B-DSPA: A Blockchain-based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad-hoc Networks

Qi Tao,Hongwei Ding,Tian Jiang,Xiaohui Cui, *Senior Member, IEEE,*

***Abstract*—The big data of Internet of vehicles contributes to the development of intelligent transportation. Privacy protection in Vehicular Ad-hoc Networks(VANETs) is the core factor to improve user and vehicle participation. This paper proposes a novel blockchain-based dynamic extensible privacy protection and message authentication scheme for VANETs. It minimizes the computation cost of message authentication based on an elliptic curve and message batch verification. Based on the Chinese remainder theorem, this scheme protects transmitted message security by adaptively and dynamically responding to vehicles and RSUs accessing the VANET. It offers a smart contract-based forensics and tracing solution from the accident vehicle. In addition, strict security proof and analysis that the scheme meets the security requirements for the VANET. It evaluates the efficiency of the scheme, and the results show its practicality.**

***Index Terms*—privacy protection, VANET, smart contract, traceability, forensics.**

I. Introduction

WITH the characteristics of high data rate and low service latency, 5G promotes the rapid development of the Internet of Vehicles (IoV) industry [1], including vehicle platooning, remote driving, video, and map sharing. The IoV is an important technique to realize intelligent travel and intelligent transportation [2]. Vehicular ad hoc networks (VANETs) are the most promising and important part of IoV [3]. With the deployment of VANETs, vehicles have been transformed from traditional vehicles to intelligent vehicles. VANETs are referred to as vehicle-to-everything, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-pedestrian (V2P) [4]. A typical VANET includes On-Board Units (OBUs) embedded in the vehicle, Roadside Units (RSUs) installed alongside the road, and Trusted Authorities(TAs) [5].

The Dedicated Short Range Communication (DSRC) protocol states that a vehicle-embedded OBU broadcasts a traffic message every 100-300 milliseconds to other vehicles [6].Once receiving a traffic message, the RSU would either deliver the message to the traffic management department if it contains any useful information, or respond to it if the sending vehicle is nearby and the message is related to a situation that can be handled locally. For example, if a vehicle reports a pothole on the road, the RSU can immediately alert other vehicles in the area to slow down and avoid the pothole. The RSU has the capability to monitor and analyze the traffic conditions in its vicinity. It can collect data on traffic volume, speed, and congestion levels. Based on this data, the RSU can generate reports and summaries that provide insights into the traffic management department. With the traffic situations from RSUs, it is helpful for the traffic management department to make informed decisions and take appropriate actions to manage the traffic flow [7]. The application of VANETs provides a perfect convenience for passengers to travel [8]. By obtaining traffic information from adjacent vehicles and RSUs, vehicles will be able to effectively avoid obstacles, choose the best navigational route, and detect hazards while driving. If a vehicle breaks down or crashes, the VANET system could identify the location and situation in time, and quickly send rescue information to the surrounding traffic police and medical institutions, speeding up the efficiency of road safety assurance [9]. The VANET has great advantages to promote the development of smart transportation [10]. However, due to transmitting messages with the open wireless network, attackers can easily obtain information and spread the tampered information to other vehicles, which may lead to serious traffic accidents. Although countries are increasing their investment and research in VANET technology, it still faces the following challenges that must be focused on and solved.

1) With the mobility characteristics of the limited mobile area, fast network topology changes, frequent network access and interruption, and complex communication environment in the VANET, it is difficult for VANETs to design secure communication mechanisms.
2) The transmitted message may contain sensitive information *such as the identity of the driver, the passenger inquiry preference, the vehicle's running state, driving track, location information, and personal living habits*. Once this information is obtained by malicious users, the damage to the vehicle and passenger may be incalculable. For example, if the identity of the driver is

This work was supported by the Youth Science Fund Project of South China Normal University (No. 22KJ16), the Open Research Fund Program of Key Laboratory of Agricultural Blockchain Application, Ministry of Agriculture and Rural Affairs (No. 2022KLABA06), and the National Key R&D Program of China (No. 2018YFC1604000). *(Corresponding author: X. Cui (e-mail: xcui@whu.edu.cn)).*

Q. Tao is with the South China Normal University, Guangzhou 510631, China.

H. Ding, T. Jiang, and X. Cui are with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China.

revealed, the location that the driver frequently visits *such as a school, church, or hospital*, will be exposed to the attacker, and the privacy-sensitive information may promote computer-aided crime, *such as car theft, harassment, kidnapping, etc.* Therefore, the problem of data security and privacy protection has become a challenge that must be focused on and solved in the VANETs [5].

3) Validating thousands of messages per second is a challenge for RSUs and resource-constrained vehicles. The computational complexity and overhead will linearly increase with the increase in the number of messages [8]. Therefore, the cost of computation overhead for the authentication schemes should be minimized to meet the real requirement [11].

In recent years, researchers focus on authentication signature schemes in VANETs to provide secure services. Previously proposed schemes addressed some of the security problems in VANETs, but they are not completely safe [2], [5]. The performances of these proposed schemes are not adequate to satisfy the communication requirements of VANETs [11]. The participants in the VANET are unfamiliar with each other and lack the foundation of trust among the RSUs, vehicles, and TAs [12]. It would make passengers reluctant to share information for fear of potential security risks, which may affect the orderly development of smart transportation [13]. Moreover, the accuracy and credibility of the sharing traffic messages is crucial as life may depend on it. However, it is difficult to distinct the accuracy and credibility of the sharing messages in VANET. So, it is necessary to establish a trusted system to realize security authentication and cooperative sharing. Since the features of smart contracts, consensus mechanisms, and tamper-proofing, blockchain is a feasible solution for VANETs to construct a trusted environment [14], in which blockchain would form a distributed decentralized database, and provide a method to automatically inject trust, check the credibility of the messages, and monitor communication between the participant entities.

To address the above issues, we aim to find a novel lightweight and dynamically scalable message authentication scheme for VANETs. Namely, we consider not only reducing the computation and communication overhead of the vehicle and RSU, but also adapting to the rapid entry and exit characteristics of vehicles in the RSU area. The contributions of this work are as follows.

- We analyze the security weaknesses of the scheme [5] and propose a novel B-DSPA scheme. It provides a trusted environment for data sharing based on blockchain, guarantees the validity of shared data with the characteristics of trusted storage and smart contract, and realizes traffic message sharing and management.
- It supports auto-adapt with lightweight computation overhead to the vehicle and RSU device dynamic joining or off the VANET based on the Chinese remainder theorem. And it provides a solution for the traffic management department to trace accident vehicles. Once an accident occurs, it can timely obtain relevant electronic forensics of traffic incidents by smart contracts.
- It proves that the B-DSPA scheme for the VANET meets the security and privacy requirements. And performance analysis results show the scheme has a better performance compared with the existing schemes.

The remainder of this work is as follows: We revisit existing works related to ours in Section II. Section III introduces the definitions of complexity assumptions, system model and system security goals. Section IV reviews and analyses the security of *Zhang et al.* [5] scheme. Section V constructs a novel B-DSPA scheme. Section VI describes security proof and analysis, section VII presents the performance analysis, and the conclusion is presented in section VIII.

II. Related Work

Liu et al. [15] proposed a proxy-based message authentication in VANETs, where it outsources the message verification to the proxy vehicle to reduce the computational costs of RSUs. However, *Asaar* and *Salmasizadeh* [16] pointed out that there is a serious weakness in the secret key of the scheme [15] that couldn't be against the impersonation and modification attacks. To solve the shortcoming of the scheme [15], it proposed an improved identity-based message authentication scheme using proxy vehicles [16], in which it shows that the scheme could against adaptive chosen-message attack under the elliptic curve discrete logarithm assumption. *Abdelaziz et al.* [17] proposed an enhanced authentication scheme. In their scheme, it takes a multi-antenna RSU as the wireless transceiver to mitigate the risk of location spoofing attacks. But it couldn't achieve string security and mutual authentication. To protect the security of secret key interactions, *Ma et al.* [9] proposed a mutually authenticated key agreement scheme with an elliptic curve discrete logarithm. In the scheme [9], to protect passengers' privacy, it used a securely agreed session key to transmit the secret key. But their scheme couldn't meet the situation where RSU is required to validate a large number of messages in a second. *Li et al.* [18] proposed a lightweight message authentication scheme for VANETs. In the scheme [18], it used hash functions and exclusive-OR operations instead of a bilinear map to reduce the computation overhead, and it could be against common attacks and keep the communication data secret. But simultaneous authentication of massive messages would result in serious message latency in the scheme [18]. *Zhang et al.* [19] constructed an RSU-aided message authentication scheme with a message authentication code. In their scheme, it generated many one-time session keys and certificates for each vehicle and nearby RSUs to enhance privacy and confidentiality. But, it is a tedious task for key and certificate management.

To reduce the communication overhead caused by certificates, researchers began to focus on certificateless signature schemes. *Horng et al.* [20] provided an efficient certificateless aggregate signature in VANETs. However, *Li et al.* [21] proved that the scheme [20] was not safe and couldn't defend malicious-but-passive KGC(Key Generation Center) attacks. *Mei et al.* [2] proposed secure identity authentication with a certificateless aggregate signature. However, their schemes

haven't improved the authentication efficiency significantly because of the bilinear pairings and hash-to-point operations. *Li et al.* [22] proposed a pseudonym swap with a provable unlinkability scheme in VANETs, in which it found that the pseudonyms of the vehicles may be related to each other, leading to serious privacy leakage of the vehicle trajectory. To solve this problem, it proposed an improved scheme based on a pseudonym exchange scheme [22]. The proposed scheme, however, couldn't defend the impersonation attacks because swapping pseudonyms between vehicles meant that they would know each other's private keys.

In practice, high-speed traffic flows would generate a huge number of messages at the same time. The method based on one-by-one authentication will lead to a delay in receiving traffic information and it is difficult to achieve a real-time traffic system [23]. *Zhong et al.* [24] proposed a privacy-preserving authentication with full aggregation for VANETs using bilinear pairings. However, it is inefficient due to the cumbersome bilinear pairing operations. *Lee et al.* [25] proposed an authentication of the batch scheme based on bilinear pairing. In their scheme, the vehicle transmitted messages with pseudo-identity and generated the private key with a timestamp using a one-way hash function instead of a map-to-point function against replay attacks. *Bayat et al.* [26] detailed that there is a weakness in the secret key of *Lee et al.*'s [25] scheme, which can be used by a malicious vehicle to impersonate another vehicle. A privacy-preserving authentication with full aggregation for VANETs using bilinear pairings has been proposed in [24]. *Ali et al.* [27] proposed an improved efficient ID-CPPA(Identity-based Conditional Privacy-preserving Authentication) signature scheme based on a bilinear map for V2I communication, in which it provided a batch signature verification solution to reduce the computational cost on the RSU. *Bagga et al.* [12], [13] proposed a blockchain-based batch authentication scheme, in which each vehicle in a dynamically formed cluster broadcasts a message to its member and nearby RSU. But, the proposed scheme couldn't support backward security that the vehicle has left still could access the traffic information. In addition, in their batch verification scheme, any signature would affect the validity of the batch signature. It was inefficient because most signatures in the batch may be valid. So, a secure and privacy-enhancing communication scheme (SPECS) was proposed in [28] to improve the authentication efficiency and scalability for metropolitan area IVC. In the scheme [28], SPECS provided a software-based method to meet the privacy requirement and achieved lower message overhead than previous solutions in the message verification phase. However, *Horng et al.* [29] found that the SPECS [28] couldn't be against impersonation attacks. The malicious vehicle in a group could counterfeit another group member to send fake messages securely among themselves in the scheme [28]. To solve the shortcoming of the scheme [28], an improved secure scheme was proposed [29], which achieved the security and privacy requirements and overcame the weaknesses of SPECS. *Prasad et al.* [30] proposed a group authentication scheme based on secret key sharing and forward secrecy. In their scheme, the participant's equipment in a group could authenticate each other and the formal security was demonstrated based on BAN logic.

Existing security authentication schemes still face some problems in terms of security and efficiency. Most of the existing schemes mainly based on ideal trusted vehicles to resist enemy attacks, which is difficult to meet practical application needs. Besides, the communication equipment embedded in the vehicle has the characteristics of limited computing resources and fast-moving, which requires the security scheme should have better performance in message verification. The accuracy and credibility of the transmitted data is important in VANETs. To deal with the above challenges, we propose a lightweight and secure B-DSPA scheme based on the Chinese remainder theorem for VANETs.

III. Preliminaries

A. Complexity Assumptions

Assume that q-order cyclic additive group G with a generator P, where q is a large prime number. q-order cyclic additive group G_T with a generator g. There is a bilinear map $e : G \times G \to G_T$. It has the following properties [26], [29].

- Bilinear: For all $A, B, P \in G$, and $x, y \in Z_p$, there is an efficient algorithm to calculate $e(A, B)$, and $e(xA, yB) = e(A, B)^{xy}$;
- Nondegenerate: $e(P, P) \neq 1$;
- Symmetric: $e(A, B) = e(B, A)$;

Elliptic Curve Discrete Logarithm(ECDL) assumption [31]. Given two points $P \in G$ and $xP \in G$, it is negligible for the advantage to get $x \in Z_p^\star$ in probability polynomial time.

B. Chinese Remainder Theorem (CRT)

Define $k_1, k_2, \ldots, k_n$ be n pairwise relatively prime positive integers, and $gcd(k_i, k_j)_{i \neq j} = 1$. Define $t_1, t_2, \ldots, t_n$ be integers. Then, CRT states that the pair of congruences [5], [9],

$$x \equiv t_1 \bmod k_1$$
$$x \equiv t_2 \bmod k_2$$
$$x \equiv t_3 \bmod k_3$$
$$\ldots$$
$$x \equiv t_n \bmod k_n$$

has a unique solution in modulo K, where $K = k_1 k_2 \ldots k_n$. Define $T = t_1 t_2 \ldots t_n$. Then it can calculate the $x = \sum_{i=1}^{n} t_i K_i K_i^{-1} \bmod K$. Where $K_i = K/k_i$, and $K_i K_i^{-1} \equiv 1 \bmod k_i$.

C. System Model

The proposed system model for VANET is consist of TA, Motor-vehicle Department (MVD) subordinated to the TMD, RSUs, and OBUs, as shown in Fig. 1. The details are as follows.

- **MVD and TA.** The MVD and TA are trusted management devices in the system network. TA is in charge of the generation of the system public key and trace key, and the regulation of vehicle dynamic access to the VANET. It requires the TA should have the powerful computation, and usually set multiple TAs to avoid performance

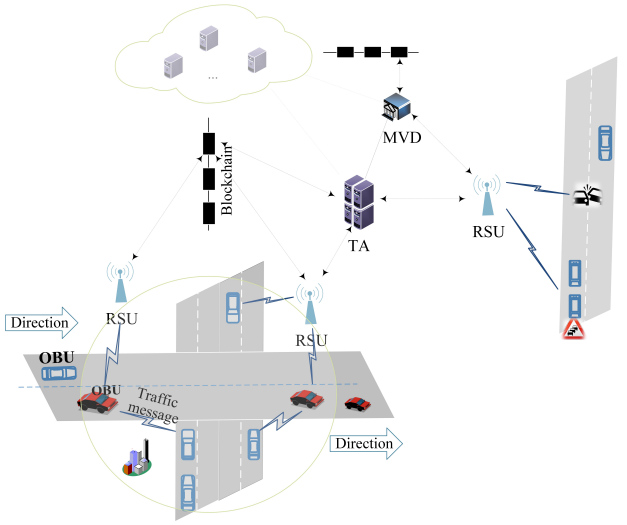

Fig. 1. System model for the proposed B-DSPA scheme. Once an accident happened, the vehicle reported to the nearby RSU, then the RSU verified the message and transmitted it to the MVD server for traceability and forensics.

bottlenecks. The system entities, such as vehicles, RSUs, and MVD servers, should be registered with TA before an operation, then TA will issue the secret params for them by a secure socket layer protocol [27]. MVD is responsible for tracking down the offending vehicle and conducting electronic forensics throughout the accident.

- **RSUs.** The RSUs are wireless communication devices, distributed all over the system network, serving as bridges between the management layer and the application layer. With the wireless propagation characteristics, each RSU delivers messages in a specified area. RSU devices receive traffic messages from the vehicles in its cluster and authenticate them in a batch. It assumes RSU devices are semi-trusted, collecting and mining vehicle information out of curiosity, but wouldn't refuse message verification.
- **OBUs.** The OBU device is embedded in the vehicle. It communicates with nearby RSU devices and other vehicles to get the latest traffic messages by DSRC protocol. The OBU device includes a Tamper-Proof Device (TPD) that is used to store the secret key from TA, which has less computation and storage memory [5]. OBUs are unreliable and vulnerable to attack [32].

D. Security Model and Goals

It is a core function of VANETs to protect privacy and message security. The scheme is CPA security if there exists no poly(t)-time algorithm for any adversary Λ to win the following games with non-negligible advantages ε.

- **Setup.** The adversary Λ forges a challenge message signature $\{m^{'}, sg^{'}, RID^{'}, T^{'}\}$. The simulator $\mathbb{C}$ calls the system setup, and returns the public key $\{P_{pub1}, P_{pub2}\}$ to Λ. The Λ can query random oracles, pseudo-identity, and signatures from the simulator $\mathbb{C}$.
- **Inquiry.** In this phase, Λ can query the results of random oracles $h_i(i = RID, m)$, pseudo-identity PID and signature sg multiple times from simulator $\mathbb{C}$. The adversary will forge a message signature $\{m^{'}, sg^{'}\}$ based on $\{PID^{'}, T^{'}\}$.
- **Forgery.** The adversary Λ wins the game only if Verify$(P_{pub1}, P_{pub2}, m^{'}, sg^{'}) =$ true.

The B-DSPA scheme should satisfy the following security requirements [1], [9], [31]. This part introduces the security goals of the proposed scheme.

- *Message integrity:* The B-DSPA scheme can check the shared message's integrity to prevent the adversary from changing it.
- *User anonymity:* It should preserve the privacy of the vehicle's users, even if an adversary intercepts the communications as they are being transmitted, the user's real identity and behavior cannot be discovered.
- *Traceability:* TMC devices can discover the vehicle's real identity from the accident messages, preventing malicious vehicles from denying their responsibility for traffic accidents.
- *Perfect forward/backward secrecy:* The B-DSPA scheme should support perfect forward secrecy to protect the privacy of messages transferred, in which the leaving vehicle can't access the message from the VANET. In addition, it should support perfect backward secrecy so that any newly joined vehicle can't access the old message from the existing vehicle in VANET.
- *Resistance to attacks:* The B-DSPA scheme should resist some basic attacks including the Man-in-the-Middle attack, the replay attack, and the collusion attack.

IV. Review of the PA-CRT Scheme

Zhang et al. [5] proposed a CRT-based message authentication scheme (PA-CRT) to provide secure communication between vehicles. With the characteristic of CRT, it generates a domain key for each vehicle in VANET. The details of the scheme [5] are as follows.

- System initialization and secure domain key generation
  1) Given public parameters $(p, q, E, G, Z_q^{\star})$. The trusted authority(TA) selects a param $s \in Z_q^{\star}$, $P \in G$, and calculates a public key $P_{pub} = sP$;
  2) TA selects a random $sk_i \in Z_q^{\star}$ for each vehicle applying for registration and calculates var_i for the vehicle. Then calculate $u = \sum_{i=1}^{n} var_i$;
  3) TA selects a random domain key $k_d \in Z_q^{\star}$, and calculates $r_d = uk_d$, $K_{pub} = k_dP$; Then pulish the system parameters $\{r_d, K_{pub}\}$ to each vehicle and RSU device.
- Pseudo identity generation and message signature
  1) After receiving the system parameters from TA, the vehicle calculates a new domain key $k_d = r_d \bmod sk_i$, and $S_i = a_ik_d \bmod q$.
  2) Select a random param $r \in Z_q^{\star}$, and calculate the pseudo-identity $ID = \{ID_1 = rP, ID_2 = RID_i \oplus H(rP_{pub})\}$;
  3) Select the current time T and calculate $\beta_i = H_3(ID, M, T)$. Then the traffic message M is signed with the signature $\sigma_i = S_i + \beta_i r_i \bmod q$.

- Message verification
  The verifier first checks the freshness of T, and then checks whether the formula $\sigma_i \cdot P = a_i P_{pub} + \beta_i ID_1$ holds true or not. Only if the result is true, the verifier accepts the message, otherwise rejects the message.
- Domain key updating
  1) When a new vehicle V_x accesses the current VANET, the TA selects a random $sk_x \in Z_q^\star$ and calculates the var_x for V_x. TA selects a new k_d, updates the param $u^{'} = u + var_x$, and $r_d^{'} = u^{'} k_d$. Then broadcast the param $r_d^{'}$ to all vehicles. After receiving the $r_d^{'}$, the vehicle would calculate a new domain key $k_d^{'}$ and generate the message signature with $k_d^{'}$ as shown in the phase of pseudo-identity generation and message signature.
  2) When a vehicle V_x leaves the current VANET, the TA selects the var_x from the storage memory based on the vehicle's identity. Update the param $u^{'} = u - var_x$, and $r_d^{'} = u^{'} k_d$. Then TA broadcast the param $r_d^{'}$ to all vehicles. After receiving the $r_d^{'}$, the vehicle would calculate a new domain key $k_d^{'}$ and generate the message signature with $k_d^{'}$ as shown in the phase of pseudo-identity generation and message signature.

A. Security Analysis of the PA-CRT Scheme

The domain key is the core param to protect the perfect forward and backward security of the scheme [5]. But, there exists a serious weakness in the system domain key k_d in the scheme [5], which may cause serious security risks to vehicles. Detailed analysis is as follows.

1) According to the details in the scheme [5], the system param $r_d = u \cdot k_d$ is public to every vehicle. Since $k_d \in Z_q^\star$ is a random param for different vehicles, the $u \in Z_q^\star$ is the same for every vehicle. So, according to the Euclidean algorithm [33], the adversary can get the param u by computing $u = \gcd(r_{d,1}, r_{d,2}, \ldots, r_{d,i})$. What's worse, it is easier to get u as more vehicles and RSUs are colluding.
2) After obtaining the param u, it means the adversary can get the system domain key k_d by computing $k_d = r_d \cdot u^{-1}$.
3) The relationship between parameter $r_d^{'}$ and parameter u is an incremental one that varies with vehicles. Combined with the deterministic characteristics of vehicle travel routes, the adversary can deduce each vehicle's secret param var_x by monitoring and collecting the $r_d^{'}$ in VANET. After that, the adversary can determine in real-time which vehicle is entering or leaving the VANET based on the changes in the parameters $r_d^{'}$. Even the adversary can compute and broadcast param $r_d^{'} = u - var_x$ to control the communication system of the vehicle V_x, which will bring serious security risks to the driver.

According to the weaknesses in the scheme [5], we propose a novel secure and lightweight B-DSPA scheme with CRT in the next section. In the proposed scheme, to resist the analysis attack, the system parameter r_d is eliminated, and the control parameter α is embedded into the system public key, which protects the security of the scheme based on the ECDL assumption.

V. Proposed B-DSPA Scheme

This section discusses the proposed B-DSPA scheme. Details of the operation of the B-DSPA scheme as shown in Fig. 2, in which the TA server, using multiplexing to provide registration services via the registration server and key issue services by the public key generation (PKG) server, communicates with RSU and multiple vehicles. To create a trust environment for VANETs, it selects TA servers and MVD servers as the nodes to construct a blockchain network. If a vehicle enters or exits the RSU area, the RSU records the information into blockchain. Besides, the RSU also should upload the received messages to the blockchain for consensus verification and distributed storage. The characteristics of trusted storage and consensus mechanism in blockchain can guarantee the validity of shared messages [34]. Once a vehicle traffic accident occurs, the scheme will conduct electronic forensics on the vehicle at the period time of the accident based on the pre-set smart contract, and send it to MVD.

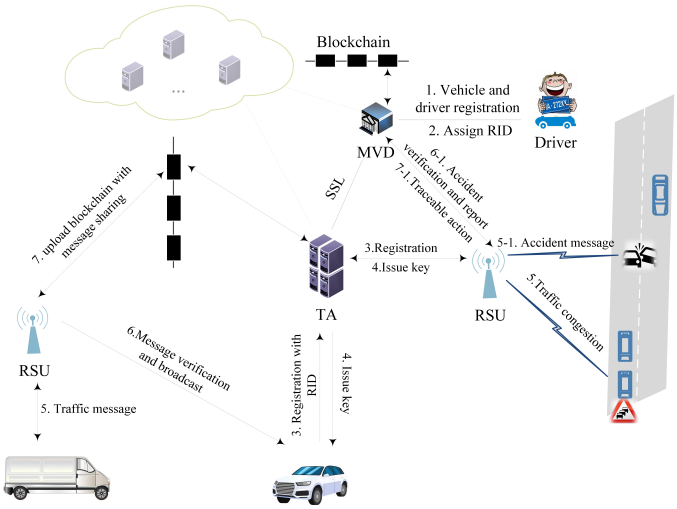

Fig. 2. Details of the operation of the B-DSPA scheme.

The B-DSPA scheme includes eight algorithms system initialization, system setup, generation of pseudo-identity and message signature, tracking the offending vehicle, message verification, batch message verification, and vehicle access/off the VANET. Each algorithm will be detailed as follows.

- **System init.** This algorithm is executed by a trust MVD server. According to traffic laws and enforcement [35], each vehicle owner should go to the MVD with personal information and vehicle materials to register the vehicle. The registration process is shown in Fig. 3. MVD checks the legitimacy of the registration data. Then select random param $RID, PWD \in Z_q^\star$ as the registration identity and password of the vehicle.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3289057

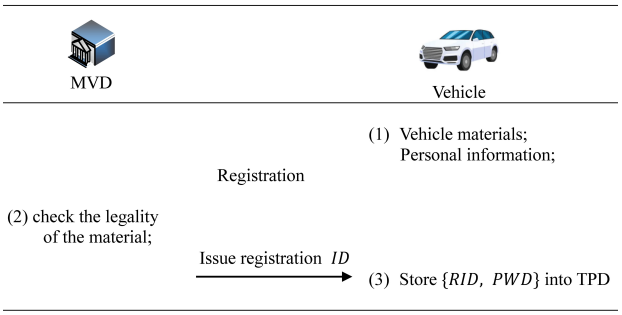

Fig. 3. The registration process of a vehicle.

- **System setup.** This algorithm is executed by a trust TA server to generate the system parameters. It inputs a secure param $\Theta \in N$ to generate the params (G, G_T, e), where G and G_T are the additive groups with the same order q, and $e : G \times G \to G_T$ is a bilinear map. Then TA takes the system parameters into RSUs and MVD through a secure channel. And the system parameters would be received by OBU when the vehicle is across the ETC gate [29]. The system setup steps are shown in Fig. 4.

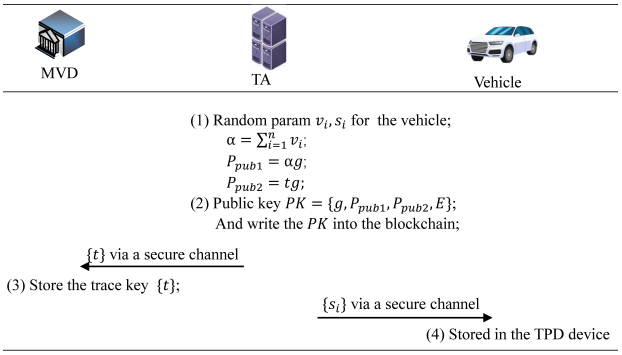

Fig. 4. The processing of the system setup.

1) TA randomly selects a q-order additive group G based on the elliptic curve $E : y^2 = x^3 + ax + b$ mod q over a prime finite field $Z_q^\star$. And select a generator g of group G.
2) TA selects random params $v_i, s_i \in Z_q^\star$ for the vehicle V_i and RSU device, and $1 \equiv v_i \bmod s_i$. For any two different vehicles V_i and V_j, the $\gcd(s_i, s_j)_{i \neq j} = 1$. Then define the system control param $\alpha = \sum_{i=1}^{n} v_i$, and calculate the public key $P_{pub1} = \alpha g \in G$. Define $E = e(g, P_{pub1})$.
3) TA selects two cryptographic hash functions h, h_1, h_2.
4) TA selects a random trace secret key $t \in Z_q^\star$ for the MVD to support tracing the accident vehicle. Then calculate the public key $P_{pub2} = tg$.
5) It uploads the system parameters $PK = \{G, G_T, h, h_1, h_2, g, P_{pub1}, P_{pub2}, E\}$ into the blockchain and publishes to any participant such as RSUs, vehicles, and MVD.
6) When accessing through ETC or gas station, TA sends the secret param s_i and stored in the TPD device of the vehicle V_i. And the trace key t is sent to the MVD by a secure SSL channel.

- **Generation of pseudo-identity and message signature.** This algorithm is executed by the TPD of the vehicle to generate a pseudo-identity based on its identity RID. The vehicle transmits messages to a nearby RSU device for communication with pseudo-identity. The message authentication is shown in Fig. 5.

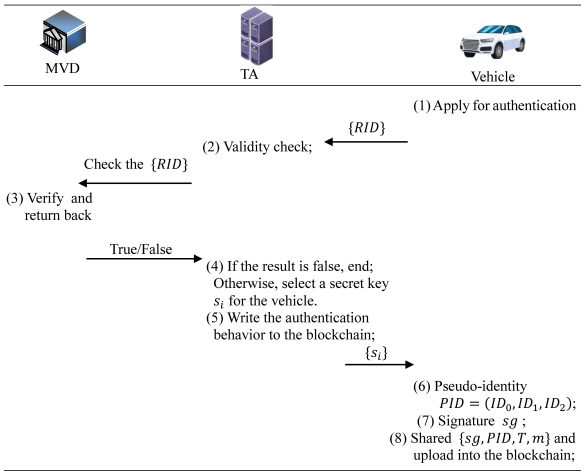

Fig. 5. The processing of message m authentication.

1) The vehicle V_i applies for authentication from a TA server. After receiving the registration application, TA server would connect with the MVD server to verify the validity of the application. Only if the vehicle registration is valid, it issues a random secret param s_i to V_i by a secure channel. Additionally, it writes the authentication behavior of the vehicle V_i into the blockchain for future evidence.
2) The vehicle V_i compares the pre-stored $RID^{'}, PWD^{'}$ with the input data RID, PWD. And if they are equal, perform the following steps.
3) The TPD takes RID, s_i and system parameters as input and calculates $T_1 = h(RID)$. It generates the pseudo-identity $PID = \{ID_0, ID_1, ID_2\}$:

$$\begin{aligned} ID_0 &= T_1 g, \\ ID_1 &= RID \oplus h_1(P_{pub2} T_1), \\ ID_2 &= s_i g. \end{aligned} \tag{1}$$

4) Then it inputs the current time T and signs the message m by (2) to generate the signature sg.

$$sg = \frac{P_{pub1}}{s_i + T_1 + h_2(m, PID, T)} \quad mod \quad q. \tag{2}$$

5) The vehicle V_i broadcasts $\{sg, PID, T, m\}$ to nearby RSU devices and vehicles.

- **Tracking the offending vehicle.** This algorithm is executed by the MVD server that is deployed in the traffic management department. Once traffic accidents happened, MVD would analyze the pseudo-identity and track the traffic accident vehicle as shown in Fig. 6.

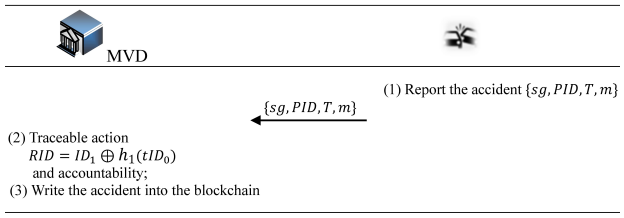

Fig. 6. The traceable action of an accident.

1) The vehicle and nearby RSU report the traffic accident message $\{sg, PID, T, m\}$ to the MVD.
2) Once receiving the message, the MVD device first checks the validation of the message with (4). Then take traceable action with equation (3) to get the real identity of the vehicle involved.

$$RID = ID_1 \oplus h_1(tID_0). \tag{3}$$

3) In addition, it shares the accident message into blockchain for the annual inspection and evaluation of vehicles. Since vehicles are usually associated with their owners, the traffic management department would obtain the vehicle user information based on the RID. The forensics process is shown in the electronic forensics algorithm based on smart contract.

Algorithm (Forensic): Electronic forensics with a smart contract

Input: the accident vehicle pseudo-identity, timestamp, interval time $\{PID, T, \Delta t\}$

Output: the related message

1: Function forensic(PID, T)
2: messages ← null
3: **For** $\{PID', T'\}$ in messages $\{sg', PID',\ T', m'\}_{i|i=1,...,n}$
4: **If** $PID == PID'$ and $(T - \Delta t) \le T' \le T$ **Then**
5: messages. push (m');
6: **End If**
7: End For
8: Return messages
9: End Function

Since the TVD can't get the vehicle's PWD and s_i, so it can't fake the vehicle's message signature.

- **Message verification.** This algorithm is mainly executed by RSUs as shown in Fig. 7, of course, the vehicle also can verify messages if necessary. There is a pre-defined transmission delay δt.
  1) When receiving a message, it first checks the current time $T^{'}$. If $(T^{'} - T) > \delta t$, it would reject the message and outputs $\perp$, otherwise, it would do the next step.
  2) It takes $\{sg, PID, T, m\}$ as input and checks whether (4) holds. The equation is detailed as follows:

$$\begin{aligned} & e(sg, (ID_0 + ID_2 + gh_2(m, PID, T))) \\ & = e(\frac{P_{pub1}}{(s_i + T_1 + h_2(m, PID, T))}, \\ & \quad (T_1 g + s_i g + gh_2(m, PID, T))) \\ & = e(g, g)^{(\frac{\alpha}{(s_i + T_1 + h_2(m, PID, T))})(T_1 + s_i + h_2(m, PID, T))} \\ & = e(g, P_{pub1}) = E. \end{aligned} \tag{4}$$

  3) If (4) is held, the RSU device broadcasts the message, and the vehicle accepts it. Otherwise, reject the message and outputs $\perp$.

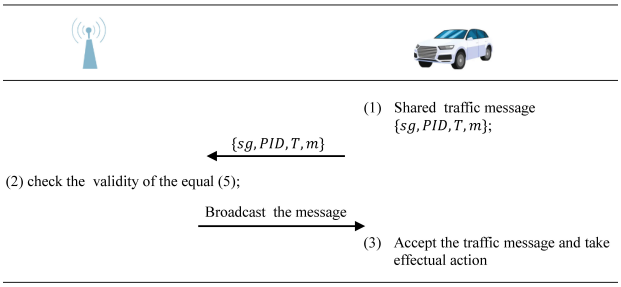

Fig. 7. The processing of message m verification.

- **Batch message verification.** This algorithm is mainly executed by RSUs. RSUs usually receive multiple messages simultaneously. It supports batch message verification.
  1) Select a random vector $V = \{v_1, v_2, .., v_n\}$ to ensure the validity of the batch verification results based on the small exponent test scheme [26].
  2) Then, it takes the received messages $\{sg, PID, T, m\}_{i|i=1,\ldots,n}$ as input. Then verify (5).

$$\begin{aligned} & e(\sum_{i=1}^{n} v_i(sg_i), \sum_{i=1}^{n} v_i(ID_{0i} + ID_{2i} + gh_2(m_i, PID_i, T_i))) \\ & = \sum_{i=1}^{n} v_i e(\frac{\alpha g}{s_i + T_1 + h_2(m, PID, T)}, \\ & \qquad (T_{1i} + s_i + h_2(m_i, PID_i, T_i))g) \\ & = \sum_{i=1}^{n} v_i e(\alpha g, g) \\ & = \sum_{i=1}^{n} v_i E. \end{aligned} \tag{5}$$

  3) If (5) is held, the RSU device broadcasts all messages, and the vehicle accepts them.
- **Vehicle access to the VANET.** This algorithm is executed by a TA server to update the system control param α as shown in Fig. 8. When an outside vehicle V_m accesses the control area of the current VANET, it would execute the following steps.
  1) The vehicle V_m would apply for authentication. TA sever will do the validity check by connecting with the MVD server based on the vehicle's identity.
  2) Select random $\{v_m, s_m\} \in Z_q^\star$ for V_m, and update the system control param $\alpha^{'} = \alpha + v_m$, $P_{pub1}^{'} = \alpha^{'} g$. It also can support several vehicles accessing the VANET at the same time by computing $\alpha^{'} = \alpha + \sum v_m$, and updating $P_{pub1}^{'}$.
  3) Record the V_m entering the VANET into the blockchain. And publish the new $P_{pub1}^{'}$ to any devices in VANET.

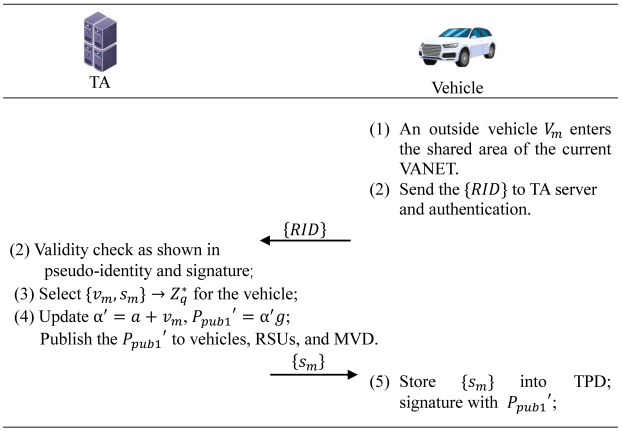

Fig. 8. The processing of an outside vehicle V_m access to the VANET.

4) V_m stores the s_m in the TPD device, calculates the pseudo-identity PID, and generates a signature by $P_{pub1}^{'}$.

This algorithm also adapts to the new RSU device dynamic joining the VANET.

- **Batch off the VANET.** This algorithm is executed by a TA server as shown in Fig. 9. When several vehicles V_m off the current VANET.

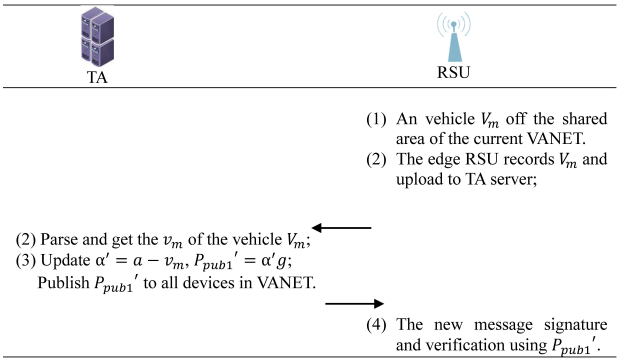

Fig. 9. The processing of a vehicle V_m off the VANET.

1) The edge RSUs would report the message to a TA server. TA server will parse the vehicle's identity and update the system control param $\alpha^{'} = \alpha - v_m$. It can also support several vehicles leaving the VANET by computing $\alpha^{'} = \alpha - \sum v_m$.
2) Record the V_m off the VANET into the blockchain. And publish the new $P_{pub1}^{'} = \alpha^{'} g$ to any devices in VANET.
3) After that, the existing vehicle in VANET generates a new signature using $P_{pub1}^{'}$.

This algorithm also adapts to the existing RSU device dynamic off the VANET.

VI. Security Proof and Analysis

This section analyzes the efficiencies of the B-DSPA scheme in meeting the security requirements under the presumption that the ECDL assumption is difficult to solve.

A. Security Proof

Theorem 1. (CPA-Secure) Assume the adversary can access a random oracle model and obtain the ciphertext of any message. If there is no existing poly(t)-time for an adversary to solve the ECDL problem with non-negligible advantage ε, the B-DSPA scheme would be security against chosen-plaintext security attacks. If an adversary Λ can forge an effective signature, it will succeed with non-negligible advantages ε under the model as shown in section II. Define parameters q_h, q_{PID}, q_{sg} are used to label the query number of random oracles h, PID and sg, respectively. So, there exists a poly(t)-time algorithm Λ with probability $\varepsilon' = \frac{\varepsilon}{(q_h q_{h_m} q_{PID})}$ for Λ to solve the ECDL assumption. The security simulation proceeds as follows.

Proof. Given an instance $(g, A = ag)$ of ECDL assumption based on the elliptic curve $E : y^2 = x^3 + ax + b \bmod q$ over a big prime finite field $Z_q^\star$, the challenger $\mathbb{C}$'s goal is to distinct $Z \stackrel{?}{=} a$. The challenger $\mathbb{C}$ selects two cyclic groups G and G_T with the same large prime order q. And there is a bilinear map $e : G \times G \rightarrow G_T$. The adversary Λ would forge a random challenge message signature $\{m', sg', RID', T'\}_j$. According to [9], [36], it constructs a simulation process as follows.

Init. The challenger $\mathbb{C}$ selects collision-resistant cryptographic hash functions h, h_1, h_2. Selects $\Psi \in \{0, 1\}$ and sets $< A, B >=< g, \alpha g >$. Define $Z = \alpha$ if $\Psi = 1$, otherwise, set $Z = R$.

Setup. The challenger $\mathbb{C}$ selects a generator g of group G and param $p \in Z_q^\star$ randomly. And calculate the public key $P_{pub1} = \alpha g, P_{pub2} = tg$, then send $\{G, G_T, h, h_1, h_2, g, P_{pub1}, P_{pub2}\}$ to the adversary Λ. Define parameters q_{h_i}, q_{PID}, q_{sg} used to label the query number of random oracles $h_i (i = 0, 2)$, the pseudo-identity and signature, respectively.

Inquiry. Adversary Λ is allowed to query the results of $h_i\,(i = RID, m)$, pseudo-identity *PID* and signature sg multiple times. The simulator $\mathbb{C}$ maintains the empty list L_{h_i}, L_{PID} and L_{sg} as follows.

1) h-Query. The simulator $\mathbb{C}$ let a list L_h to store the result (RID_i, h). After receiving a query request $\{RID_i \mid RID_i \neq RID'\}$ from Λ, $\mathbb{C}$ checks L_h and returns the result if the request had been received. Otherwise, $\mathbb{C}$ selects a random parameter $\beta \in Z_q^\star$, and returns the result $h = \beta$ to Λ, then adds (RID_i, h) into L_h.
2) h_2-Query. The simulator $\mathbb{C}$ uses the list L_{h_2} to store a message (m_i, h_2). Then select random parameter $\sigma \in [1, q_{h_2}]$. After receiving a query request $\{m_i\}$ from Λ, $\mathbb{C}$ returns the result from L_{h_2} if the same value has been queried. Otherwise, $\mathbb{C}$ processes as follows:
   a) If $\sigma = j$, it selects a random $\eta \in Z_q^\star$ and publishes $h_2 = h\,(m_i) = \eta g$ to Λ. Then it adds (m_i, h_2) into L_{h_2}.
   b) If $\sigma \neq j$, it selects random $\{\eta, \Delta\} \in Z_q^*$ and publishes $h_2 = h\,(m_i) = (\eta + \Delta)g$ to Λ. Then it adds (m_i, h_2) into L_{h_2}.

3) *PID*-Query. The simulator $\mathbb{C}$ uses a list L_{PID} to store pseudo-identity (RID_i, PID). After receiving a query request $\{RID\}$ from Λ, $\mathbb{C}$ sends the result from L_{PID} if the same value has been queried. Otherwise, $\mathbb{C}$ processes as follows.
   a) If $RID_i \neq RID'$, it selects a random $\{\gamma, \omega\} \in Z_q^*$, and returns $PID = \{ID_0 = \beta g, ID_1 = RID_i \oplus \gamma g, ID_2 = \omega g\}$ to Λ. Then adds $\{RID_i, PID\}$ into L_{PID}.
   b) If $RID_i = RID'$, once the adversary Λ can get the real identity RID, combined with the characteristic of a one-way hash function, it means the target vehicle has been compromised and any secret param would be accessed by Λ. It stops and defines the process event as E_1.
4) Signature-Query. processes the signature query (PID, m_i, T) as follows:
   a) If $m_i = m'$ and $RID_i \neq RID'$, it checks $(RID_i, h), (m_i, h_2)$, and (RID_i, PID), then calculates the signature $sg = \frac{P_{pub1}}{s_i + T_{1i} + h_2(m_i, PID_i, T)}$. And send sg to Λ.
   b) If $m_i = m' \wedge RID_i = RID$, stops and defines the process event as E_2.

Forgery. Λ selects a random challenge message $\{m_i, RID_i, T\}$, and outputs signature $sg = \frac{P_{pub1}}{s_i + T_1 + h_2(m_i, PID, T)}$ of the message m_i. If $m_i = m' \wedge RID_i \neq RID'$, Λ failed to forge the signature. Only if $m_i = m' \wedge RID_i = RID$, the adversary succeeds and the equation $\mathrm{e}\left(sg, (ID_0 + ID_2 + gh_2(m', PID, T))\right) = E$ is held as follows. Assume $\psi = 1$ and no vehicles entered or exited the VANET during the attack.

$$\begin{aligned}
&\mathrm{e}\left(sg, (ID_{0i} + ID_{2i} + gh_2\left(m', PID_i, T\right))\right) = \\
&= \mathrm{e}\left(\frac{P_{pub1}}{s_i + T_1 + h_2(m', PID', T')}, (\beta \mathrm{g} + s_i' g + gh_2\left(m', PID_i, T\right))\right) \\
&= \mathrm{e}\left(\frac{P_{pub1}}{s_i + T_1 + h_2(m', PID', T')}, (\beta + s_i' + h_2\left(m', PID_i, T\right)) g\right) \\
&= \mathrm{e}\left(g, P_{pub1}\right) = E
\end{aligned}$$

So, the adversary Λ can forge signature $\{m', sg', RID', T'\}$ with an advantage $\varepsilon' = \varepsilon / \left(q_h q_{h_2} q_{PID}\right)$, where the probability of $h(RID) = h\left(RID'\right)$ is $1/q_h$,the probability of $h_2 = h\left(m'\right)$ is $1/q_{h_2}$, and the probability of $L_{RID} = L_{RID'}$ is $1/q_{PID}$.

In conclusion, the B-DSPA scheme is CPA security under the random oracle model.

B. Security Analysis

This section would discuss whether the B-DSPA scheme satisfies the required security requirements introduced in section II (Security goals).

1) **Message integrity and user anonymity:** As proof of theorem 1, it is hard for the adversary with advantage $\varepsilon^{'} = \frac{\varepsilon}{q_h q_{h_2} q_{PID}}$ to deal with the ECDL assumption in probability polynomial time. Since the B-DSPA scheme is CPA-Secure, so it can achieve message integrity by checking the validity of the message verification formula (4). In addition, since the vehicle's pseudo-identity $PID = ID_0 = T_1 g, ID_1 = RID \oplus h_1(tgT_1), ID_2 = s_i g$ satisfied with ECDL assumption, so the adversary couldn't deduce the real identity RID from PID. Hence, the proposed scheme for VANETs can achieve message integrity and user anonymity.
2) **Traceability:** TVD server had received the track secret key $\{t\}$ from the TA by SSL channel. while receiving the accident report $\{sg, PID, T, m\}$ from a vehicle or nearby RSU device, it can discover the vehicle's real identity RID based on formula (3) and $\{t\}$, where $RID = ID_1 \oplus h_1(tID_0)$. It would be useful for the traffic management department to track and prevent vehicles from denying their responsibility for traffic accidents. Hence, the B-DSPA scheme provides traceability.
3) **Perfect forward/backward secrecy:** Since a vehicle joins (or leaves) the current VANET, the system would re-calculate the control param α based on the algorithm of vehicle join (or batch leave) as shown in section IV. So, the system will publish a freshness public key $P_{pub1}^{'} = \alpha^{'} g$ to all participants in VANET. After receiving the new public key, the vehicle will use $P_{pub1}^{'}$ for traffic message signature and verification. So, the new vehicle can't verify and access the old message by $P_{pub1}^{'}$, which helps the system achieve perfect backward secrecy. In addition, once a vehicle is off the current VANET, the system public key $P_{pub1}^{'}$ would be updated in time. So the exiting vehicle can no longer access the traffic message in the original network. Hence, the B-DSPA scheme also supports perfect forward secrecy to protect shared messages.
4) **Resistance to attacks:** In the B-DSPA scheme, the basic attacks are the Man-in-the-Middle attack, the replay attack, the modification attack, and the collusion attack. The analysis is as follows.
   a) **Resistance to Man-in-the-Middle attack:** Assume an adversary has got a vehicle's pseudo-identity $\{ID_0, ID_1, ID_2\}$, and attempts to impersonate a vehicle to forge a valid message signature $\{m, sg, T\}$. If the adversary wants to generate a valid message signature to deceive other vehicles, it should calculate the signature params (s_i, T_1), so it firstly gets the T_1 from ID_0 or ID_1, and s_i from ID_2. According to the analysis of theorem 1, it is hard for the adversary to solve the ECDL assumption to get (s_i, T_1). So, the B-DSPA scheme can resistance to Man-in-the-Middle attacks.
   b) **Resistance to replay attack:** According to the description of the B-DSPA scheme, the freshness timestamp T is used to generate a signature. It can defend the message replay attack by verifying whether the formula (4) is held.
   c) **Resistance to modification attack:** As proof of theorem 1, the adversary can't forge a valid message signature. The proposed system would accept the shared traffic message only if (4) is held. So, the B-DSPA scheme can resistance to modification attacks.

TABLE I
SECURITY COMPARISON BETWEEN DIFFERENT SCHEMES

Security Features	[2]	[5]	[9]	[11]	[18]	[22]	[26]	[27]	[29]	Ours
Pseudo-identity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Message authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Traceability	✓	✓	×	✓	✓	×	✓	✓	✓	✓
Unlinkability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity privacy protection	✓	✓	✓	✓	✓	×	✓	✓	✓	✓
Perfect forward secrecy	×	✓	✓	×	×	×	×	×	✓	✓
Perfect backward secrecy	×	✓	×	×	×	×	×	×	×	✓
Resistance to replay attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resistance to Man-in-the-Middle attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resistance to collusion attack	×	×	✓	✓	✓	✓	✓	✓	✓	✓

[1] ✓ means the scheme has the feature. × means the scheme doesn't have the feature.

d) **Resistance to collusion attack:** Assume an adversary has got serval vehicles' pseudo identity $ID_i = \{ID_{0i}, ID_{1i}, ID_{2i}\}$ and attempts to impersonate another vehicle $ID_{j|j\neq i}$ to forge a valid message signature $\{m, sg, T\}$. To forge a valid signature, it should deduce the parameters (s_i, T_1) from ID_j. As the analysis of theorem 1, the adversary can't deduce valid params (s_i, T_1) under the ECDL assumption. Hence, the B-DSPA scheme for VANETs can resistance to collusion attacks between vehicles.

To reflect the security of the scheme more clearly, the existing state-of-the-art schemes [2], [5], [9], [11], [18], [22], [26], [27], [29] are selected for comparison. According to the result in table I, the B-DSPA scheme can meet the full of basic security requirements for VANETs.

VII. PERFORMANCE ANALYSIS

In this section, it would discuss the performance analysis of the B-DSPA scheme against existing schemes in VANETs based on cycle additive super elliptic curve group [2], [5], [9], [11], [29], [37].

A. Computation Cost Analysis

It selects a bilinear map $e : G \times G \rightarrow G_T$ with 80 bits security level. And the cyclic additive groups G is generated by a 512-bit prime point P with a 160-bit prime order q on the super singular elliptic curve $E : y^2 = x^3 + x(\text{ mod } P)$ with embedding degree 2. To calculate the execute cost of the basic cryptographic operations, it constructs an experiment environment with the MIRACL library [38] under the experiment platform including Windows 7 operating system, an Intel I7-4770 processor with 3.40 GHz, and 4 GB memory. The basic computation cost is shown in table II, in which the cost of hash function operation and point addition operation is negligible.

To compare the computation cost of the proposed B-DSPA scheme with existing related schemes, it takes the computational cost of anonymity, message signature and its verification, and batch message verification as the core indicator as shown in table III. Define PIMS is the total time of pseudo-identity generation, private key generation and message signature. SVOM is the total time of single verification of one message. BVMM is the total time of batch verification of multiple traffic messages.

TABLE II
THE COMPUTATION OVERHEAD COMPARISON

Notion	**Define**	**Computational cost (ms)**
T_{bp}	a bilinear pairing operation $e(A, B)$.	4.211
T_{sm}	the time of a scale multiplication operation xP of an elliptic curve.	0.442
T_{ssm}	the time of a small-scale multiplication operation related to an elliptic curve.	0.0276
T_{mtp}	the time of mapping a string to a point G.	4.406

The comparison results of computation overhead of different schemes are shown in table III. In the scheme [2], it should calculate 9 scale multiplication operations to generate pseudo-identity, private key and signature. So the PIMS of the scheme is $9T_{sm} \approx 9 \times 0.442 \approx 3.978ms$. The SVOM of scheme [2], including 4 bilinear pairing and 2 scale multiplication operations, is $4T_{bp} + 2T_{sm} \approx 4 \times 4.211 + 2 \times 0.442 \approx 17.728ms$. The BVMM of schemes, including 4 bilinear pairing and 4n small scale multiplication operations, is $4T_{bp} + 4nT_{ssm} \approx (16.844 + 0.1104n)ms$. In the scheme [9], it calculates 3 scale multiplication operations to generate pseudo-identity and message signature, so the PIMS of the scheme [9] is $3T_{sm} \approx 3 \times 0.442 \approx 1.326ms$. The SVOM of the scheme [9] including 14 scale multiplication operations, is $14T_{sm} \approx 14 \times 0.442 \approx 6.188ms$. Since the scheme [9] couldn't support batch message verification, the BVMM is $(6.188n)ms$ to verify n messages. Then the cost of PIMS, SVOM, and BVMM in the schemes [5], [11], [29], [37] can be calculated with a similar method as shown in table III. The PIMS of the proposed B-DSPA scheme needs 4 scale multiplication operations, including 3 scale multiplication operations to generate PID and 1 multiplication operation to generate traffic message signature. Hence, PIMS of the B-DSPA is $4T_{sm} \approx 4 \times 0.442 \approx 1.768ms$. The SVOM of the B-DSPA scheme, including 1 bilinear map operation and 1 scare multiplication operation, is $T_{bp} + T_{sm} \approx$

TABLE III
COMPUTATION OVERHEAD OF DIFFERENT SCHEMES

Scheme	PIMS	SVOM	BVMM
[2]	$9T_{sm} \approx 9 \times 0.442 \approx 3.978ms$	$4T_{bp} + 2T_{sm} \approx 4 \times 4.211 + 2 \times 0.442 \approx 17.728ms$	$4T_{bp} + 4nT_{ssm} \approx (16.844 + 0.1104n)ms$
[5]	$2T_{sm} \approx 2 \times 0.442 \approx 0.884ms$	$3T_{sm} \approx 3 \times 0.442 \approx 1.326ms$	$(n+2)T_{sm} + nT_{ssm} \approx (0.884 + 0.4696n)ms$
[9]	$3T_{sm} \approx 3 \times 0.442 \approx 1.326ms$	$14T_{sm} \approx 14 \times 0.442 \approx 6.188ms$	$14nT_{sm} \approx (6.188n)ms$
[11]	$7T_{sm} + T_{mtp} \approx 7 \times 0.442 + 4.406 \approx 7.5ms$	$3T_{sm} \approx 3 \times 0.442 \approx 1.326ms$	$2nT_{ssm} + T_{sm} \approx (0.442 + 0.0552n)ms$
[29]	$4T_{sm} + 2T_{mtp} \approx 4 \times 0.442 + 2 \times 4.406 \approx 10.58ms$	$2T_{bp} + 2T_{sm} + T_{mtp} \approx 13.712ms$	$2T_{bp} + 2nT_{ssm} + nT_{mtp} \approx (4.4612n + 8.422)ms$
[37]	$5T_{sm} \approx 5 \times 0.442 \approx 2.21ms$	$4T_{sm} \approx 1.768ms$	$3nT_{ssm} + T_{sm} \approx (0.442 + 0.0828n)ms$
Our scheme	$4T_{sm} \approx 4 \times 0.442 \approx 1.768ms$	$T_{bp} + T_{sm} \approx 4.211 + 0.442 \approx 4.653ms$	$T_{bp} + nT_{ssm} \approx (4.211 + 0.0276n)ms$

$4.211 + 0.442 \approx 4.653ms$. The total cost of BVMM in the B-DSPA scheme to batch verify n message signatures, where it would calculate 1 bilinear map operation and n small-scale multiplication operations. So the BVMM of the proposed B-DSPA scheme is $T_{bp} + nT_{ssm} \approx (4.211 + 0.0276n)ms$.

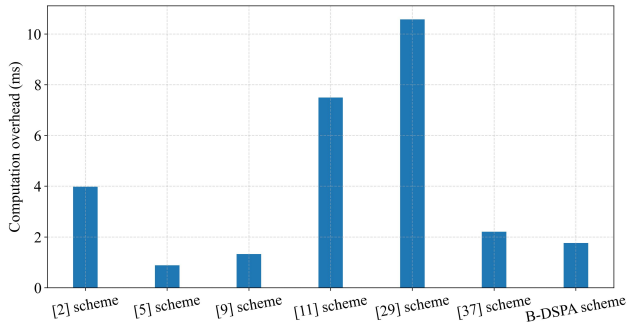

Fig. 10. Computation overhead to sign one message.

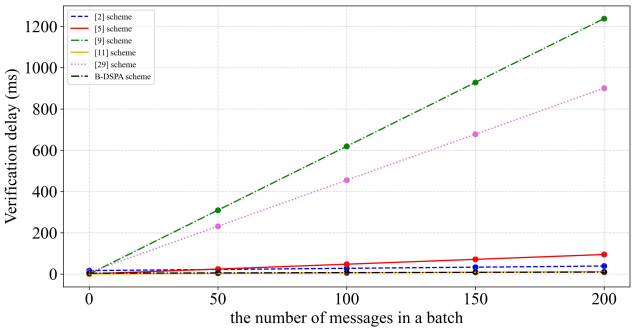

Fig. 11. Computation overhead to batch message verification.

In order to more clearly show the performance benefit of the proposed B-DSPA scheme, it compared the total execution time of message signature in this scheme with the related schemes, as shown in Fig. 10. The comparison results in Fig. 10 show that the proposed B-DSPA scheme has lower computation cost compared with other schemes [2], [11], [29], [37]. Fig. 11 shows the time delay of 200 messages batch verification between the B-DSPA scheme and the related schemes. According to the comparison results in Fig. 11, when 200 pieces of messages are verified in a batch, the performance of the B-DSPA scheme increased by 89.7% compared with scheme [5]. And as the number of messages in a batch increases, the advantage of the B-DSPA scheme will be more better. When more than 150 pieces of messages are verified, the B-DSPA scheme has the best effect compared with others [2], [5], [9], [11], [29]. If the number of batch verification messages is less than 136, with the computation cost of a bilinear mapping, the performance advantage of the B-DSPA scheme is not obvious compared with the schemes [11], [37]. However, the cost of T_{ssm} in the schemes [11], [37] is twice and thrice that of the proposed scheme respectively. Therefore, with the increase in the message number, the performance advantage of the B-DSPA scheme will be more obvious.

In practice, fast-moving vehicles in VANET generate a large number of messages. Vehicles in motion often receive multiple alternative traffic messages at the same time. In addition, the more complex the road conditions, the faster the traffic conditions change, and the more information the vehicle receives at the same time. Therefore, the obvious performance advantages of our proposed scheme in batch processing of messages will be more suitable for practical applications.

TABLE IV
THE COMPUTATION COST COMPARISON OF DIFFERENT SCHEMES

Scheme	PIMS	BVMM (200 message signatures)
[2]	55.6%	75%
[5]	–	89.7%
[9]	–	99.2%
[11]	76.4%	15.2%
[29]	83.3%	98.9%
[37]	20%	42.8%

The performance improvement of the proposed B-DSPA scheme with respect to the state-of-the-art schemes is listed in table IV. The total cost of PIMS in proposed B-DSPA scheme is 1.768ms, which has the improvement of $(3.978 - 1.768)/3.978 \times 100\% \approx 55.6\%$, $(7.5 - 1.768)/7.5 \times 100\% \approx 76.4\%$, 83.3%, 20%, respectively over the schemes [2], [11], [29], [37]. The performance of scheme [5]$(0.884ms)$ and scheme [9] $(1.3263ms)$ are slightly better than that of the proposed B-DSPA scheme $(1.768ms)$, but the message verification performance in the proposed scheme is significantly better than the scheme [9]. With a similar manner, it can calculate the performance improvement of the BVMM of the proposed scheme for 200 message batch verification. The BVMM of the proposed B-DSPA scheme has the improvement

of $(38.924 - 9.731)/38.924 \times 100\% \approx 75\%$, 89.7%, 99.2%, 15.2%, 98.9%, and 42.8%, respectively over the schemes [2], [5], [9], [11], [29], [37]. The results in table IV show that the performance of the proposed B-DSPA scheme is significantly improved compared with the existing schemes.

In addition, we simulated the blockchain network environment based on Hyperledger Fabric v2.4.1 [1] to evaluate the performance of the proposed scheme. The blockchain network is deployed on virtual machine, with 2 cores and 4 GB memory, created by VMware® Workstation 16 Pro. Define a maximum size of 40MB for receiving and sending messages in the blockchain. The cache size for CouchDB is 32MB, which is used to stored received traffic message.

The performance overhead based on single-thread and multithreaded data query access is shown in the Fig. 12. According to the performance loss of single thread receiving data access request, the cost of system initialization is about $300ms$. Single-threaded working mode can't take full advantage of blockchain performance. So, we simulate multiple threads responding concurrently to data requests and set the number of threads as 10. The number of data access requests is 50,100, 150 and 200, the response cost of per request is (346-300) /50 $\approx$ $0.92ms, 2.56ms, 3.15ms$ and $3.45ms$, respectively. Besides, Hyperledger Fabric explore [2] is used to test the performance overhead of traffic messages stored into the blockchain. The cost of each message written into the blockchain is about $[5.7ms, 8.5ms]$.

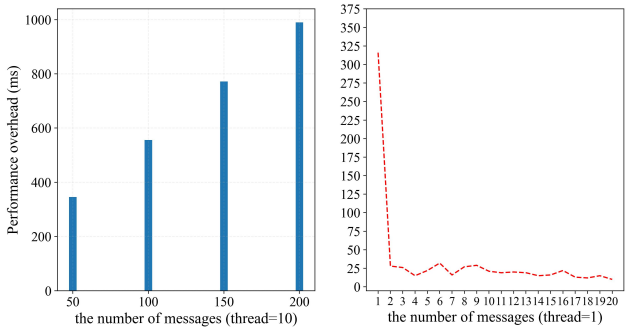

Fig. 12. Performance overhead of electronic forensics.

B. Communication Cost Analysis

The communication cost is mainly consumed in signature, pseudo-identity and timestamp. Assume the network quality is good and the data transmission will not be affected. Let the sizes of elements in $Z_q^\star$, G and G_T are $128bytes$. And the sizes of the result of a hash function and timestamp are $64bytes$ and $4bytes$ respectively. The communication overhead is shown in table V. According to the comparison of communication overhead, our scheme needs $500bytes$ that is better than the schemes [2], [9], [11], [37].

[1]https://github.com/hyperledger/fabric

[2]https://github.com/hyperledger-labs/blockchain-explorer

TABLE V
THE SIZE OF COMMUNICATION OVERHEAD

Scheme	Sending a single message	Sending n messages
[2]	$640bytes$	640n $bytes$
[5]	$388bytes$	388n $bytes$
[9]	$772bytes$	772n $bytes$
[11]	$644bytes$	644n $bytes$
[29]	$384bytes$	384n $bytes$
[37]	$580bytes$	580n $bytes$
Our scheme	$500bytes$	500n $bytes$

VIII. CONCLUSION

This paper analyzes the security vulnerability of the existing schemes and proposes a B-DSPA scheme based on CRT. The B-DSPA scheme adopts point multiplication based on an elliptical curve and has a better performance compared with the cost for the bilinear map in the existing schemes. This scheme supports batch message validation and minimizes the computing overhead of message verification for the RSUs. It provides an effective way for accident tracing and electronic forensics. The results of security analysis and performance analysis show that the B-DSPA scheme can meet the basic security requirements for VANETs, and the better lightweight performance cost can adapt to the fast-moving characteristic of the Vehicle in the VANET.

Our future research will focus on the security of VANETs with the goal of exploring more lightweight, and fine-grained access control solutions based on blockchain to satisfy the requirements of more complicated scenarios.

REFERENCES

[1] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5g vehicle-to-everything services: Gearing up for security and privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2019.

[2] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in iov," *IEEE Systems Journal*, vol. 15, no. 1, pp. 245–256, 2020.

[3] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[4] S.-h. Sun, J.-l. Hu, Y. Peng, X.-m. Pan, L. Zhao, and J.-y. Fang, "Support for vehicle-to-everything services based on lte," *IEEE Wireless Communications*, vol. 23, no. 3, pp. 4–8, 2016.

[5] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[6] 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.

[7] M. Abdelgadir, R. A. Saeed, and A. Babiker, "Mobility routing model for vehicular ad-hoc networks (vanets), smart city scenarios," *Vehicular Communications*, vol. 9, pp. 154–161, 2017.

[8] M. Azees, P. Vijayakumar, and L. J. Deboarh, "Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[9] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.

[10] M. M. Bhavani and A. Valarmathi, "Smart city routing using gis & vanet system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 5679–5685, 2021.

[11] G. Thumbur, G. S. Rao, P. V. Reddy, N. Gayathri, D. K. Reddy, and M. Padmavathamma, "Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1908–1920, 2020.

[12] Y. Yang, D. He, H. Wang, and L. Zhou, "An efficient blockchain-based batch verification scheme for vehicular ad hoc networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 5, p. e3857, 2022.

[13] P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar, "Blockchain-based batch authentication protocol for internet of vehicles," *Journal of Systems Architecture*, vol. 113, p. 101877, 2021.

[14] S. El-Switi and M. Qatawneh, "Application of blockchain technology in used vehicle market: A review," in *2021 International Conference on Information Technology (ICIT)*. IEEE, 2021, pp. 49–54.

[15] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Transactions on vehicular technology*, vol. 64, no. 8, pp. 3697–3710, 2014.

[16] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409–5423, 2018.

[17] A. Abdelaziz, C. E. Koksal, R. Burton, F. Barickman, J. Martin, J. Weston, and K. Woodruff, "Beyond pki: Enhanced authentication in vehicular networks via mimo," in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2018, pp. 1–5.

[18] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[19] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks," in *2008 IEEE international conference on communications*. IEEE, 2008, pp. 1451–1457.

[20] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.

[21] J. Li, H. Yuan, and Y. Zhang, "Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Cryptology ePrint Archive*, 2016.

[22] X. Li, H. Zhang, Y. Ren, S. Ma, B. Luo, J. Weng, J. Ma, and X. Huang, "Papu: Pseudonym swap with provable unlinkability based on differential privacy in vanets," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 789–11 802, 2020.

[23] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for vanets," in *2013 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2013, pp. 4609–4614.

[24] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in vanet," *Information Sciences*, vol. 476, pp. 211–221, 2019.

[25] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for vanet," *Wireless networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[26] 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.

[27] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets," *Vehicular Communications*, vol. 22, p. 100228, 2020.

[28] 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.

[29] 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.

[30] M. Prasad and R. Manoharan, "Secure group authentication scheme for lte-advanced," in *Soft Computing: Theories and Applications*. Springer, 2018, pp. 167–179.

[31] 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.

[32] A. Kalogianni, "Hackers wirelessly disable a jeep cherokee from 10 miles away with uconnect," https://www.digitaltrends.com/cars/uconnect-hackers-jeep-cherokee/, 7 2015, (Accessed on 13/11/2022).

[33] F. Lemmermeyer, "The euclidean algorithm in algebraic number fields," *Expositiones Mathematicae*, vol. 13, pp. 385–416, 1995.

[34] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future generation computer systems*, vol. 107, pp. 841–853, 2020.

[35] N. C. on Uniform Traffic Laws, *Uniform Vehicle Code and Model Traffic Ordinance*. National Committee on Uniform Traffic Laws and Ordinances, 1987.

[36] J. Sun, Y. Su, J. Qin, J. Hu, and J. Ma, "Outsourced decentralized multi-authority attribute based signature and its application in iot," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 1195–1209, 2019.

[37] Q. Mei, H. Xiong, Y. Zhao, and K.-H. Yeh, "Toward blockchain-enabled iov with edge computing: Efficient and privacy-preserving vehicular communication and dynamic updating," in *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, 2021, pp. 1–8.

[38] C. D. Walter, "Simple power analysis of unified code for ecc double and add," *Ches*, vol. 3156, no. 11, pp. 191–204, 2004.

Qi Tao received the Ph.D. degrees from School of Cyber Science and Engineering, Wuhan University, in 2021. He is currently a lecturer in South China Normal University. His research interests mainly include data governance and security, blockchain technology, cloud computing and food safety.

Hongwei Ding is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. He current research interests include deep learning and image processing.

Tian Jiang is currently pursuing the Ph.D. degree at the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His research interests include cybersecurity, adversarial attack and defense.

Xiaohui Cui received the Ph.D. degree in computer science and engineering from university of Louisville, American, in 2004. He is currently a Professor of the School of Cyber Science and Engineering, Wuhan University. He is the chief scientist of the national key research and development program of china. His main research interests include big data, cluster intelligence theory, blockchain technology, and high-performance computing.