vehicle's secret key. Therefore, the adversary cannot access the communication sent prior to their entry into the domain, thus the proposed scheme satisfies the backward secrecy requirement.

4) Perfect forward secrecy: In the proposed algorithm, an adversary cannot compute the current domain key k_d after leaving the domain, as discussed earlier in the backward secrecy technique. After a vehicle V_i leaves the domain, TA subtracts its share value, which is the multiplication of x_i and y_i, and extracts var_i from μ to produce μ'. The rekeying message γ_d' is formed from the product of updated μ' and newly generated domain key value k_d'. It is feasible for a vehicle to obtain the new domain key even after they leave the domain, since the personal keying information is not included. Such vehicles might obtain k_d' from the rekeying value, which is infeasible to be sent as a broadcast message from TA. Therefore, the vehicle has to multiply its private key value with the numbers from 1 to q, where q is the maximum domain key value. At a certain point, the vehicle will define a value $\vartheta = \gamma'$ (i.e. $sk_i \times \omega = \vartheta$). On receiving this ω value, vehicle V_i can obtain a series of number S, which will divide the number ω. So the set of numbers $\{\omega \bmod 1, \omega \bmod 2, ..., \omega \bmod \omega\} = 0$ represent the value of S. In this serious of numbers, the number $k_d' \in S$ is included in the newly generated domain key k_d'. For this case, we assume that the size of sk_i is ω bits, then the attacker should perform 2ω multiplication. Due to this reason, deriving k_d' by choosing a large sk_i value for each vehicle's secret key incurs significant computation time. Now, the size of sk_i is set as 1024 bits, which has been previously set to 128, 256 and 512 bits. In order to obtain the set of S values that divides the number ω, the attacker (after leaving the domain) can use brute force attack further to access the new domain key by selecting exploiting values from the set S. If this attempt requires 1μs, then then total time would be $2^{S-1}\mu$s. Therefore an adversary cannot obtain the domain key for the purpose of accessing to the current communication, which implies that our proposed algorithm satisfies the forward secrecy requirement.

5) Traceability: TA can extract the vehicle's real identity from the received pseudo identity ID_i that contains two parts $-$ $ID_{i,1}$ and $ID_{i,2}$ where $ID_{i,1} = r_i \cdot P$ and $ID_{i,2} = RID_i \oplus H_1(r_i \cdot \mathrm{P}_{pub})$. TA uses the master secret s, and computes

$$\begin{aligned} RID_i &= ID_{i,2} \oplus H_1(r_i \cdot \mathrm{P}_{pub}) \\ &= ID_{i,2} \oplus H_1(r_i \cdot s \cdot \mathrm{P}) \\ &= ID_{i,2} \oplus H_1(s \cdot ID_{i,1}). \end{aligned} \tag{18}$$

Besides, we are not using traditional user's real identity RID and password PWD devices. Instead, our proposed scheme uses Fingerprints for identity verification, so that a given user's identity can be accurately traced out through the Fingerprint. Therefore, TA can trace vehicles based on its any disputed signature.

6) Un-linkability: A pseudo identity ID_i is used for generating the message signature. In our scheme, the random number used in the identity verification process is not repeated, and each pseudo identity of each signature is unique. Thus, no adversary could relate with any number of signatures sent by the same vehicle. Thus, our proposed scheme supports unlinkability.

7) Resistance to impersonation attack: To impersonate a vehicle to other vehicles or RSUs, the adversary must generate a valid message $\{M_{\mathrm{i}}, ID_{\mathrm{i}}, T_{\mathrm{i}}, \sigma_i^*\}$ satisfying the equation $\sigma_i \cdot P = \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1}$. According to Theorem 1, it is evident that no polynomial adversary can forge a valid message. Therefore, the proposed PA-CRT scheme for VANETs can withstand the impersonation attack.

8) Resistance to modification attack: According to Theorem 1, we know that any modification of the message $\{M_{\mathrm{i}}, ID_{\mathrm{i}}, T_{\mathrm{i}}, \sigma_i^*\}$ could be identified by checking whether the equation $\sigma_i \cdot P = \alpha_i \cdot K_{pud} + \beta_i \cdot ID_{i,1}$ holds true or not. Therefore, the proposed PA-CRT scheme for VANETs can withstand the modification attack.

9) Resistance to replay attack: The proposed PA-CRT scheme adopts the current timestamp T to compute the message signature $\sigma_i = S_i + \beta_i \cdot r_i \bmod q$, where $\alpha_i = H_2(ID_i || T_i)$ and $\beta_i = H_3(ID_i || M_i || T_i)$. Therefore, the timestamp T_i is included in the signature and the proposed scheme can withstand replay attacks.

10) Resistance to collusion attack: Collusion attack means that several adversaries collude with each other to extract the secret key. Specifically, the adversaries cooperatively calculate the updated domain key after leaving the domain. Owing to the fact that the value of var_i is subtracted from μ, several prior vehicle cannot collude to access the updated domain key k_d since the used pairwise relative prime number is sufficiently large. Assume a scenario which has two adversaries, adversary A has obtained the key values sk_1, k_d, and adversary B has obtained the key values sk_3 and k_d at time '$t-2$'. At time '$t-1$', the adversary A leaves the domain with two key values, which are sk_1 and k_d. At the time 't', the adversary B receives the rekeying message r_g from TA, and then calculates k_d. At time '$t+1$', the adversary B leaves the domain with the two key values sk_3 and k_d. Now adversaries A and B

could exchange the keys sk_1, k_d, sk_3 and k_d. However, they still cannot collude to obtain the updated domain key k_d broadcasted at time 't+2' because var_1 and var_3 are excluded from μ. Thus, the proposed PA-CRT scheme for VANETs can withstand the collusion attack.

V. Performance analysis and comparison

This section demonstrates the efficiencies of our proposed PA-CRT against existing schemes [19], [20], [22], [25], [32], [35] in terms of the computation and communication overhead.

We construct the bilinear pairing on 80 bits security level, as $\overline{e} : G_1 \times G_1 \rightarrow G_T$, where G_1 is an additive group which is generated on a super singular elliptic curve $\overline{E} : y^2 = x^3 + x \bmod \overline{p}$ with embedding degree 2. We construct the elliptic curve on 80 bits security level as: G is an additive group generated on a non-singular elliptic curve $E : y^2 = x^3 + ax + b(\bmod p)$ with order q, where p, q are two 160 bits prime number and $a, b \in Z_p^*$.

A. Computation Cost Analysis and Comparison

This section analyses the computation overheads of our proposed scheme against a few existing schemes. We compute the execution time of basic cryptographic operations using the MIRACL library [44]. For ease of comparison between the analysed methods, we employ the same execution time as in the He et al. scheme [20], as shown in Table II. Besides, some notations about execution time are defined as follows:

TABLE II
Execution time of several cryptographic operations

Cryptographic operation	Time (ms)
T_{bp}	4.2110
$T_{bp \cdot m}$	1.7090
$T_{bp \cdot sm}$	0.0535
$T_{bp \cdot a}$	0.0071
T_{mtp}	4.406
$T_{e \cdot m}$	0.4420
$T_{e \cdot sm}$	0.0138
$T_{e \cdot a}$	0.0018
T_h	0.0001

- T_{bp}: The excution time of the bilinear pairing operation $\overline{e}(P, Q)$, where $\overline{P}, \overline{Q} \in G_1$;
- $T_{bp \cdot m}$: The time to execute the scale multiplication operation $x \cdot \overline{P}$ which is related to bilinear pairing, where $\overline{P} \in G_1$ and $x \in Z_{\overline{q}}^*$;
- $T_{bp \cdot sm}$: The time to execute a small scale multiplication operation $v_i \cdot \overline{P}$ which is related to bilinear pairing, where $\overline{P} \in G_1$, $v_i \in [1, 2^t]$ is a small random integer, and t is a small integer;
- $T_{bp \cdot a}$: The time to execute the point addition operation $\overline{P} + \overline{Q}$ which is related to bilinear pairing, where $\overline{P}, \overline{Q} \in G_1$;
- T_{mtp}: The time to execute the MapToPoint;
- $T_{e \cdot m}$: The time to execute the scale multiplication operation $x \cdot P$ which is related to elliptic curve, where $P \in G$ and $x \in Z_q^*$;
- $T_{e \cdot sm}$: The time to execute the small scale multiplication operation $v_i \cdot P$ useing the small exponent test technology, where $P \in G$, $v_i \in [1, 2^t]$, and t is a small integer;
- $T_{e \cdot a}$: The time to execute the point addition operation $P + Q$ which is related to elliptic curve, where $P, Q \in G$;
- T_h: The time to execute a secure hash operation.

AIDM denotes the anonymous identity generation and message signing, SVOM denotes the single verification of one message, BVMM denotes the batch verification of multiple messages phases. Table III lists the comparison of the computation overhead between several related schemes and our proposed scheme.

TABLE III
Computation cost of seven authentication schemes

	AIDM	SVOM	BVMM
Horng et al. [25]	$4T_{bp.m} + 1T_{bp.a} + 2T_{mtp} + 1T_h \approx 15.6552ms$	$2T_{bp} + 2T_{bp.m} + 1T_{bp.a} + 1T_{mtp} + 1T_h \approx 16.2532ms$	$2T_{bp} + 2nT_{bp.m} + nT_{bp.a} + nT_{mtp} + nT_h \approx 7.8312n + 8.422ms$
Bayat et al. [19]	$5T_{bp.m} + 1T_{bp.a} + 1T_{mtp} + 2T_h \approx 12.9583ms$	$3T_{bp} + 1T_{bp.m} + 1T_{mtp} + 1T_h \approx 18.7481ms$	$3T_{bp} + nT_{bp.m} + (3n-3)T_{bp.a} + nT_{mtp} + nT_h \approx 6.1364n + 12.6117ms$
Shim et al. [32]	$3T_{bp.m} + 2T_{bp.a} + 1T_h \approx 5.1413ms$	$3T_{bp} + 2T_{bp.m} + 1T_{bp.a} + 2T_h \approx 16.0583ms$	$3T_{bp} + (n+1)T_{bp.m} + (3n-3)T_{bp.a} + (2n)T_h \approx 1.7035n + 14.3207ms$
Malhi et al. [22]	$4T_{bp.m} + 2T_{bp.a} + 2T_h \approx 6.8504ms$	$3T_{bp} + 3T_{bp.m} + 1T_{bp.a} + 2T_h \approx 17.7673ms$	$3T_{bp} + (3n)T_{bp.m} + nT_{bp.a} + (3n)T_h \approx 5.1344n + 12.633ms$
He et al. [20]	$3T_{e.m} + 3T_h \approx 1.3263ms$	$3T_{e.m} + 2T_{e.a} + 2T_h \approx 1.3298ms$	$(n+2)T_{e.m} + (3n-1)T_{e.a} + 2nT_{e.sm} + 2nT_h \approx 0.4752n + 0.8822ms$
Wu et al. [35]	$2T_{e.m} + 2T_h \approx 0.8842ms$	$3T_{e.m} + 2T_{e.a} + 2T_h \approx 1.3298ms$	$(2n+2)T_{e.m} + (2n)T_{e.a} + (2n)T_h \approx 0.8878n + 0.884ms$
The proposed	$2T_{e.m} + 2T_h \approx 0.8842ms$	$3T_{e.m} + 2T_{e.a} + 1T_h \approx 1.3297ms$	$(n+2)T_{e.m} + nT_{e.sm} + nT_{e.a} + (2n)T_h \approx 0.4578n + 0.884ms$

We conduct a detailed analysis on Horng et al.'s scheme [25], in order to investigate the bilinear pairing characteristics in VANETs [19], [22], [25], [32]. In Horng et al.'s scheme [25], the computation of AIDM requires four scalar multiplication operations, one point addition operation, two MapToPoint operations and one hash operation. Thus, the total computation cost of this step is $4T_{bp \cdot m} + 1T_{bp.a} + 2T_{mtp} + 1T_h \approx 15.6552$ms. The computation of SVOM involves two bilinear pairing operations, two scalar multiplication operations, one point addition operation, one MapToPoint operation and one hash operation. Thus the total computation cost of this step is $2T_{bp} + 2T_{bp \cdot m} + 1T_{bp.a} + 1T_{mtp} + 1T_h \approx 16.2532ms$. The computation of BVMM requires two bilinear pairing operations, $2n$ scalar multiplication operations, n point addition operations, n MapToPoint operations and n hash operations. Thus, the total computation cost of this step is $2T_{bp} + 2nT_{bp \cdot m} + nT_{bp \cdot a} + nT_{mtp} + nT_h \approx (7.8312n + 8.422)ms$.

We conduct a detailed analysis of the proposed scheme to depict the ECC-based characteristic efficiency in VANETs [20], [35]. The computation of AIDM requires two scalar multiplication operations and two hash operations. Thus the total computation overhead is $2T_{e \cdot m} + 2T_h \approx 0.8842ms$. The computation of SVOM requires three scalar multiplication operations, two point addition operation and one hash operation. Thus the total computation overhead of this step is $3T_{e \cdot m} + 2T_{e \cdot a} + 1T_h \approx 1.3297ms$. The computation of BVMM requires $(n+2)$ scalar multiplication operations, n small scalar

multiplication operations, n point addition operations and $2n$ hash operations. Thus the computation overhead of this step is $n+2)T_{e\cdot m}+nT_{e\cdot sm}+nT_{e\cdot a}+2nT_h \approx (0.4578n+0.884)ms$.

From Table III it is evident that the cost of an anonymous identity generation and a single message signing in the proposed scheme only characterises 0.8842ms, while the cost of generating AIDM in Horng et al [25], Bayat et al [19], Shim et al [32], Malhi et al [22], He et al [20] and Wu et al [35] schemes characterises 15.6552, 12.9583, 5.1413, 6.8504, 1.3263 and 0.8842, respectively.

In order to highlight the benefits of the proposed PA-CRT scheme in the single message verification process, we compare the execution times of single verification in the proposed scheme with six state-of-art schemes [19], [20], [22], [25], [32], [35], as shown in Fig. 5. Based on the results shown in Table III and Fig. 5, the proposed PA-CRT scheme for VANET characterises lower computation overhead than the six state-of-art schemes for VANETs.

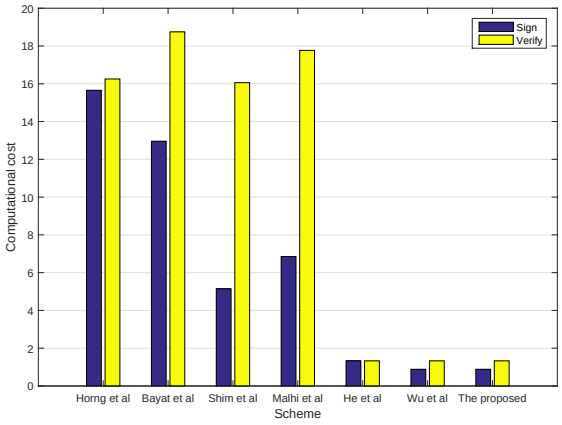


Fig. 5. Computation overhead to sign and verify one message.

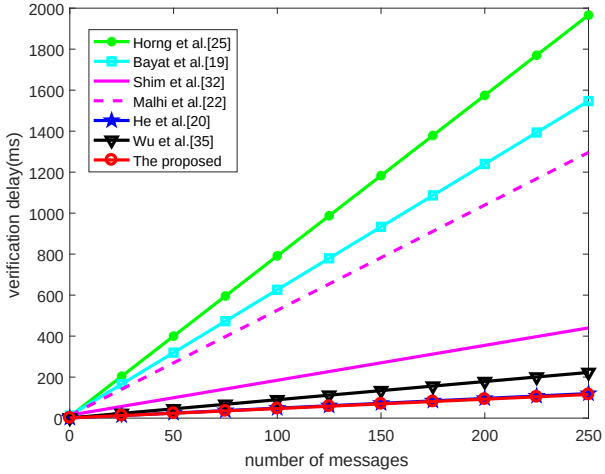


Fig. 6. Verification delay of batch verification versus the amount of messages.

Fig. 6 illustrates the delay incurred in the batch verification process, for different number of messages in the batch. For 250 messages in the batch, the verification delay is witnessed at 1966, 1547, 440, 1296, 120, 223 and 115 ms respectively for Horng et al.'s scheme [25], Bayat et al.'s scheme [19], Shim et al.'s scheme [32], Malhi et al.'s scheme [22], He et al.'s scheme [20], Wu et al.'s scheme [35] scheme and the proposed PA-CRT scheme, respectively. Thus, the proposed scheme is more efficient than the others schemes in batch verification phase when the traffic load increases.

The result of the computation costs of the analysed five schemes is listed in Table III. As shown in Table III, the computation overhead of AIDM of our proposed scheme is 5.1413 ms, which decreases by $(15.6552-0.8842)/15.6552 \approx 94.35\%$, $(12.9583-0.8842)/12.9583 \approx 93.18\%$, $(5.1413-0.8842)/5.1413 \approx 82.80\%$, $(6.8504-0.8842)/6.8504 \approx 87.09\%$, $(1.3263-0.8842)/1.3263 \approx 33.33\%$ and $(0.8842-0.8842)/0.8842 \approx 0\%$ respectively, against Horng et al.'s scheme [25], Bayat et al.'s scheme [19], Shim et al.'s scheme [32], Malhi et al.'s scheme [22], He et al.'s scheme [20], Wu et al.'s scheme [35] scheme. The performance of our proposed scheme against the other compared schemes in terms of AIDM, SVOM and BVMM are presented in Table IV.

TABLE IV
THE COMPUTATION OVERHEAD COMPARISON

Scheme	AIDM	SVOM	BVMM(50 messages)
Horng et al. [25]	94.35%	91.82%	94.06%
Bayat et al. [19]	93.18%	92.91%	92.56%
Shim et al. [32]	82.80%	91.72%	76.10%
Malhi et al. [22]	87.09%	92.52%	91.17%
He et al. [20]	33.33%	0.01%	3.52%
Wu et al. [35]	0	0.01%	47.79%

B. Communication Overhead Analysis and Comparison

This section focuses on the communication overhead introduced by the pseudo identity, signature and timestamp. As mentioned earlier, the size of $\bar{p}$ is 64 bytes and the size of p is 20 bytes, hence the size of the elements in G_1 is 128 bytes and the size of elements in G is 40 bytes. In addition, the size of output of a hash function and timestamp are 20 bytes and 4 bytes, respectively. Since the traffic related information is the same in all of the schemes, it is appropriate to analyse the size of the signature. The communication overhead of several schemes is listed in Table V.

TABLE V
SIZE OF COMMUNICATION OVERHEAD

Scheme	Sending one message	Sending n messages
Horng et al. [25]	384 bytes	384n bytes
Bayat et al. [19]	388 bytes	388n bytes
Shim et al. [32]	644 bytes	644n bytes
Malhi et al. [22]	516 bytes	516n bytes
He et al. [20]	144 bytes	144n bytes
Wu et al. [35]	148 bytes	148n bytes
Our proposed	84 bytes	84n bytes

The size of single message excluding (ID_i, σ_i) of Horng et al. [25] is $128 \times 3 = 384$ bytes, which includes three

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2019.2904274, IEEE Transactions on Dependable and Secure Computing

elements in G_1 $(ID_{i1}, ID_{i2}, \sigma_i \in G_1, 128 \times 3 = 384$ bytes), where $ID_i = (ID_{i1}, ID_{i2})$. The size of single message excluding (ID_i, T_i, U_i) of Bayat et al. [19] is $128 \times 3 + 4 = 388$ bytes, which includes three elements in G_1 $(ID_{i1}, ID_{i2}, U_i \in G_1, 128 \times 3 = 384$ bytes) and one timestamp ($T_i, 4$ bytes), where $ID_i = (ID_{i1}, ID_{i2})$. The size of single message excluding $\{ID_i, T_i, U_i, V_i, W_i\}$ of Shim et al. [32] is $128 \times 5 + 4 = 644$ bytes, which includes five elements in G_1 $(ID_{i1}, ID_{i2}, U_i, V_i, W_i \in G_1, 128 \times 5 = 640$ bytes) and one timestamp ($T_i, 4$ bytes), where $ID_i = (ID_{i1}, ID_{i2})$. The size of single message excluding $\{M_i, PSI, P_{v_i}, U_i, V_i\}$ of Malhi et al. [22] is $128 \times 4 + 4 = 516$ bytes, which includes four elements in G_1 $(PSI, P_{v_i}, U_i, V_i \in G_1, 128 \times 4 = 512$ bytes) and one timestamp ($T_i, 4$ bytes). The size of single message excluding $(ID_i, R_i, \sigma_i, T_i)$ of He et al. [20] is $40 \times 3 + 20 \times 1 + 4 \times 1 = 144$ bytes, which includes three elements in G $(ID_{i1}, ID_{i2}, R_i \in G_1, 40 \times 3 = 120$ bytes), one hash function's output ($\sigma_i \in {Z_q}^*, 20$ bytes) and one timestamp ($T_i, 4$ bytes), where $ID_i = (ID_{i1}, ID_{i2})$. The size of single message excluding $\{M_i, ID_{v_i}, T_{v_i}, T_i, R_i, h_{k_i}, \delta_i\}$ of Wu et al. [35] is $40 \times 3 + 20 \times 1 + 4 \times 2 = 148$ bytes, which includes three elements in G $(ID_{v_i}, R_i, h_{k_i} \in G_1, 40 \times 3 = 120$ bytes), one hash function's output ($\delta_i \in {Z_q}^*, 20$ bytes) and one timestamp ($T_{v_i}, T_i, 4 \times 2 = 8$ bytes). The size of single message excluding of our proposed scheme is $40 \times 1 + 20 \times 2 + 4 \times 1 = 84$ bytes, which includes one element in G $(ID_{i1} \in G_1, 40$ bytes), two hash function's output $(ID_{i2}, \sigma_i \in {Z_q}^*, 20 \times 2 = 40$ bytes) and one timestamp ($T_i, 4$ bytes), where $ID_i = (ID_{i1}, ID_{i2})$. Thus, from the above analysis it is clearly evident that our proposed PA-CRT scheme characterise a lower communication overhead.

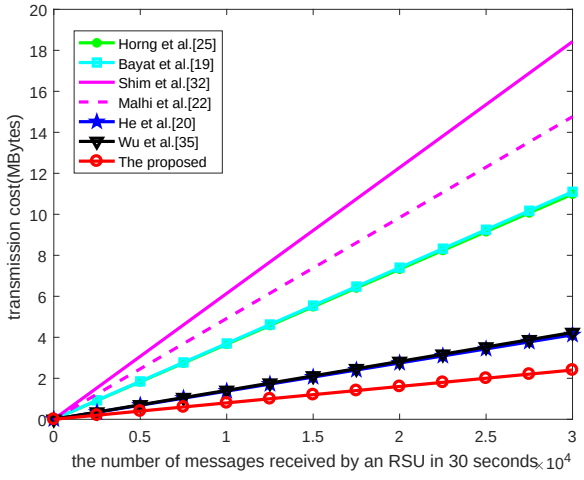


Fig. 7. Number of messages received by an RSU in 30 s versus the transmission cost.

The transmission cost of the studied techniques has been analysed in a network comprising 100 vehicles in a single RSU range. From Fig. 7, it is obvious that the transmission overhead increases linearly with an increasing number of messages received by an RSU within a period of 30s. It can be observed that the transmission overhead of our proposed scheme is better than 21.88 percent to that of Horng et al.'s scheme [25], 21.65 percent to that of Bayat et al.'s scheme [19], 13.04 percent to that of Shim et al.'s scheme [32], 16.28 percent to that of Malhi et al.'s scheme [22], 58.33 percent to that of He et al.'s scheme [20] and 56.76 percent to that of Wu et al.'s scheme [35] respectively. Furthermore, our proposed scheme can save bandwidth consumption up to a level of 8.58MB, 8.70 MB, 16.02 MB, 12.36MB, 1.72 MB and 1.83MB to that of Horng et al.'s scheme [25], Bayat et al.'s scheme [19], Shim et al.'s scheme [32], Malhi et al.'s scheme [22], He et al.'s scheme [20] and Wu et al.'s scheme [35] respectively, when the number of the messages received by an RSU reaches 30000 within period of 30s.

C. TA Serving Rate

When a vehicle leaves the coverage range of a domain D_y, TA needs to update the domain key in order to prevent old vehicles from accessing the new domain key, which ensures forward secrecy. When a vehicle enters into the range of domain D_y, TA will perform some addition operations in order to update the domain key.

Let T_{gen} denote the time required for one TA to generate the domain key and the domain public key for m DOMAIN message. To calculate the TA serving rate, we first estimate the time required for one TA to generate the domain key and the domain public key for m DOMAIN message. In the proposed scheme, the time required for one TA to generate the domain key and the domain public key for one DOMAIN message is as follows:

$$T_{gen} = T_{e.m} = 0.442ms. \tag{19}$$

Let v denotes the average speed of a vehicle that varies from 5m/s to 10m/s (or 18km/h to 36km/h), and d denotes the communication range of a domain which is considered to be 1000 m and N denotes the density of vehicles that varies from 600 to 800 for a city road highway. Let p^* denotes the probability of vehicles to successfully receive the DOMAIN messages from TA.

Therefore, the TA serving rate r_{ser} can be calculated as

$$r_{ser} = \frac{p^* \cdot d}{v \cdot T_{gen} \cdot N} \tag{20}$$

Fig. 8 shows the serving rate r_{ser} for various vehicle density N and various average speed v between a vehicle and the TA, for a TA range $d = 1000m$.

From Fig. 8, it can be observed that the serving rate r_{ser} of the TA gradually decreases when both the vehicle speed v and vehicle density N increases. In addition, it is evident that the TA can effectively generate 679 DOMAIN messages for every 300ms. Therefore, it can be concluded that our proposed scheme characterises a lower range of message loss with an increase in the number of vehicles in the communication domain.

VI. Conclusion

This paper proposed a Chinese remainder theorem-based conditional privacy-preserving authentication scheme for securing communications in VANETs. To reduce the probability

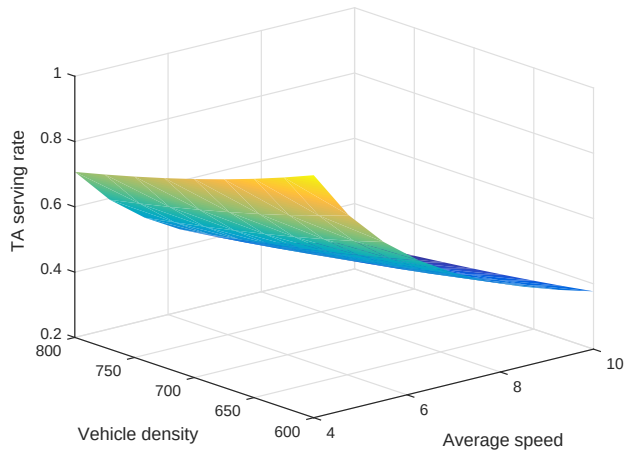


Fig. 8. TA serving rate for various vehicle density and various average speed of vehicles.

of personal information including real identity and password being compromised, this paper proposed a scheme using fingerprints instead of real identity and password for identity verification. The proposed scheme eliminates the need for using an ideal TPD, thus avoids the risk of compromising a vehicle's TPD leading to entire system failure. Security analysis proved that the proposed PA-CRT signature scheme is secure under the random oracle model. Besides, the use of the Chinese remainder theorem has been proven to improve transmission efficiency. Furthermore, the proposed scheme characterise an effective signature verification mechanism due to the use of elliptic curve instead of bilinear pairing. The performance analysis demonstrated the effectiveness of our proposed scheme against the compared existing schemes, which further exhibited the likelihood of our proposed scheme for real-life VANETs deployments. We plan to explore enhancing the security and user privacy in a more dynamic environment comprising 5G network base station, driver handheld devices etc.

REFERENCES

[1] J. J. Cheng, J. L. Cheng, M. C. Zhou, F. Q. Liu, S. C. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[2] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[3] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 ghz dsrc-based vehicular safety communication," *IEEE Wireless Communications*, vol. 13, no. 5, 2006.

[4] A. Boukerche, H. A. Oliveira, E. F. Nakamura, and A. A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," *Computer communications*, vol. 31, no. 12, pp. 2838–2849, 2008.

[5] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[6] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET communications*, vol. 4, no. 7, pp. 894–903, 2010.

[7] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[8] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

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

[10] J. Xu, D. Zhang, L. Liu, and X. Li, "Dynamic authentication for cross-realm soa-based business processes," *IEEE Transactions on Services Computing*, vol. 5, no. 1, pp. 20–32, 2012.

[11] L. Liu, N. Antonopoulos, M. Zheng, Y. Zhan, and Z. Ding, "A socioecological model for advanced service discovery in machine-to-machine communication networks," *Acm Transactions on Embedded Computing Systems*, vol. 15, no. 2, pp. 1–26, 2016.

[12] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *Communications Magazine IEEE*, vol. 46, no. 4, pp. 108–114, 2008.

[13] J. Kang, Y. Elmehdwi, and D. Lin, "Slim: Secure and lightweight identity management in vanets with minimum infrastructure reliance," in *International Conference on Security and Privacy in Communication Systems*, 2017, pp. 823–837.

[14] J. Li, H. Lu, and M. Guizani, "Acpn: A novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel & Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[15] J. Kang, D. Lin, W. Jiang, and E. Bertino, "Highly efficient randomized authentication in vanets," *Pervasive & Mobile Computing*, vol. 44, pp. 31–44, 2018.

[16] H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey," *Wireless Communications & Mobile Computing*, vol. 16, no. 6, pp. 643–655, 2016.

[17] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 1229–1237.

[18] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

[19] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," *Wireless networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

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

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

[22] A. Malhi and S. Batra, *Privacy-preserving authentication framework using bloom filter for secure vehicular communications*. Springer-Verlag, 2016.

[23] G. Kumaresan and T. A. Macriga, "Group key authentication scheme for vanet intrusion detection (gkavin)," *Wireless Networks*, vol. 23, no. 3, pp. 1–11, 2016.

[24] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Specs: Secure and privacy enhancing communications schemes for vanets," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011.

[25] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-specs+: Batch verification for secure pseudonymous authentication in vanet," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[26] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 283–10 295, 2017.

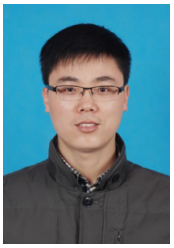
[27] A. Wasef, Y. Jiang, and X. Shen, "Ecmv: efficient certificate management scheme for vehicular networks," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–5.

[28] M. McGurrin, K. Gay *et al.*, "Usdot guidance summary for connected vehicle pilot site deployments: security operational concept," United States. Dept. of Transportation. ITS Joint Program Office, Tech. Rep., 2016.

[29] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[30] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in vanets," *Computer Communications*, vol. 71, pp. 50–60, 2015.
[31] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 246–250.
[32] K.-A. Shim, "Cpas: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.
[33] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.
[34] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on hmac for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.
[35] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *International Journal of Distributed Sensor Networks,13,3(2017-3-01)*, vol. 13, no. 3, p. 155014771770089, 2017.
[36] X. Zheng, C.-T. Huang, and M. Matthews, "Chinese remainder theorem based group key management," in *Proceedings of the 45th annual southeast regional conference*. ACM, 2007, pp. 266–271.
[37] J. Zhou and Y.-h. Ou, "Key tree and chinese remainder theorem based group key distribution scheme," in *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2009, pp. 254–265.
[38] P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralised group key management for secure multicast communication," *IET information Security*, vol. 8, no. 3, pp. 179–187, 2014.
[39] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1985, pp. 417–426.
[40] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.
[41] S. H. Islam and G. P. Biswas, "A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks," *annals of telecommunications - annales des tlcommunications*, vol. 67, no. 11-12, pp. 547–558, 2012.
[42] J. M. De Fuentes, "Overview of security issues in vehicular ad-hoc networks,," *Handbook of Reseach on Mobility & Computing*, 2010.
[43] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of cryptology*, vol. 13, no. 3, pp. 361–396, 2000.
[44] E. Wenger and M. Werner, "Evaluating 16-bit processors for elliptic curve cryptography," in *International Conference on Smart Card Research and Advanced Applications*, 2011, pp. 166–181.

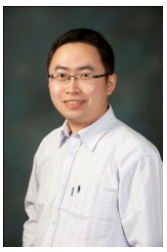
Jing Zhang is now a Ph.D. student in the School of Computer Science and Technology, Anhui University. Her research interest is vehicle ad hoc network.



Jie Cui received the Ph.D. degree in Computer Science and Technology from University of Science and Technology, China in 2012. He is currently an Associate Professor with the School of Computer Science and Technology, Anhui University, China. He has published over 50 papers. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, and software-defined networking (SDN).

Hong Zhong is a Professor (from 2009) and the Dean of the School of Computer Science and Technology, Anhui University, China. She received Ph.D. degree in University of Science and Technology of China in 2005. She has published over 100 papers. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, and software-defined networking (SDN).

Zhili Chen was born in Fujian Province, China, in 1980. He received his PhD degree in computer science from University of Science and Technology of China in 2009. He is currently a professor and Ph.D. supervisor of School of computer science and technology at Anhui University. He has published more than 40 papers. His main research interests include privacy preservation, secure multiparty computation, information hiding, spectrum auction and game theory in wireless communications.



Lu Liu is the Professor of Distributed Computing in the University of Derby, United Kingdom. Prof Liu received the Ph.D. degree from University of Surrey, UK (funded by DIF DTC) and MSc in Data Communication Systems from Brunel University, UK. Prof Liu's research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society (BCS).