IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 6, 2019, accepted April 22, 2019, date of publication May 9, 2019, date of current version May 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2915794

A Lightweight Privacy-Preserving Protocol for VANETs Based on Secure Outsourcing Computing

ZHIJUN WEI[1], JING LI[2], XIANMIN WANG[2], AND CHONG-ZHI GAO[2]
[1]School of Computer Science, Beijing Institute of Technology, Zhuhai 519088, China
[2]School of Computer Science, Guangzhou University, Guangzhou 510006, China

Corresponding author: Jing Li (lijing@gzhu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61472091, in part by the Natural Science Foundation of Guangdong Province for Distinguished Young Scholars under Grant 2014A030306020, in part by the Guangzhou Scholars Project for Universities of Guangzhou under Grant 1201561613, in part by the Science and Technology Planning Project of Guangdong Province, China, under Grant 2015B010129015, in part by the National Natural Science Foundation for Outstanding Youth Foundation under Grant 61722203, and in part by the JSPS KAKENHI under Grant JP15K00028.

ABSTRACT In the VANET systems, the leakage of some sensitive data or communication information will cause heavy losses for life and property. Then, a higher security level is required in the VANET systems. Meanwhile, fast computation powers are needed by devices with limited computing resources. Thus, a secure and lightweight privacy-preserving protocol for VANETs is urgent. In this paper, we first propose an identity-based signature that achieves unforgeability against chosen-message attack without random oracle. In order to reduce the computational cost, we design two secure and efficient outsourcing algorithms for the exponential operations, where a homomorphic mapping based on matrices conjugate operation is used to achieve the security of both exponent and base numbers. Furthermore, we construct a privacy-preserving protocol for VANETs by using outsourcing computing and the proposed IBS, where a proxy re-signature scheme is presented for authentications. In the VANET privacy-preserving protocol, TA authorizes RSU to act as an agent and RUS converts OBU's signature into TA's signature, which effectively hides the real identity of vehicle OBU. Meanwhile, TA has access to trace the real identity of OBU using its secret key when malicious messages are found. Then, the protocol provides anonymity, traceability, and privacy. In addition, with respect to the efficiency, our scheme does not need pairing operations and exponential operations. Thus, the calculation burdens for the VANET system can be significantly reduced.

INDEX TERMS Identity-based signature, VANETs privacy-preserving protocol, outsourcing computing.

I. INTRODUCTION

The Internet of thing (IoT) is a network that realizes overall interconnection of people and people, people and objects, objects and objects. The main feature of IoT is to obtain information from the physical world using radio frequency identification and sensors, and then transmit information by Internet and mobile communication networks [2], [11], [13], [32]. Intelligent computing technologies are adopted to analyze and process information, so as to enhance the perception of the material world and achieve intelligent decision-making and controlling. IoTs can be applied to military, industrial, power grid and water network, transportation, logistics, energy saving, environmental protection, medical and health, smart home and other fields. However, facing various attacks [9] in the open environment, to achieve data privacy is one challenge in the applications of IoTs. For example, personal hobbies, shopping habits and tourist routes are generally personal privacy information, and related to the safety of users' lives and property. Therefore, users' data security, identity privacy and location privacy will directly affect the development and popularization of IoTs [1], [20], [28], [33]. In this work, we mainly study privacy-preserving issues [10], [15], [31] for vehicular ad hoc networks (VANET) that is an important branch of IoTs [3], [30].

VANET is a self-organizing traffic information system that supports fast mobile communications. Under the background of intelligent transportations, VANET is convenient for the communications between any two vehicles. The vehicles can realize the information sharing and exchanging, where the

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaochun Cheng.

driver uses the emergency alarm to deal with the dangers in time, and adjust the route based on traffic information to avoid traffic accidents and congestions. This system contains three parties, Trusted authorities (TA), On Board Unit (OBU) and Road Side Unit (RSU). The responsibility of TA is to do identity authentication, certificate distribution, revocation management and information storage for each node in VANETs, and TA can be regarded as an authority center; OBU is a vehicle node, which is equivalent to the mobile terminal in the communication system. RSU is a roadside infrastructure node, and this node is similar to the communication base station in communication systems. For instance, it is often built on the roadside gas stations, restaurants, shops and other fixed network communication devices. Some simple RSUs can also be set up in the street lamps, traffic signs and other existing road infrastructures. Vehicular ad hoc networks allow communications between two OBUs or between OBU and RSU by Dedicated Short Range Communication (DSRC). In VANETs, each vehicle enables to periodically broadcast its basic vehicle information and traffic accidents in real time. This fact can make other vehicles take corresponding measures in time and effectively improve the traffic conditions. In addition, RSU cannot only broadcast some related information on restaurants, hotels and gas stations within its jurisdiction, but also broadcast road conditions, parking warnings, and traffic information.

However, since the communications of VANETs depend on a wireless channel within unstability, it will undoubtedly suffer various malicious ribs and attacks, such as injecting false information, modifying or replaying previous information, etc. For users' privacy information, these attacks and threats will become safety hazard in VANET systems. The main attacks are shown as follows: (1) Forgery information: the adversary deliberately puts forged false information into the VANET and gains illegal interests; (2) Illegal controlling: the adversary illegally manipulates roadside communications units to obtain privileged vehicles treatments such as free trial; (3) Replay attacks: the adversary re-sends the information recorded in the vehicle communication unit to cheat other members in VANET systems; (4) Witch attacks: the malicious vehicle illegally gets or occupies multiple identity information, then issues false messages to create illusion of traffic jams; (5) Message delaying: some malicious users delay sending or broadcasting messages, the legitimate users cannot handle messages in time and it may cause major life and property loss; (6) Privacy disclosure: the adversary steals information stored in vehicles or roadside communication units, resulting in the disclosure of the users' privacy information; (7) Tampering information: after a traffic accident, the perpetrators attacks the VANET system and tampers the location, direction and speed of their vehicles to evade legal responsibilities. In summary, the security of VANETs is particularly important, since it is closely related to the life and property of vehicle drivers. The malicious attacks will affect the network's operation and reduce its reliability. Then, how to ensure the safety and privacy of VANETs is an urgent problem. Moreover, the number of vehicles is largely increasing, which will cause huge computational cost for this system. Therefore, a secure and lightweight privacy-preserving protocol for VANETs is necessary. In particular, we can ''borrow'' the source of cloud servers to cut down the local computational cost [7], [18], [25].

Contributions: In this work, we first propose an identity-based signature (IBS) based on the standard RSA assumption. This signature scheme can be proved to be unforgeable against chosen-message attack without random oracle. Furthermore, we design two secure and efficient outsourcing algorithms for the exponential operation–$u^a \ mod \ n$. These outsourcing algorithms are divided into two situations based on the secure requirements of exponent and base numbers: (1) a is secret, u is public; (2) Both u and a are secret. Particularly, we use a homomorphic mapping based on matrices conjugate operation to achieve the second situation. The security of this outsourcing algorithm depends on the intractability of integer factorization for n and it provides verification function.

By using the outsourcing computations and the above IBS, we construct a privacy-preserving protocol for VANETs, where a proxy re-signature is designed and introduced for authentications. TA authorizes RSU to act as an agent, and RUS runs a proxy re-signature algorithm to convert OBU's signature into TA's signature, which effectively hides the real identity of OBU. At the same time, TA can quickly and accurately trace the real identity of the OBU using its secret key when malicious messages are found. Then the proposed scheme provides anonymity, traceability and privacy. The security of the VANETs privacy-preserving protocol is based on the IBS's security. In addition, with respect to the efficiency, our scheme does not need pairing operations, and the above outsourcing algorithms make each party avoid to execute large exponential operations. Thus, the calculation burdens for VANET systems can be considerably reduced.

In sum, we have the following contributions:

- We propose an identity-based signature that achieves unforgeability against chosen-message attack without random oracle.
- We provide some efficient outsourcing algorithms for exponentiation computation, especially, the outsourcing algorithm based on the homomorphic mapping.
- We construct a novel and efficient privacy-preserving protocol for VANETs based on the above security model and the outsourcing algorithms.

The rest of this work is organized as follows: In Section II, the related work is given. In Section III, some basic definitions are reviewed and the system models are given. Section IV presents an identity-based signature and a novel privacy-preserving protocol. In Section V, the security and performance analysis are shown. Finally, conclusions are provided in Section VI.

II. RELATED WORK

For achieving the security of VANETs, the researchers have proposed various privacy-preserving protocols based

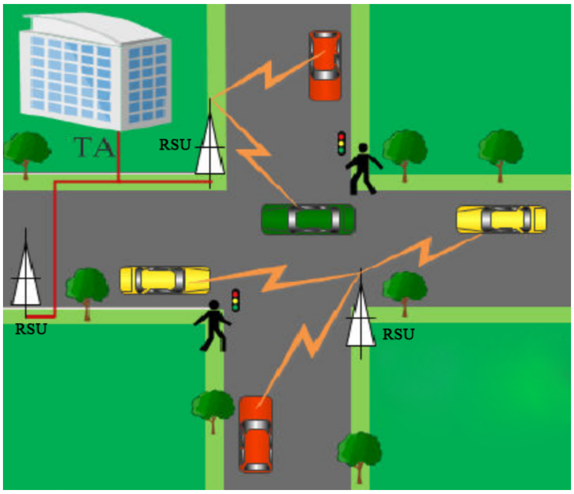


FIGURE 1. Traffic of VANET.

on the public key cryptographic schemes: In 2005, Raya and Hubaux [26] proposed a VANET privacy-preserving scheme by using a traditional PKI technology, which protects the real identity of OBU by periodically replacing certificates. For traceability, TA associates anonymous certificates with real OBU by finding a maintained table. In 2007, Lin *et al.* [23] first introduced group signature into VANET privacy-preserving algorithm, where OBU does not need to keep a large number of pseudonym keys and certificates. In INFOCOM'08, Lu *et al.* [24] designed a new secure scheme using group signature technology. The main idea is to introduce "on-the-fly" short-term group-member certificates and decrease the scope of RSU's jurisdiction. The scheme improves the system efficiency and solves the problem of key escrowing. In 2010, Wu *et al.* [29] presented a new scheme specifically for V2V communications, where they introduced a threshold to protect the credibility of messages and proposed a privacy-preserving mechanism with a priori preserving and a posteriori preserving. In 2013, Horng *et al.* [12] described a privacy-preserving scheme, which achieves message integrity and authentication and resists collusion attacks. In 2016, Sumreen and Karimulla [27] designed an agent-based authentication scheme with distributed computing, where the proxy server can verify multiple messages simultaneously. In 2018, Li *et al.* [16] constructed an efficient certificateless public key cryptographic authentication scheme with anonymous authentication. In addition, the scheme reduces the replication attacks and it provides a malicious-node alarm mechanism. The above schemes have made contributions for the security model of VANETs, we will pay much attention to construct lightweight authentication and revocation protocols with verifiable computations [6], [14], [19]. In the same year, some conditional privacy-preserving authentication schemes are proposed using hash functions [8], [17]. Compared with the previous work on VANET's privacy-preserving, our work will provide more efficient algorithms by outsourcing computations and present higher security model and the corresponding protocol.

III. PRELIMINARIES

We will review some basic secure concepts in this section.

A. DEFINITIONS

Definition 1 (Standard RSA Assumption (SRSA) [4]): Let p and q be two large primes, and set $n = pq$. Randomly choose an element $y \in Z_n$ and a prime number $e < n$. It is difficult to compute x such that $x^e = y\ (mod\ n)$. We say that the standard RSA assumption is a (t_R, ε_R)-RSA assumption if for any t_R-time, the advantage $Adv_{\mathcal{A}}$ of an attacker $\mathcal{A}$ solving the RSA problem meets $Adv_{\mathcal{A}} < \varepsilon_R$.

The RSA problem provides a natural approach for designing digital signatures, where the public key is N and the secret key is (p, q, x). Then a signature will consist of (e, y), where e depends on the given message and y is the signature. Next, an equivalent RSA hard problem will be derived from the following Lemma.

Lemma 1 [4]: Given $\alpha, \beta \in Z_n^*$ and $a, b \in Z$ such that $\alpha^a = \beta^b$, one can efficiently calculate $\gamma \in Z_n^*$ such that $\gamma = \beta^{\frac{gcd(a,b)}{a}}$.

Definition 2 (Equivalent RSA problem (ERSA) [4]): Given $y \in Z_n$ and a prime e, output α, a such that $\alpha^e = y^a$, where $gcd(a, e) = 1$.

Solving the ERSA problem is equivalent to solve the SRSA problem. In fact, on one hand, suppose that one can output (α, a) such that $\alpha^e = y^a$ for given y, e, where $gcd(a, e) = 1$. Then, based on Lemma 1,

$$x = \alpha^{\frac{gcd(e,a)}{a}} = \alpha^{\frac{1}{a}}$$

can be computed efficiently. Since

$$x^e = \alpha^{e\frac{1}{a}} = (\alpha^e)^{\frac{1}{a}} = (y^a)^{\frac{1}{a}} = y,$$

x is the solution of the SRSA problem. On the other hand, if one can output x such that $x^e = y$, then (α, a) is one solution of the equivalent RSA problem, where a is randomly chosen and α can be derived from $\alpha^e = y^a$ by the oracle of the SRSA problem.

B. SECURITY MODEL OF IBS

We now describe the security model for an IBS based on one challenge-response game between an adversary and a challenger. In the game, the adversary is allowed to issue a polynomial number queries of private key extraction for identities set ID and signatures for challenge identity $id^* \notin ID$. Then the game for unforgeability against adaptively chosen identity and message attacks is described as below.

- Setup Phase: The challenger generates and sends the public key to the adversary.
- Query Phase: The adversary adaptively makes a polynomial number of the following queries:
  • It randomly selects u_0 identities $\{id_i : i = 1, \cdots, u_0\}$. The challenger answers by running Ext algorithm to return the private key for each query-identity id_i.
  • It selects a challenge identity $id^* \neq id_i\ (i = 1, \cdots, u_0)$ and randomly chooses l messages $m_1, \cdots, m_l$ with

respect to id^*. The challenger computes the signature for each message by running Ext algorithm and Sign algorithm for id^*.

- Forgery Phase: The adversary returns a signature for id^* and m^* ($m^* \neq m_i$).

C. SECURITY REQUIREMENTS FOR VANETS

The object of VANETs is to improve the efficiency of traffic management, reduce road traffic congestion and protect the personal safety of drivers and passengers. However, the common attacks have seriously threatened the VANET system. A secure protocol for VANETs should satisfy the following requirements [23], [24], [26].

- Authentication: A basic requirement for secure communications is to verify the source of the transmitted messages in VANET. Message authentication guarantees that any malicious user cannot send messages in a false name.
- Non-repudiation: Non-repudiation means that the message sender cannot deny its transmitted message. The false message in VANET often misleads the vehicle users, so each user needs to be responsible for the sent message. Non-repudiation can effectively combat forgery attacks, that is, any malicious user fails to invest false information into VANET.
- Integrity: Messages have not been tampered in the course of broadcasting or sending. Integrity ensures the authenticity and reliability of the messages and improves the security of the system.
- Privacy: In the VANET system, some information is related to the privacy of users, which cannot be revealed to any unauthorized party. The confidentiality of messages can effectively combat privacy leakage and replay attacks.
- Anonymity: Any party without permission cannot obtain the personal information of the vehicle users or track the vehicle users according to the transmitted information.
- Traceability: Traceability means that TA can trace the real identity of the vehicle in time after a traffic accident, and investigate the legal responsibility. In VANETs, the TA is responsible for monitoring the safety and identity of vehicles.
- Revocation: TA has access to revoke malicious users from the VANET system, effectively terminating illegal infringement and ensuring the safety of vehicle users.
- Real time: Due to the huge network scale and changeable network topology, replaying the expiration information not only causes the overload of VANET system, but destroys the effective order of traffic roads. Therefore, real-time in VANETs is especially important for system security.

IV. CONSTRUCTIONS

In this section, we propose an IBS scheme, two outsourcing algorithms, then construct a novel privacy-preserving protocol.

A. IDENTITY-BASED SIGNATURE

The ISB scheme is designed as follows.

- **Setup**: Let p and q be two large primes, and $n = pq$. Choose a random element $g \in Z_n$, secure hash functions H: $Z_n^2 \rightarrow Z_n$ and H_0: $U \times Z_n \rightarrow Z_n$, where U is the identity set.
  The public key is $pk = (g, n, U, H, H_0)$, the master secret key is $sk = (p, q)$.
- **Ext**: The private key for identity $id \in U$ is created as $g_{id} = g^{\frac{1}{w_{id}}}$ $(mod\ n)$, where $w_{id} = H_0(id, v_{id})$ and v_{id} is randomly chosen for id. Then, id's private key is (g_{id}, v_{id}).
- **Sign**: For message $m \in Z_n$, the signer id randomly picks up r and calculates
  $$\sigma = g_{id}^{H(m,r)} \ mod\ n.$$
  The signature of message m is (v_{id}, r, σ).
- **Ver**: A receiver accepts the signature(m, v_{id}, r, σ) if
  $$g^{H(m,r)} = \sigma^{w_{id}} \ mod\ n$$
  holds, where $w_{id} = H_0(id, v_{id})$. Otherwise, the receiver rejects it.

B. SECURITY PROOF

We now prove the security of the IBS scheme with two chameleon hash functions H and H_0.

Theorem 1: Suppose that (t_R, ε_R)-RSA assumption holds, then the signature scheme is (t, ε)-secure and

$$\varepsilon \approx \frac{e-1}{e}\varepsilon_R, \quad t \approx t_R,$$

where (e, y, n) is the given RSA challenge and e is a large prime.

Proof: Let $\mathcal{A}$ be an adversary and $\mathcal{C}$ be the simulator. Then a RSA game is constructed between $\mathcal{A}$ and $\mathcal{C}$ as follows.

- **Setup**: Let p and q be two primes, and $n = pq$. Meanwhile, we employ chameleon hash functions H, H_0 and compute
  $$g = y^{\prod_{j=1}^{u_0} w_j} \ (mod\ n)$$
  for w_j, where w_j is randomly chosen such that $gcd(w_j, e) = 1$. The adversary is allowed to issue u_0-query of private key for identities. Let $w = \prod_{j=1}^{t} w_j$. The simulator outputs public key (g, n, H, H_0, U).
- **Query of private key**: The adversary randomly chooses u_0 identities (denoted by $U_0 = \{id_j : j = 1, \ldots, u_0\}$). The simulator sets $w_{id_j} = w_j$ and uses the trapdoor to derive v_{id_j} from $w_{id_j} = H_0(id_j, v_{id_j})$. Then it computes
  $$g_{id_j} = y^{e_{id_j}},$$
  where $e_{id_j} = \prod_{i \neq j, i \in U_0} w_{id_i}$. Then the simulator returns the private key (g_{id_j}, v_{id_j}) for identity id_j $(j = 1, \cdots, u_0)$.
- **Query of signature**: The adversary issues signature-queries of m_i $(i = 1, \cdots, l)$ for challenge identity $id^* \in U \backslash U_0$. The simulator selects random number $d_1, \cdots, d_l$

and sets $w_{id^*} = e$, then computes $v_{id^*}, d_i w_{id^*}$, where $w_{id^*} = H(id^*, v_{id^*})$. After that, the simulator derives r_i from $H(m_i, r_i) = d_i w_{id^*}$ and returns $(\sigma_i, r_i, v_{id^*})$ as the signature of message m_i, where $\sigma_i = g^{d_i}$. Note that, $\sigma_i = g^{d_i} = g^{\frac{H(m_i,r_i)}{w_{id^*}}}$. That is, $(\sigma_i, r_i, v_{id^*})$ is a valid signature of message m_i.

- **Forgery**: For the challenge identity id^*, the adversary outputs a signature $(m_0, \sigma, r, v_{id^*})$ such that $\sigma^{w_{id^*}} = g^{H(m_0,r)} \ mod \ n$. Namely, $\sigma^e = y^{wH(m_0,r)}$.

Now we analyze the probability of obtaining a RSA solution for the simulator $\mathcal{C}$. If

$$gcd(H(m_0, r), e) = 1,$$

then the simulator computes

$$x = \sigma^{\frac{gcd(wH(m_0,r),e)}{wH(m_0,r)}}$$

based on Lemma 1. The solution of the given RSA challenge is x. Otherwise, output $\perp$. Thus, in the case of $gcd(H(m_0, r), e) = 1$, the simulator can construct a solver of SRSA problem. Note that e is a prime. Then, we have

$$\varepsilon \approx \frac{e-1}{e}\varepsilon_R.$$

C. OUTSOURCED ALGORITHMS

In this section, we propose two outsourcing algorithms for exponential operation-u^a $(mod \ n)$ to a cloud server. According to the privacy of u and a, the outsourcing algorithms can be divided into two situations: (1) a is secret, u is public; (2) Both u and a are secret. The corresponding algorithms are given as below. That is, $A1(u, a_i) = u^{a_i}$ for secret a_i.

Algorithm 1 ($A1$). Let u be public, and a_i be secret for $i = 1, \ldots, n_0$. The target is to compute u^{a_i} with the help of a cloud server (an untrusted third party).

- **Setup**. The user first computes and keeps $u_0 = u^{a_0}$. Then the user sends $a_i - a_0$ and u to the cloud server.
- **Outsourcing computation**. The cloud returns $u^{a_i - a_0}$ to the user.
- **Output**. The user outputs $u^{a_i} = u^{a_0} \cdot u^{a_i - a_0}$.

Algorithm 2 ($A2$). Let u and a_i be secret for $i = 1, \ldots, n_0$. The target is to outsource u^{a_i} without revealing u and a_i. That is, $A2(u, a_i) = u^{a_i}$ for secret a_i, u.

- **Setup.** The user first computes and keeps $u_0 = u^{a_0}$. Then it randomly chooses a 2×2 invertible matrix H, and sends $a_i - a_0$ and

$$A_i = H \cdot \begin{pmatrix} u & r_i \\ 0 & u^l \end{pmatrix} \cdot H^{-1}$$

to the cloud server, where r_i is randomly selected and $l = 2$ (l can be any small integer).

- **Outsourcing computation**. The cloud server returns $B_i = A_i^{a_i - a_0}$ to the user.
- **Verification and output**. The user calculates $C_i = H^{-1} B_i H$ and gets $(C_i)_{11}, (C_i)_{22}$. It first checks whether $(C_i)_{11}^2 = (C_i)_{22}$ or not. If it holds, then this means $(C_i)_{11} = u^{a_i - a_0}$. The user outsputs $u^{a_i} = u^{a_0} \cdot u^{a_i - a_0}$.

Correctness: The correctness is obtained immediately. Since $HAH^{-1} \cdot HBH^{-1} = HABH^{-1}$, then

$$B_i = A_i^{a_i - a_0} = H \cdot \begin{pmatrix} u & r_i \\ 0 & u^l \end{pmatrix}^{a_i - a_0} \cdot H^{-1}$$
$$= H \cdot \begin{pmatrix} u^{a_i - a_0} & r_i' \\ 0 & (u^l)^{a_i - a_0} \end{pmatrix} \cdot H^{-1}.$$

If the cloud server returns a valid B_i, then $(C_i)_{11} = u^{a_i - a_0}$ and $(C_i)_{22} = u^{2(a_i - a_0)}$.

Note that, the local user only needs one exponential operation as a precalculation. In addition, Algorithm 2 can be used to outsource exponential operations in various situations with respect to u's and a's privacy. In next section, we will adopt the above outsourcing algorithms to construct a lightweight VANET privacy-preserving protocol.

D. PRIVACY-PRESERVING PROTOCOL FOR VANETS

The basic idea of the VANET privacy-preserving protocol is that TA authorizes RSU to act as an agent and run a proxy re-signature algorithm. RSU converts OBU's signature into TA's signature to protect the identity of OBU. At the same time, TA can quickly and accurately trace the real identity of the OBU and revoke this OBU, when any party finds malicious messages. The protocol is given as below.

- **Setup**: TA selects two large primes p and q. Then, $n = pq$. Choose a random element $g \in Z_n^*$, and collision resistant hash functions $H: Z_n^2 \rightarrow Z_n$, $H_0: U \times Z_n \rightarrow Z_n$, where U is the identity set.
  The system master secret key is $sk = (p, q)$ and public key is $pk = (g, n, U, H, H_0)$.
- **Key Generation**: This stage can be divided into three sub-stages.
  - TA picks up e, d such that $e \cdot d \equiv 1 \ (mod \ \varphi(n))$ and publishes e. Then, d is the secret key for TA.
  - OBU randomly chooses x_{OBU} and computes $v_{OBU} = g^{x_{OBU}}$. Then OBU selects k, computes $w_1 = H_1(g^k \| ID)$, $w_2 = k + w_1 \cdot v_{OBU}$ and sends (ID, w_1, w_2, v_{OBU}) to TA, where $H_1 : \{0, 1\}^\lambda \rightarrow Z_n$. If $w_1 = H_1(g^{w_2} \cdot v_{OBU}^{-w_1} \| ID)$, then TA can ensure that v_{OBU} and ID are real identification of the OBU. Finally, TA computes $w_{OBU} = H_0(ID, v_{OBU})$ and sends private key $g_{OBU} = g^{w_{OBU}^{-1}}$ to OBU. Here, TA can use the above outsourcing algorithms, then $g^{w_{OBU}^{-1}} = A1(g, w_{OBU}^{-1})$, $g^{w_2} = A1(g, w_2)$ and $v_{OBU}^{-w_1} = A2(v_{OBU}, -w_1)$.
  - RSU establishes its own public encryption algorithm Enc_{RSU} with public-secret key pair (pk_{RSU}, sk_{RSU}).
- **Key Generation for Re-signature**: TA randomly chooses s_{OBU} and computes $A1(g, s_{OBU}) = g^{s_{OBU}}$. Then RUS's re-signature key for OBU is $(ID, g^{s_{OBU}}, y_{OBU})$, where $y_{OBU} = d \cdot w_{OBU} \cdot s_{OBU}$. At the same time, TA adds $\{ID, g^{s_{OBU}}\}$ into a list T and maintains T for tracing the OBU's real identity.

- **OBU Signature**: The message sent by the vehicle OBU contains four domains: message type ID_{type}, message load payload PL, time-stamp $Time$ and the signature for the first three information, where the payload is composed of vehicle location, direction, speed, traffic incident and other basic information. Time-stamp identifies the exact time of message's generation. Then OBU runs the following algorithms:
  - For message $m = ID_{type}\|PL\|Time$, OBU randomly selects r and runs Algorithm 2 to obtain
  $$\sigma = g_{OBU}^{H(m,r)} = A2(g_{OBU}, H(m,r)).$$
  - OBU uses the public key of RSU to encrypt $M = (ID, v_{OBU}, m, r, \sigma)$, then OBU sends $Enc_{RSU}(M)$ to the RSU.
- **Re-signature**: RSU decrypts $Enc_{RSU}(M)$ to get $M = (ID, v_{OBU}, m, r, \sigma)$, and checks whether $(\sigma)^{H_0(ID,v_{OBU})} = g^{H(m,r)}$ or not. If the equation holds, then RSU uses his re-signature key to compute $\sigma' = \sigma^{(y_{OBU})r}$ and broadcasts $(m, r, \sigma', (g^{s_{OBU}})^r)$, where $\sigma' = A1(\sigma, (ry_{OBU})$.
- **Verification**: Any party can verify the validity of $(m, r, \sigma', (g^{s_{OBU}})^r)$. If $(\sigma')^d = (g^{r\cdot s_{OBU}})^{H(m,r)})$ holds, then the verifier outputs 1, otherwise, outputs 0.
- **Tracing and revocation**: The tracing process is done by TA, and the revocation process is executed by TA and the RSU.
  - **Tracing.** If $(\sigma')^d \neq (g^{r\cdot s_{OBU}})^{H(m,r)})$, TA has access to trace the real identity of the corresponding OBU. TA uses its secret key to compute r^{-1} $(mod\ \varphi(n))$ and $A1(g^{r\cdot s_{OBU}}, r^{-1}) = (g^{r\cdot s_{OBU}})^{r^{-1}} = g^{s_{OBU}}$, then TA finds the corresponding $\{ID, g^{s_{OBU}}\}$ in the local list T.
  - **Revocation.** Once TA finds a malicious vehicle OBU, TA sends $g^{s_{OBU}}$ to the RSU to revoke this OBU. At the same time, TA and RSU delete ID, $g^{s_{OBU}}$ from list T.

The correctness of the scheme is shown as below.

- **Correctness of OBU's signature.** Since $H_0(ID, v_{OBU}) = w_{OBU}$ and
$$\sigma = g_{OBU}^{H(m,r)} = (g^{w_{OBU}^{-1}})^{H(m,r)},$$
then $\sigma^{H_0(ID,v_{OBU})} = \sigma^{w_{OBU}} = g^{H(m,r)}$.
- **Correctness of RSU's re-signature.** Since $e \cdot d \equiv 1\ (mod\ \varphi(n))$ and
$$\begin{aligned}\sigma' &= \sigma^{(y_{OBU})r}\\ &= \sigma^{(d\cdot w_{OBU}\cdot s_{OBU})r}\\ &= H(y^{k_5k_4}, x^{k_5k_2\alpha})\\ &= (g^{w_{OBU}^{-1}H(m,r)})^{(d\cdot w_{OBU}\cdot s_{OBU})r}\\ &= g^{dH(m,r)r\cdot s_{OBU}},\end{aligned}$$
then $(\sigma')^e = (g^{r\cdot s_{OBU}})^{H(m,r)})$.

V. ANALYSIS AND DISCUSSION

In this section, we will present the security and efficiency for the proposed VANET privacy-preserving protocol.

A. SECURITY ANALYSIS

The security of the VANET protocol includes key security, non-forgery, message verifiability, privacy, anti-replay attack and traceability.

- **Key security.** According to the key generation, the secret key of OBU is $g_{OBU} = g^{w_{OBU}^{-1}}$. Although g, w_{OBU} are known to RSU, the RSU fails to compute w_{OBU}^{-1} due to the intractability for factorizing n into p, q. In addition, the RSU cannot solve the secret key d from a system of equations $y_{OBU} = d \cdot s_{OBU} \cdot w_{OBU}$, since s_{OBU} is changeable for different OBU. Thus, the secret key of TA is secure.
- **Non-forgery.** Based on the non-forgery of the IBS scheme, the new protocol also provides the non-forgery.
- **Verifiability.** RSU adopts the public key of OBU to check the validity of message m. After re-signature, other users verify the new signature using TA's public key. Due to the non-forgery of the two signatures, the verifier can ensure the messages' authenticity.
- **Privacy.** The privacy includes the identity's anonymity of OBU and the security of communication between OBU and RSU.
  - TA authorizes RSU to serve as a semi-trusted agent. RSU converts OBU's signature to TA's signature within its re-signature key. This converting can hide the real identity of the vehicle OBU and realize the anonymity of OBU. That is, no one can track the identity of OBU.
  - OBU uses pk_{RSU} to encrypt M and sends the ciphertext to RSU. Only the RSU can decrypt the encrypted message. Thus, the public key encryption ensures the security of communications from OBU to RSU.
- **Anti-replay attack.** The message generated by OBU contains four domains: ID_{type}, payload PL, time-stamp $Time$ and the signature. Thus, RSU can test the existing of attacks when adversary modifies the time-stamp $Time$. The application of time-stamp cannot only guarantee the freshness of messages, but also effectively resist replay message attacks.
- **Traceability.** When the message is a malicious code, TA uses its secret key to compute $g^{s_{OBU}}$ and finds the corresponding real identity ID of OBU, then removes the OBU from the maintained list T. After that, TA sends $(ID, g^{s_{OBU}})$ to RSU, and RSU revokes the qualification of this malicious vehicle OBU. OBU does not participate in the whole process, which effectively ensures the objectivity of traceability. Malicious vehicles will no longer be able to participate in VANET legitimate communications through RSU, thus it cannot continue to break the system.

B. EFFICIENCY ANALYSIS

The efficiency of the proposal for VANETs directly affects its practicability. Now we present the efficiency analysis on storage cost, communication cost and computation cost.

1) STORAGE COST.

We first present the parameter setting in our scheme. IFP for public key $n = p \cdot q$ is the underlying hard problem to ensure the scheme's security. Then, let the secure parameter be $\lambda = \log n \approx 1024$, where p, q are about 512 bits. Now we discuss the storage cost based on the three different parties: TA, OBU and RSU.

- **TA's storage cost**: TA keeps p, q, d as its secret key. Meanwhile, TA needs to maintain a revocation list $T = \{ID, g^{s_{OBU}}\}$, where ID is 32-bit and $g^{s_{OBU}}$ is 1024-bit. Suppose that the number of OBUs is N. Then, TA keeps $1056N + 2048$ bits.
- **OBU's storage cost**: OBU only needs to carry its signature key g_{OBU}, its size is about 1024 bits.
- **RSU's storage cost**: Firstly, RSU carries an encryption secret key sk_{RSU}. At the same time, each RSU acts as a proxy to re-signature and keeps $\{ID, g^{s_{OBU}}, y_{OBU}\}$ for N OBUs. Then, RSU needs to keep $1056 + 2 \cdot 1024 \cdot N$ bits.

TABLE 1. Comparison for communication cost.

	Key generation		Signature		Re-signature		Revocation	
	Mul	Exp	Mul	Exp	Mul	Exp	Mul	Exp
NOP	3	2	0	1	0	3	0	1
OP	5	0	17	0	51	0	1	0

2) COMMUNICATION COST.

We will discuss the communication cost in the following situations:

- **TA-to-OBU**: In the key-generation, TA sends the corresponding secret key g_{OBU} to each OBU, then it needs to transmit data with $1024N$ bits.
- **TA-to-RSU**: There are two rounds communications from TA to RSU. In the key-generation, TA sends re-signature key $\{ID, g^{s_{OBU}}, y_{OBU}\}$ to RSU. In the revocation phase, TA sends $g^{s_{OBU}}$ to RSU for revoking OBU's ID. Thus, TA transmits 3104-bit data.
- **OBU-to-RSU**: OBU sends the encrypted signature to RSU. Suppose that the plaintext and ciphertext for Enc_{RSU} have the same size. In the signature phase, the message m sent by vehicle OBU contains four domains: message type ID_{type}, load payload PL, timestamp $Time$ and the signature $\sigma \ (mod\ n)$ for the first three information. The first three elements are set to be 32-bit, and the signature is about 1024-bit. OBU sends $Enc_{RSU}(ID \| v_{OBU} \| m \| r \| \sigma)$ to RSU, where r is 160-bit. Then, OBU needs to transmit 2336-bit data to RSU.

3) COMPUTATION COST.

We analyze the computation cost with respect to different stages: Key-generation, Signature, Re-signature and Tracing, where the cost of hash computing can be ignored. To show the advantage of the proposed outsourcing algorithms, we discuss non-outsourced protocol and outsourced protocol (note that, we only describe the outsourced one in Section 3.4).

We first present computation cost of the corresponding non-outsourced privacy-preserving VANET protocol.

- In the key generation, TA calculates OBU's secret key $g_{OBU} = g^{w_{OBU}^{-1}}$ and TA needs a multiplication for getting w_{OBU}^{-1} and an exponential (Exp) operation modulo n. In addition, TA creates re-signature key for RSU, and computes $g^{s_{OBU}}, y_{OBU} = e \cdot w_{OBU} \cdot s_{OBU}$. Then, TA requires two exponential operations and three multiplications (Mul) in the key-generation stage.
- In the signature phase, OBU only calculates $\sigma = g_{OBU}^{H(m,r)}$ and it needs one exponential operation.
- In the re-signature phase, RSU checks whether $(\sigma)^{H_0(ID, v_{OBU})} = g^{H(m,r)}$ or not. Meanwhile, it computes re-signature $\sigma' = \sigma^{(y_{OBU})r}$. Thus, RSU needs three exponential operations.
- In the tracing phase, TA executes one exponential operation for computing $(g^{r \cdot s_{OBU}})^{r^{-1}}$.

Now we analyze the corresponding outsourced scheme. For each outsourced algorithm, the user needs to do one exponential operation as pre-calculation. According to applicable circumstances of the proposed outsourced algorithms, we see that (a) the user only needs one multiplication for computing one exponential operation in Algorithm 1; (b) the user requires 17 multiplications for computing one exponential operation in Algorithm 2. Then we give a comparison table for the computation cost between the non-outsourced protocol (NOP) and the outsourced protocol (OP).

Next we present the graphic comparisons for the computation cost based on four stages, where we don't depict the pre-computation for one exponential operation in the outsourced protocol. In Fig. 2, "x axis" denotes the number of vehicles

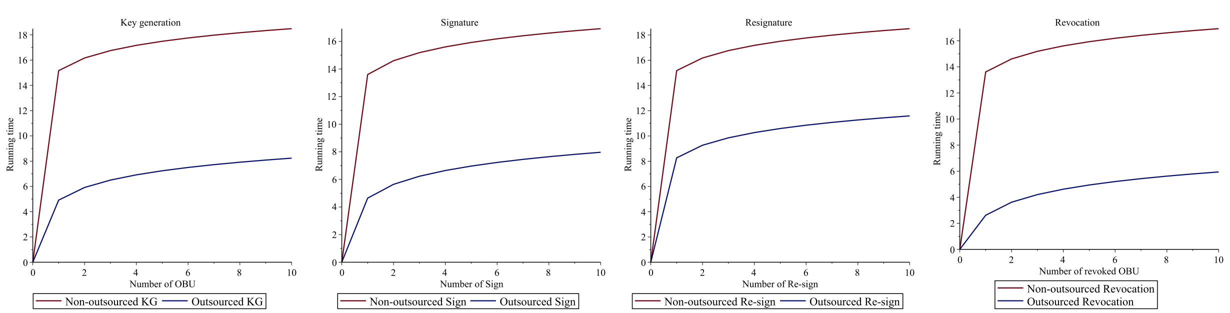


FIGURE 2. Comparison between non-outsourced and outsourced protocols.

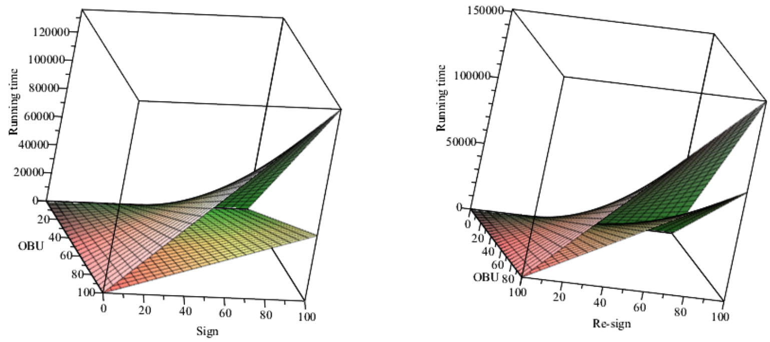


FIGURE 3. Comparison for signature and re-signature stages.

(OBU) or the number of signatures (or re-signatures) and "y axis" denotes the corresponding running time in microseconds (ȩÌs). Besides, since the outsourced scheme only uses multiplication module n, thus, to explicitly depict the huge gap between the two schemes, we adopt the logarithmic scales towards "y axis". Furthermore, in Fig. 3, we provide two three-dimensional comparison graphs for signature and re-signature stages, where "x axis" denotes the number of OBUs and "y axis" indicates the number signatures (or re-signatures), "z axis" is the running time.

Remark: We test the running time of one multiplication operation and one exponential operation with 1024-bit by using C ++ on a virtual Linux machine over a computer with Intel I7 6500U CPU and 16 GB memory. The results show that one multiplication operation needs 6.0471 μs and one exponential operation needs 12.384 ms.

VI. CONCLUSION

In this paper, we first propose an identity-based signature (IBS) that is unforgeable against chosen-message attack without random oracle. Then, to cut down the computational cost, we present two secure and efficient outsourcing algorithms for the exponential operations. These outsourcing algorithms have general applicability for most cryptosystems within exponential operations. Furthermore, we construct a privacy-preserving protocol in VANETs based on the outsourcing computations and the above IBS scheme, where a proxy re-signature is presented and introduced for authentications. The proposed VANET protocol provides anonymity, traceability and privacy. In addition, with respect to the efficiency, our schemes don't need pairing operations and exponential operations. Thus, the calculation burdens for VANET systems can be significantly reduced. In the future work, we will design stronger VANETs privacy-preserving protocols based on homomorphic signature schemes [5], [21], [22].

REFERENCES

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[3] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: A generic cloud computing model for vehicular Ad Hoc networks," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 96–102, Feb. 2015.

[4] D. Cash, R. Dowsley, and E. Kiltz, "Digital signatures from strong RSA without prime generation," in *Proc. PKC*, 2015, pp. 217–235.

[5] W. Chen, H. Lei, and K. Qi, "Lattice-based linearly homomorphic signatures in the standard model," *Theor. Comput. Sci.*, vol. 634, pp. 47–54, Jun. 2016.

[6] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2014, pp. 148–162.

[7] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2386–2396, Sep. 2014.

[8] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Veh. Commun.*, vol. 14, pp. 15–25, Oct. 2018.

[9] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[10] C.-Z. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, "Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack," *Inf. Sci.*, vol. 444, pp. 72–88, May 2018.

[11] M. K. Giluka, T. V. Pasca, T. Priyadarshi, and B. R. Tamma, "Enhanced class based dynamic priority scheduling to support uplink IoT traffic in LTE-A networks," *J. Netw. Comput. Appl.*, vol. 107, pp. 93–112, Apr. 2018.

[12] S.-J. Horng *et al.*, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[13] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT," *IEEE Access*, vol. 6, pp. 20085–20103, 2018.

[14] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and T. Yi, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *J. Netw. Comput. Appl.*, vol. 106, pp. 117–123, Mar. 2018.

[15] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," *Knowl.-Based Syst.*, vol. 79, pp. 18–26, May 2015.

[16] C. Li, X. Zhang, H. Wang, and D. Li, "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks," *Sensors*, vol. 18, no. 1, p. 194, 2018.

[17] J. Li *et al.*, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Veh. Commun.*, vol. 13, pp. 104–113, Jul. 2018.

[18] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2201–2210, Aug. 2014.

[19] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 425–437, Feb. 2015.

[20] T. Li, C. Gao, L. Jiang, W. Pedrycz, and J. Shen, "Publicly verifiable privacy-preserving aggregation and its application in IoT," *J. Netw. Comput. Appl.*, vol. 126, pp. 39–44, Jan. 2019.

[21] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[22] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[23] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[24] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229–1237.

[25] X. Ma, J. Li, and F. Zhang, "Outsourcing computation of modular exponentiations in cloud computing," *Cluster Comput.*, vol. 16, no. 4, pp. 787–796, 2013.

[26] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. ACM Workshop Secur. Ad Hoc Sensor Netw. (SASN)*, 2005, pp. 11–21.

[27] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3697–3710, Aug. 2015.

[28] G. Sun *et al.*, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *J. Netw. Comput. Appl.*, vol. 89, pp. 3–13, Jul. 2017.

[29] Q. Wu, J. Domingo-Ferrer, and Ú. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[30] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.

[31] X. Zhang, X. Chen, J. Wang, Z. Zhan, and J. Li, "Verifiable privacy-preserving single-layer perceptron training scheme in cloud computing," *Soft Comput.*, vol. 22, pp. 7719–7732, Dec. 2018.

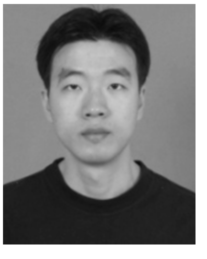
[32] X. Zhang, Y.-A. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over VoLTE via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[33] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and challenges," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, 2014.

ZHIJUN WEI was born in 1970. He received the bachelor's degree from the Hebei University of Science and Technology, in 1995, and the master's degree from the Beijing Institute of Technology, in 2011. He is currently a Lecturer with the Beijing Institute of Technology, Zhuhai, He main research interests include Java EE, computer software and theory, and encryption algorithm.

JING LI was born in 1986. She received the B.S. degree from Inner Mongolia Normal University, in 2010, the M.S. degree from Shananxi Normal University, in 2013, and the Ph.D. degree from the Beijing University of Posts and Telecommunications. She is currently with Guangzhou University. Her research interests include cloud computing, applied cryptography, and privacy-preserving.

XIANMIN WANG was born in 1984. He received the B.S. degree from Suzhou University, Jiangsu, China, in 2006, the M.S. degree in computer science from the Jiangxi University of Science and Technology, Jiangxi, China, in 2013, and the Ph.D. degree in computer science from Beihang University, in 2017. He is currently with the School of Computer Science, Guangzhou University. His research interests include deep learning, image processing, and understanding.



CHONG-ZHI GAO was born in 1976. He received the Ph.D. degree in applied mathematics from Sun Yat-sen University, in 2004. He is currently a Professor with the School of Computer Science and Educational Software, Guangzhou University. His research interests include cryptography and privacy in machine learning.