This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

LPPA: Lightweight Privacy-preserving Authentication from Efficient Multi-key Secure Outsourced Computation for Location-based Services in VANETs

Jun Zhou, *Member, IEEE* Zhenfu Cao, *Senior Member, IEEE* Zhan Qin, *Member, IEEE*
Xiaolei Dong, Kui Ren, *Fellow, IEEE*

Abstract—Location-based service (LBS) in vehicular ad hoc networks (VANETs) has significantly benefited information acquisition from geographically based social networking. Authentication guarantees the unforgeability and the effectiveness of LBS information. Unfortunately, owing to a large quantity of redundant or useless LBS messages disseminated in VANETs, the heavy authentication overhead of the existing work adopting a periodically released authentication key, filtering with message identifiers or exploiting public key (fully) homomorphic encryption (FHE), is either intolerable by resource-constrained on-board units (OBUs) or inappropriate to the realtime controlling requirement for VANETs. In this paper, an efficient multi-key secure outsourced computation scheme MSOC without exploiting public key FHE is firstly proposed, in the setting of two non-colluding servers, namely the cloud and the cryptographic service provider (CSP). Then, based on MSOC, an efficient and secure comparison protocol LSCP is devised, without the interaction between the server and the users. Furthermore, a lightweight privacy-preserving authentication protocol LPPA for LBS in VANETs is proposed, by eliminating duplicate and useless encrypted LBS messages before authentication is executed, through a newly devised efficient privacy-preserving information filtering system. Both user's location privacy and interest privacy are well protected against even the collusion between the roadside units (RSUs) serving as the cloud (or CSP) and malicious users. Especially, the property of ciphertext re-encryption of our proposed MSOC also guarantees the interest pattern privacy whether two users accept the same LBS information. Finally, formal security proof and extensive simulation results verify the effectiveness and practicability of our proposed LPPA.

Index Terms—Lightweight authentication, privacy-preserving filtering, multi-key secure outsourced computation, efficiency, location based service, VANETs

1 Introduction

Vehicular ad hoc network (VANET) has been increasingly becoming one of the most convincing platforms for enhancing the road safety and providing location-based services (LBS) on road in the next generation of communications [1,2]. Vehicles are able to communicate with each other (V-2-V Communication) and with the roadside infrastructures (V-2-I Communication). Location-based service is a derivative application of VANETs, where vehicles collect and broadcast passing-by services such as traffic information, weather information, shop or restaurant recommendation in their neighborhood and only the authorized vehicular users who subscribed location-based service can successfully decrypt and access the provided information.

Unfortunately, besides LBS ciphertext access control, it is also frequently threatened by repudiation and modification attacks where the adversary intends to forge the vehicle identity and manipulate LBS information for his own interest [3,4,5]. These false LBS information would lead to users' inconvenience, potential traffic disasters and should be prevented from dissemination in VANETs. Moreover, the location privacy of vehicles is required to be well protected since a sequence of positions one specific vehicular user visited would disclose his private living habit.

Recently, X. Lin et al. proposed a timed efficient and secure vehicular communication (TSVC) scheme with privacy preservation [4]. By utilizing the techniques of hash chain and message authentication code, it aims to minimize both the signature generation and verification overhead on vehicle's side without compromising the underlying security and privacy requirements. However, to resist replay attack, it is required in [4] that the private authentication key has to be released a period of waiting time δ after message dissemination, which is necessary to be longer than the maximum message transmission delay from the source to the destination. Therefore, TSVC only adapts to the scenario of disseminating routine LBS contents that are released every regular time interval, but not the emergency situations requiring timely authentication in VANETs.

To further reduce the authentication cost, X. Lin et al.

- *J. Zhou (corresponding author), Z. Cao and X. Dong are with Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai, China.*
  E-mail: {jzhou, zfcao, dongxiaolei}@sei.ecnu.edu.cn
- *Z. Qin and K. Ren are with the Institute of Cyberspace Research, Zhejiang University, Hangzhou, China.*
  Email: {qinzhan, kuiren}@zju.edu.cn

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

proposed an efficient cooperative message authentication scheme in VANETs [5]. It minimizes redundant authentication efforts from the receiver's aspect in that each message with a distinct identifier is verified by a single vehicular user which reports afterwards the verification result in its neighborhood. Unfortunately, the duplicate/redundant messages collected by vehicles passing by the same road section have not been filtered (i.e. messages with different identifiers are likely associated to the same content and become redundant), which would occupy a great deal of unnecessary communication bandwidth and computational cost for authentication. Besides, it is likely to charge a specific vehicular user more computational resources to authenticate an irredundant but useless LBS message, namely out of the range of his interest. Finally, the intervention of a online Trusted Authority (TA) for token generation incurs additional interactions with vehicular users.

More seriously, the vehicular user's location privacy in the existing work [4,5,10] was not directly hidden, but indirectly protected by the technique of multiple pseudonyms. However, it was reported that a series of locations of the target vehicle with specific pseudonyms can be utilized together with some background information to infer the true identity of the user [11]. On the other hand, the periodically updating pseudonyms and their corresponding anonymous certificate generation and verification would also bring a large amount of computational and communication cost on the user's end.

Privacy-preserving message filtering exploiting the technique of secure outsourced computation is a convincing solution. Most of the state-of-the-art [15-18,20-24,29,34] exploited public key (fully) homomorphic encryption (FHE) [19,31,32] on each data input to achieve secure delegated function evaluation in the encrypted domain. Unfortunately, the heavy computational and communication complexity are intolerable by resource-constrained vehicular users. To address these issues, in this paper, a lightweight privacy-preserving authentication scheme LPPA for location-based service in VANETs is proposed. The main contributions are presented as follows.

Firstly, without exploiting public key fully homomorphic encryption (FHE), an efficient multi-key secure outsourced computation scheme MSOC is proposed, by exploiting any one-way trapdoor permutation (OWTP) only once in the offline phase to encrypt all data inputs $m_{i,i'}(i = 1, 2, \cdots, n_S; i^{'} = 1, 2, \cdots, n_i)$ in a batch manner, where each sender Sen_i hold n_i messages.

Then, based on MSOC, a lightweight and secure comparison protocol LSCP is devised without interactions between the cloud and users. The issue of privacy-preserving integer comparison is transformed into evaluating an underlying judging polynomial in the encrypted domain.

Finally, by exploiting our devised MSOC and LSCP, a lightweight privacy-preserving authentication protocol LPPA for location-based services in VANETs is proposed. It optimizes both computational and communication effort for authentication, by individually filtering the transmitted LBS messages in the encrypted domain for each user from both factors of redundancy and usefulness.

Finally, formal security proof shows our proposed LPPA can effectively protect the location privacy and the interest privacy of vehicular users. Especially, the property of ciphertext re-encryption of our proposed MSOC also guarantees the interest pattern privacy whether two vehicular users accept the same LBS information for their common interest. The extensive simulations demonstrate the efficiency advantages of our proposed MSOC and LPPA over the state-of-the-art in the aspects of both computational and communication overhead.

The remainder of this paper is organized as follows. We discuss related work in the next section. In Sec. 3, the preliminaries, network architecture and security models are presented. Then, an efficient multi-key secure outsourced computation scheme MSOC, a lightweight and secure comparison protocol LSCP and a lightweight privacy-preserving authentication protocol LPPA for LBS in VANETs are respectively proposed in Sec. 4 and Sec. 5. In Sec. 6 and Sec. 7, we give the formal security proof and performance evaluations of our proposed MSOC, LSCP and LPPA. Finally, we conclude our paper in Sec. 8.

2 Related Work

Recently, there have appeared several research focusing on secure and efficient packet forwarding in VANETs [4,5,7-11,14,22]. Lin et al. proposed a time efficient and secure vehicular communication (TSVC) scheme [4] by exploiting a carefully designed symmetric MAC tag for message authentication and the efficiency was significantly enhanced compared to the conventional PKI based signatures [30]. Unfortunately, it disables to handle the emergency cases where LBS messages need realtime authentication. Zhang et al. proposed a RSU-aided message authentication scheme RAISE [9] where RSUs are exploited to verify the authenticity of the messages disseminated by vehicles. Lin et al. proposed cooperative message authentication protocols [5,10] where each vehicle probabilistically authenticates a certain percent of received messages according to their reserved OBU resources and reports the verification results in its neighborhood, under the assumption that the vehicles are willing to collaborate in message authentication. Unfortunately, the duplicate messages collected by vehicles are not filtered, which still occupies a great deal of both redundant computational and bandwidth resources. Furthermore, the intervention of a online trusted authority (TA) for token generation and the multiple-pseudonym technique in [4,5] to achieve location privacy also incur considerable overhead to resource-constrained vehicular users. Recently, an efficient privacy-preserving relay filtering scheme PRe-Filter was proposed for delay tolerant network(DTN) in vehicular communications [14]. It avoids the junk packet delivery by explicitly setting and distributing an interest policy by message receivers for their friends where the interest privacy of vehicular users would be disclosed.

On the other hand, the issue of multi-key secure outsourced computation has been increasingly studied [15-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

18,20-24,29,34]. A. López-Alt et al. [18] proposed a secure multiparty computation on the cloud via multi-key public key FHE implemented by Brakerski's public key FHE [19]. A. Peter et al. presented efficient outsourcing multiparty computation using public key BCP cryptosystem [23]. Recently, X. Liu et al. [17,20,24] proposed privacy-preserving outsourced computation on public rational numbers with multiple keys. For privacy-preserving message recommendation and filtering, Q. Tang et al. [15] and S. Badsha et al. [16] respectively devised privacy-preserving context-aware and user-based recommendation systems. Unfortunately, most of the state-of-the-art stated above exploited public key (fully) homomorphic encryption [19,31,32] on each data input, and the heavy computational and communication complexity are intolerable by resource-constrained local users. J. Zhou et al. proposed a privacy-preserving outsourced computation without public key FHE [22], unfortunately it is only applied to the single key scenario where multiple data inputs are generated from one single user. It cannot be directly applied to privacy-preserving LBS in which vehicular users are required to send LBS messages together with their generated time, locations and ratings encrypted under different keys.

In this paper, our LPPA is proposed by designing an efficient multi-key secure outsourced computation scheme MSOC without public key FHE, which filters both duplicate and useless LBS messages for further efficiency enhancement before authentication and well protects location privacy, interest privacy and interest pattern privacy for vehicular users.

3 Network Architecture and Security Model

3.1 Preliminaries

One-way Trapdoor Permutation [22]: A one-way trapdoor permutation generator is a probabilistic polynomial time (PPT) algorithm $\mathcal{G}$ which outputs a triple of functions (f, f^{-1}, d). The former two are deterministic and the latter is probabilistic. It is required that $[d(1^\lambda)]$ is a subset of $\{0,1\}^\lambda$ and that f, f^{-1} are permutations on $[d(1^\lambda)]$ that are inverses of each other, where the notation $[\circ]$ refers to the support (i.e. the set of elements with positive probability) of $\circ$ distributed over a probability space, and λ is the security parameter. For all probabilistic polynomial time adversary $\mathcal{A}$,

$$\begin{aligned}\epsilon(\lambda) \quad = \quad & Pr[(f, f^{-1}, d) \leftarrow \mathcal{G}(1^\lambda); \\ & x \leftarrow d(1^\lambda); y \leftarrow f(x) : \mathcal{A}(f, d, y) = x]\end{aligned}$$

is negligible in λ, where f, f^{-1}, d are all computable in polynomial time $t(\lambda)$.

Euler's Theorem [33]: Let n, a be two positive integers such that the greatest common divisor $gcd(n, a) = 1$, we have

$$a^{\varphi(n)} \equiv 1 \ mod \ n,$$

where $\varphi(n)$ refers to the Euler's totient function taking n as input.

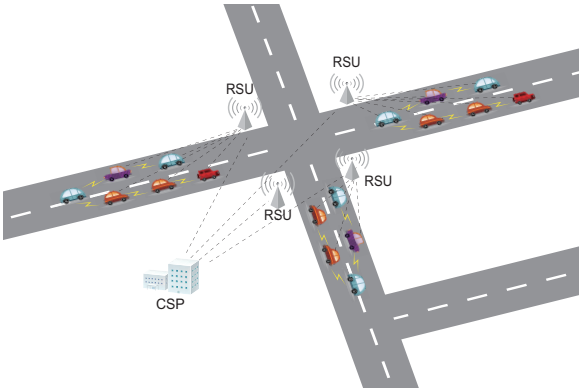


Fig. 1: Network Architecture of Privacy-preserving Location-based Service in VANETs

Chinese Remainder Theorem [33]: Let $m_1, m_2, \cdots, m_k$ be k positive integers which are coprime with each other, $m = \prod_{i=1}^{k} m_i$ and $m = m_i M_i (i = 1, 2, \cdots, k)$. There exists one and only one solution for the following congruences

$$\begin{aligned} & x \equiv b_1 \ mod \ m_1, \\ & x \equiv b_2 \ mod \ m_2, \\ & \cdots, \\ & x \equiv b_k \ mod \ m_k, \end{aligned}$$

that $x \equiv M_1^{'} M_1 b_1 + M_2^{'} M_2 b_2 + \cdots + M_k^{'} M_k b_k \ mod \ m$, where $M_i^{'} M_i \equiv 1 \ mod \ m_i (i = 1, 2, \cdots, k)$.

3.2 Network Architecture

In this subsection, we present the architecture of location-based service in VANETs. Vehicles communicate with each other in their communication range and with the roadside units (RSUs) in their neighborhood that are appropriately deployed along roads. It is of an overwhelmingly high probability that the vehicles passing by the same road section would generate and broadcast the same (duplicate) LBS contents about its surroundings [12,13]. The OBU devices equipped on vehicles are assumed to be resource-constrained and vulnerable to various attacks. The RSUs and the cryptographic service provider (CSP) works under the semi-trusted environment and cannot collude with each other. Fig. 1 demonstrates the network architecture of privacy-preserving location-based service in VANETs: 1) Vehicles running along the streets generate and broadcast the encrypted LBS messages in their neighborhood, which can be received by other users within the communication range by a single hop, or by multiple hops relay for the ones outside the communication range; 2) Each vehicular user rates on each LBS message it receives and sends the encrypted ratings to the nearby RSU. The RSU serves as the cloud server and cooperates with the CSP to filter duplicate and useless LBS messages individually for each user in the encrypted domain; 3) The RSU returns the encrypted rating predictions and the authorized users can decide, authenticate and recover the useful LBS messages by decrypting both the predicted ratings and the encrypted LBS messages.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

3.3 Security Model

In this subsection, we firstly give the definition of our proposed MSOC. Based on it, the security model of our proposed efficient multi-key secure outsourced computation scheme MSOC is given, under the setting of two non-colluding servers, namely the cloud and the CSP. Finally, we identify the security requirements of our proposed LPPA which is constructed on the proposed MSOC as building block.

3.3.1 Definition of the Proposed MSOC

The proposed MSOC comprises the following four algorithms which are defined as follows.

MSOC.Setup(1^λ): It takes the security parameter 1^λ as input and outputs the public parameters PPR and the secret keys SK for the cloud server SER, the CSP and the receiver REC.

MSOC.KeyGen(PPR): It takes PPR as input and outputs the temporary public keys $pbk_i(i = 1, 2, \cdots, n_S)$ and secret keys pvk_i for each sender Sen_i, together with the temporary public key pbk_{CSP} and secret key pvk_{CSP} for the CSP.

MSOC.Enc($PPR, pbk_i, pvk_i, m_{i,i'}$): It takes PPR, the temporary public keys $pbk_i(i = 1, 2, \cdots, n_S)$, the secret keys pvk_i of senders Sen_i and the messages $m_{i,i'}(i = 1, 2, \cdots, n_S; i' = 1, 2, \cdots, n_i)$ as input (i.e. there exist totally n_S senders, each of which holds n_i messages as data inputs), and outputs the ciphertext C_{Sen_i}.

MSOC.Eval($PPR, F, sk_{f,ser}, sk_{f,csp}, C_{Sen_i}(i = 1, 2, \cdots, n_S)$): It takes PPR, function F, secret key SK and ciphertext C_{Sen_i} as input, and outputs the function evaluation ciphertext C_F.

MSOC.Dec($PPR, sk_{f,rec}, C_F$): It takes PPR, secret key SK and the ciphertext C_F as input, and outputs the function evaluation result $F(m_1, m_2, \cdots, m_n) = F(m_{1,1}, \cdots, m_{1,n_1}, \cdots, m_{n_S,1}, \cdots, m_{n_S,n_{n_S}})$ where $n = \sum_{i=1}^{n_S} n_i$.

3.3.2 Security Model of the Proposed MSOC

We firstly give the formal security model for the data privacy of our proposed MSOC, then we present the security model for the whole protocol in the ideal/real paradigm.

Data Privacy: We take input privacy to detail the formal security model and the output privacy can be similarly derived since they are encrypted in the same form of encryption. For input privacy, we mainly focus on the security of the input encryption algorithm **MSOC.Enc** that guarantees the input indistinguishability against adaptive chosen ciphertext attack (CCA2) in the random oracle model, and the formal security model is presented as follows.

Initialization Phase: On input 1^λ, the simulator $\mathcal{B}$ runs the trapdoor permutation generator $\mathcal{G}$ to output a pair of permutations f, f^{-1} on $\{0,1\}^{2\lambda}$. We formalize the collusion among the CSP, a subset of corrupted senders and the malicious receiver. The collusion with the cloud server can be similarly formulated. The adversary $\mathcal{A}$ queries a key generation oracle to obtain the public keys $pk_{f,ser}, pk_{f,csp}, pk_{f,rec}, pbk_i(i = 1, 2, \cdots, n_S), pbk_{CSP}$, the secret key of the malicious receiver $sk_{f,rec}$, the secret keys $pvk_i(Sen_i \in T)$ where $T \subset N_{Sen}$ is a subset of corrupted senders in $N_{Sen} = \{Sen_1, Sen_2, \cdots, Sen_{n_S}\}$, the secret key and the temporary secret key of the CSP $sk_{f,csp}, pvk_{CSP}$.

Query Phase: The adversary $\mathcal{A}$ makes polynomially-bounded number of queries to the decryption oracle $\mathcal{O}^{Dec}$ and the random oracle $\mathcal{O}^{H_0}$ at most q_D, q_{h_0} times where $q_D + q_{h_0} \leq poly(\lambda)$ in total. The adversary respectively submits $C_{Sen_i}(Sen_i \in N_{Sen} \setminus T)$ and random strings $\eta_0 \in \{1\}^*$ to $\mathcal{O}^{Dec}$ and $\mathcal{O}^{H_0}$, and receives $MSOC.Dec(PPR, SK, C_{Sen_i})$ and a random string $h_0 \in \{0,1\}^{2\lambda}$ as the responses.

Challenge Phase: The adversary submits two messages $m_{i,i',0}, m_{i,i',1}$ associated to the uncorrupted sender $Sen_i \in N_{Sen} \setminus T$ to the simulator, where $|m_{i,i',0}| = |m_{i,i',1}| = 2\lambda$. On input $m_{i,i',0}, m_{i,i',1}$, the simulator flips a coin and randomly selects $\beta \in_R \{0,1\}$ and outputs $c^*_{i,i'} \leftarrow_R MSOC.Enc(PPR, pbk_i, pvk_i, m_{i,i',\beta})$ as the challenge ciphertext to the adversary.

Adaptive Query Phase: The adversary continues to make queries to the decryption oracle $\mathcal{O}^{Dec}$ and the random oracle $\mathcal{O}^{H_0}$ with the restriction that the challenge ciphertext $c^*_{i,i'}$ is not allowed to be submitted to $\mathcal{O}^{Dec}$.

Guess Phase: The adversary outputs $\beta' \in \{0,1\}$. If $\beta' = \beta$, we mean the adversary has successfully defeated the input privacy of the proposed MSOC.

Definition 2. Assume the CCA2 advantage of the adversary $\mathcal{A}$ against the input privacy of the proposed MSOC at the security parameter λ to be $AdvCCA^{MSOC}_{\mathcal{A}(t,poly(\lambda))}(\lambda) = |Pr[\beta' = \beta] - \frac{1}{2}|$ in the security game presented above. Then, we say the proposed MSOC achieves input privacy against adaptive chosen ciphertext attack if and only if for all probabilistic and polynomially-bounded adversary $\mathcal{A}$ running in time at most t and making totally at most $poly(\lambda)$ queries to the oracles $\mathcal{O}^{H_0}$ and $\mathcal{O}^{Dec}$,

$$AdvCCA^{MSOC}_{\mathcal{A}(t,poly(\lambda))}(\lambda) \leq \epsilon(\lambda), \tag{1}$$

where $\epsilon(\lambda)$ is a negligible function in λ.

Security for the Whole Protocol: We give the security model of the whole protocol using an ideal/real paradigm. We define an ideal world in which the function evaluation of F is executed through a trusted functionality Fun that receives data inputs $m_{i,i'}(i = 1, 2, \cdots, n_S; i' = 1, 2, \cdots, n_i)$ from each sender Sen_i, computes $y = F(m_1, m_2, \cdots, m_n) = F(m_{1,1}, \cdots, m_{1,n_1}, \cdots, m_{n_S,1}, \cdots, m_{n_S,n_{n_S}})$ where $n = \sum_{i=1}^{n_S} n_i$ and gives y to some receiver either in N_{Sen} or $U \setminus N_{Sen}$ where U denotes the universe of all users. It is noted that in the ideal world, the only information that any user learns is its own data input (if it has) and the output

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

y. On the other hand, a real world where all users in N_{Sen} and the receiver interactively to run the protocol MSOC.

We use $Ideal_{Fun,\mathcal{S}}(\vec{m})$ and $Real_{MSOC,\mathcal{A}}(\vec{m})$ to respectively denote the joint output of an ideal world adversary $\mathcal{S}$, all senders in N_{Sen} and the receiver in an ideal execution with functionality Fun and inputs $\vec{m} = (m_1, m_2, \cdots, m_n)$, and the joint output of a real world adversary $\mathcal{A}$, all senders in N_{Sen} and the receiver in an execution of protocol MSOC with inputs $\vec{m} = (m_1, m_2, \cdots, m_n)$. Then, we say that the protocol MSOC securely implements Fun, if for every real world adversary $\mathcal{A}$, there exists an ideal world adversary $\mathcal{S}$ with access to $\mathcal{A}$ in a black-box manner such that for all input vectors $\vec{m}$,

$$Ideal_{Fun,\mathcal{S}}(\vec{m}) \approx_c Real_{MSOC,\mathcal{A}}(\vec{m}). \quad (2)$$

3.3.3 Security Requirements of the Proposed LPPA

The proposed LPPA aims to achieve the following security goals under the assumption that the RSU does not collude with the CSP.

Location Privacy. Location privacy refers to the realtime positions together with the time each vehicular user visited is required to be protected against the collusion between malicious users and the RSU or the CSP.

Interest Privacy. Interest privacy refers to each vehicular user's ratings on different LBS messages should be protected against the collusion between malicious users and the RSU or the CSP.

Interest Pattern Privacy. Interest pattern privacy refers to the RSU or the CSP cannot tell whether two vehicular users have the common interest on the same LBS message, namely whether both of them accept the same LBS message as neither redundant nor useless.

4 THE PROPOSED MSOC

In this section, an efficient multi-key secure outsourced computation scheme MSOC is proposed, without exploiting public key FHE. In the setting of our proposed MSOC, it is assumed that each sender $Sen_i (i = 1, 2, \cdots, n_S)$ holds n_i messages $m_{i,i'} (i' = 1, 2, \cdots, n_i)$ and uploads the ciphertexts of its data inputs encrypted using its own keys. Without loss of generality, a pair of non-colluding cloud server SER and cryptographic service provider CSP collaborate to evaluate the outsourced function, namely the multivariate polynomial $F(x_1, x_2, \cdots, x_n) = \sum_{j=1}^{K} a_j \prod_{l=1}^{n} x_l^{t_{l,j}}$ of degree deg_F in the encrypted domain where $n = \sum_{i=1}^{n_S} n_i$. Finally, the authorized receiver REC can successfully decrypt the multivariate polynomial evaluation result. Note that $\cup_{l=1}^{n}\{m_l\} = \cup_{i=1,i'=1}^{n_S,n_i}\{m_{i,i'}\}, \cup_{l=1}^{n}\{t_{l,j}\} = \cup_{i=1,i'=1}^{n_S,n_i}\{t_{i,i',j}\}$, namely there exists a bijection on the indexes from (i, i') to l. Table 1 shows the notations used in MSOC. The proposed MSOC comprises the following four algorithms **Setup**, **KeyGen**, **Enc**, **Eval** and **Dec** which are detailed as follows.

TABLE 1: Notation Description for MSOC

Notation	Description
$m_{i,i'}$	The i'-th message held by sender Sen_i
$F(x_1, \cdots, x_n)$	The multivariate polynomial for multi-key secure outsourced computation
a_j	The coefficient of the j-th item $Item_j$ in multivariate polynomial F
K	The total number of items in multivariate polynomial F
$t_{l,j}$	The degree of input x_l in the j-th item $Item_j$ of multivariate polynomial F
deg_j	The degree of the j-th item $Item_j$ as $\sum_{l=1}^{n} t_{l,j}$
deg_F	The degree of multivariate polynomial F as $max(deg_1, deg_2, \cdots, deg_K)$

MSOC.Setup (1^λ): On input 1^λ where λ is the security parameter, it runs a trapdoor permutation generator denoted as a probabilistic polynomial time (PPT) algorithm $\mathcal{G}$ and outputs a pair of permutations (f, f^{-1}) on $\{0,1\}^{2\lambda}$ with three pairs of public key and secret key $(pk_{f,ser}, sk_{f,ser})$, $(pk_{f,csp}, sk_{f,csp})$ and $(pk_{f,rec}, sk_{f,rec})$ that are respectively assigned to the cloud server SER, the cryptographic service provider CSP and the receiver REC. It also outputs two cryptographic hash functions $H_0, H_1 : \{0,1\}^* \to \{0,1\}^{2\lambda}$. The public parameters are $PPR = (pk_{f,ser}, pk_{f,csp}, pk_{f,rec}, H_0, H_1)$. The secret keys $SK = (sk_{f,ser}, sk_{f,csp}, sk_{f,rec})$ are respectively kept private by the cloud server SER, the cryptographic service provider CSP and the receiver REC.

MSOC.KeyGen(PPR): The system initializes an integer $N_0 \in \{0,1\}^{2\lambda}$ and sets the message space (together with the intermediate and final function evaluation result space) to be $\mathbb{Z}_{N_0}^*$, where N_0 can be flexibly adjusted according to various computing requirements. Each sender Sen_i randomly selects three big primes p_i, q_i, s_i of size $|p_i| = |q_i| = |s_i| = \lambda$, computes $N_i = p_i q_i$ such that $N_i \geq N_0$, $T_i = p_i q_i s_i$, and p_i^{-1}, q_i^{-1} such that $p_i^{-1} p_i \equiv 1 \ mod \ q_i$ and $q_i^{-1} q_i \equiv 1 \ mod \ p_i$. The temporary public key and secret key of sender Sen_i are $pbk_i = T_i$ and $pvk_i = (p_i, q_i, s_i, N_i)$. The CSP randomly selects three primes p, q, s of size $|p| = |q| = |s| = \lambda$, computes $N = pq$ such that $N \geq N_0$ and $T = pqs$, where its temporary public key $pbk_{CSP} = T$ and the temporary secret key $pvk_{CSP} = (p, q, s, N)$.

MSOC.Enc$(PPR, pbk_i, pvk_i, m_{i,i'} (i = 1, 2, \cdots, n_S; i' = 1, 2, \cdots, n_i))$: Each sender Sen_i holding message $m_{i,i'}$ computes $m_{i,i',p_i} = m_{i,i'} \ mod \ p_i$ and $m_{i,i',q_i} = m_{i,i'} \ mod \ q_i$. Then, it randomly selects $r_i, r_{i,i'} \in_R \{0,1\}^{2\lambda}$ with the condition that $r_i \in \mathbb{Z}_T^*$ and computes

$$\begin{aligned} C_{i,ser} &= f_{pk_{f,ser}}(r_i), C_{i,csp} = f_{pk_{f,csp}}(N_i), \\ C_{i,i'} &= r_i(p_i^{-1} p_i m_{i,i',q_i}^{q_i} + q_i^{-1} q_i m_{i,i',p_i}^{p_i}) \\ &\quad + r_{i,i'} N_i \ mod \ T_i, \\ C'_{i,ser} &= H_0(r_i \parallel C_{i,1} \parallel \cdots \parallel C_{i,n_i}), \\ C'_{i,csp} &= H_0(N_i \parallel C_{i,1} \parallel \cdots \parallel C_{i,n_i}). \end{aligned} \quad (3)$$

Finally, each sender Sen_i sends $C_{Sen_i} = (C_{i,ser}, C_{i,csp}, C_{i,i'}, C'_{i,ser}, C'_{i,csp})$ to the cloud server

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

SER.

MSOC.Eval$(PPR, F, sk_{f,ser}, sk_{f,csp}, pbk_{CSP}, pvk_{CSP}, C_{Sen_i}(i = 1, 2, \cdots, n_S))$: The cloud server SER firstly decrypts $r_i = f^{-1}_{sk_{f,ser}}(C_{i,ser})$ by using its secret key $sk_{f,ser}$ and checks whether $C^{'}_{i,ser} = H_0(r_i \parallel C_{i,1} \parallel \cdots \parallel C_{i,n_i})$ holds. If it fails, SER halts the protocol; otherwise, it sends $C_{i,i'}, C_{i,csp}, C^{'}_{i,csp}$ to the CSP.

The CSP firstly decrypts $N_i = f^{-1}_{sk_{f,csp}}(C_{i,csp})$ by using its secret key $sk_{f,csp}$ and checks whether $C^{'}_{i,csp} = H_0(N_i \parallel C_{i,1} \parallel \cdots \parallel C_{i,n_i})$ holds. If it fails, CSP halts the protocol; otherwise, it randomly selects $r_{i,csp} \in_R \{0,1\}^{2\lambda}$, and re-encrypts the blinded inputs

$$\begin{aligned} &C^{'}_{i,i'} = C_{i,i'} \ mod \ N_i = r_i m_{i,i'} \ mod \ N_i, \\ &C^{'}_{i,i',q} = C^{'}_{i,i'} \ mod \ q, C^{'}_{i,i',p} = C^{'}_{i,i'} \ mod \ p, \\ &C^{"}_{i,i'} = (p^{-1}p(C^{'}_{i,i',q})^q + q^{-1}q(C^{'}_{i,i',p})^p \\ &\qquad +r_{i,csp}N) \ mod \ T, \\ &C^{'}_{rec,csp} = H_1(C^{'}_{1,csp} \parallel \cdots \parallel C^{'}_{n_S,csp} \parallel C^{"}_{1,1} \parallel \cdots \parallel \\ &\qquad C^{"}_{1,n_1} \parallel \cdots \parallel C^{"}_{n_S,1} \parallel \cdots \parallel C^{"}_{n_S,n_{n_S}}), \end{aligned} \quad (4)$$

where $p^{-1}p \equiv 1 \ mod \ q$ and $q^{-1}q \equiv 1 \ mod \ p$. Finally, the CSP sends $C_{CSP} = (C^{"}_{i,i'}, C^{'}_{rec,csp})$ to the cloud server SER.

Without loss of generality, it is assumed that the degree of the j-th item $Item_j = a_j \prod_{l=1}^{n} x_l^{t_{l,j}} (j = 1, 2, \cdots, K)$ of the outsourced multivariate polynomial F is deg_j. After receiving C_{CSP}, the cloud server SER firstly checks whether $C^{'}_{rec,csp} = H_1(C^{'}_{1,csp} \parallel \cdots \parallel C^{'}_{n_S,csp} \parallel C^{"}_{1,1} \parallel \cdots \parallel C^{"}_{1,n_1} \parallel \cdots \parallel C^{"}_{n_S,1} \parallel \cdots \parallel C^{"}_{n_S,n_{n_S}})$ holds. If it fails, the SER halts the protocol; otherwise it randomly selects $r \in_R \{0,1\}^{2\lambda}$ with the condition that $r \in \mathbb{Z}_T^*$ and computes

$$C^{"}_{i,i',ser} = r_i^{-1} C^{"}_{i,i'}, C^{"}_{i,i',SER} = r C^{"}_{i,i',ser}. \quad (5)$$

Then, it computes

$$\begin{aligned} &C_{Item_j} = r^{deg_F - deg_j} a_j \prod_{l=1}^{n} (C^{"}_{l,SER})^{t_{l,j}}, \\ &C_F^{bld} = \sum_{j=1}^{K} C_{Item_j}, C_F^{bld,'} = H_1(C^{'}_{rec,csp} \parallel C_F^{bld}), \end{aligned} \quad (6)$$

where $n = \sum_{i=1}^{n_S} n_i$, $\cup_{l=1}^{n}\{C^{"}_{l,SER}\} = \cup_{i=1,i'=1}^{n_S,n_i}\{C^{"}_{i,i',SER}\}$, $\cup_{l=1}^{n}\{t_{l,j}\} = \cup_{i=1,i'=1}^{n_S,n_i}\{t_{i,i',j}\}$ and sends $C_{SER} = (C_F^{bld}, C^{'}_{rec,csp}, C_F^{bld,'})$ to the CSP.

After receiving C_{SER}, the CSP checks whether $C_F^{bld,'} = H_1(C^{'}_{rec,csp} \parallel C_F^{bld})$ holds. If it fails, CSP halts the protocol; otherwise, it computes

$$\begin{aligned} &C_F^{CSP,1} = C_F^{bld} \ mod \ N, \\ &C_F^{CSP,2} = f_{pk_{f,rec}}(C_F^{CSP,1}), \\ &C_F^{CSP,3} = H_1(C_F^{CSP,1} \parallel C_F^{CSP,2}), \end{aligned} \quad (7)$$

and sends $C_F^{CSP} = (C_F^{CSP,2}, C_F^{CSP,3})$ back to the cloud server SER.

Finally, the SER computes

$$C_{rec,ser} = f_{pk_{f,rec}}(r), C^{'}_F = H_1(r \parallel C_F^{CSP,2}), \quad (8)$$

and sends $C_F = (C_F^{CSP}, C_{rec,ser}, C^{'}_F)$ to the receiver REC.

MSOC.Dec$(PPR, sk_{f,rec}, C_F)$: The receiver REC firstly decrypts

$$\begin{aligned} &r = f^{-1}_{sk_{f,rec}}(C_{rec,ser}), \\ &C_F^{CSP,1} = f^{-1}_{sk_{f,rec}}(C_F^{CSP,2}), \end{aligned} \quad (9)$$

by using its secret key $sk_{f,rec}$. Then, it checks whether both $C_F^{CSP,3} = H_1(C_F^{CSP,1} \parallel C_F^{CSP,2})$ and $C^{'}_F = H_1(r \parallel C_F^{CSP,2})$ hold. If it fails, the REC halts the protocol; otherwise, it decrypts the result of outsourced computation

$$F(m_1, m_2, \cdots, m_n) = r^{-deg_F} C_F^{CSP,1}. \quad (10)$$

5 The Proposed Lightweight Privacy-preserving Authentication Protocol LPPA

In this section, a lightweight privacy-preserving authentication protocol LPPA for LBS in VANETs is proposed. Before giving the description in detail, an efficient and secure comparison protocol LSCP is firstly devised as the cornerstone of our final design.

5.1 The Proposed LSCP

In this subsection, based on our proposed MSOC, a lightweight and secure comparison protocol LSCP is proposed, which comprises the following algorithms **LSCP.Setup**, **LSCP.Enc**, **LSCP.Comp** and **LSCP.Dec**. The proposed **LSCP.Setup** and **LSCP.Enc** are the same as **MSOC.Setup** and **MSOC.Enc**.

LSCP.Comp$(PPR, f_{jud}, sk_{f,ser}, sk_{f,csp}, C_{m_i}, C_{m_j})$: Taking the ciphertexts $C_{m_i} = MSOC.Enc(PPR, pbk_i, pvk_i, m_i)$ and $C_{m_j} = MSOC.Enc(PPR, pbk_j, pvk_j, m_j)$ of two integers m_i and m_j with $\lambda^{'} = 2\lambda$-bit long as input, the issue of deciding whether m_i is larger than m_j in the encrypted domain can be transformed into evaluating a corresponding judging polynomial $f_{jud}(C_{m_i}, C_{m_j})$ in the encrypted domain.

We show how to construct the judging polynomial f_{jud} in the plaintext as follows. Firstly, without loss of generality, it is noted that m_i can be represented in the following form (i.e. C_{m_j} can be performed the same)

$$m_i = m_{i,\lambda^{'}-1} 2^{\lambda^{'}-1} + m_{i,\lambda^{'}-2} 2^{\lambda^{'}-2} + \cdots + m_{i,0}. \quad (11)$$

Therefore, the binary representation of m_i, namely $m_{i,\lambda^{'}-1} m_{i,\lambda^{'}-2} \cdots m_{i,0}$ can be straightforwardly derived by bit decomposition.

Then, it is observed that for single bit comparison between $m_{i,s} (s = 0, 2, \cdots, \lambda^{'} - 1)$ and $m_{j,s}$, we can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

obtain the judging polynomial $f_{jud,l}(m_{i,s}, m_{j,s})(s = 1, 2, \cdots, \lambda^{'} - 1; l = 1, 2, 3)$ by the truth table method such that

$$\begin{aligned} &f_{jud,1}(m_{i,s}, m_{j,s}) = m_{i,s} - m_{i,s}m_{j,s} = 1 \\ &\quad if\ and\ only\ if\ m_{i,s} > m_{j,s}, \\ &f_{jud,2}(m_{i,s}, m_{j,s}) = 2m_{i,s}m_{j,s} - m_{i,s} - m_{j,s} + 1 = 1 \\ &\quad if\ and\ only\ if\ m_{i,s} = m_{j,s}, \\ &f_{jud,3}(m_{i,s}, m_{j,s}) = m_{j,s} - m_{i,s}m_{j,s} = 1 \\ &\quad if\ and\ only\ if\ m_{i,s} < m_{j,s}. \end{aligned} \tag{12}$$

By Eqn. (12) we can transfer the single bit comparison to checking whether the corresponding judging polynomial $f_{jud,l}(m_{i,s}, m_{j,s})$ equals 0 or 1. Therefore, the comparison between two integers m_i and m_j of size $\lambda^{'}$ can be achieved by sequentially performing the bit comparison from the most significant bit to the least significant one and a binary chopping method would enhance the efficiency of comparison. Let $L = \lceil \frac{\lambda^{'}}{2} \rceil$, we have

$$\begin{aligned} m_i &= \underbrace{m_{i,\lambda'-1}, \cdots, m_{i,L}}_{m_{i,h}} \underbrace{m_{i,L-1}, \cdots, m_{i,0}}_{m_{i,l}}, \\ m_j &= \underbrace{m_{j,\lambda'-1}, \cdots, m_{j,L}}_{m_{j,h}} \underbrace{m_{j,L-1}, \cdots m_{j,0}}_{m_{j,l}}. \end{aligned} \tag{13}$$

As same as is used for constructing the judging polynomial for bit comparison, the judging polynomial $f_{jud}(m_i, m_j)$ between integers m_i and m_j can be constructed by recursively exploiting the following judging polynomial for $m_{i,h}, m_{i,l}, m_{j,h}, m_{j,l}$ with the binary chopping method

$$\begin{aligned} &f_{jud}(m_i, m_j) \\ &= f_{jud,1}(m_{i,h}, m_{j,h})(1 - f_{jud,2}(m_{i,h}, m_{j,h})) \\ &(1 - f_{jud,3}(m_{i,h}, m_{j,h}))(f_{jud,2}(m_{i,l}, m_{j,l}) \\ &(1 - f_{jud,1}(m_{i,l}, m_{j,l}))(1 - f_{jud,3}(m_{i,l}, m_{j,l})) \\ &+ f_{jud,3}(m_{i,l}, m_{j,l})(1 - f_{jud,2}(m_{i,l}, m_{j,l})) \\ &(1 - f_{jud,1}(m_{i,l}, m_{j,l}))) + f_{jud,1}(m_{i,l}, m_{j,l}) \\ &(1 - f_{jud,2}(m_{i,l}, m_{j,l}))(1 - f_{jud,3}(m_{i,l}, m_{j,l})) \\ &(f_{jud,1}(m_{i,h}, m_{j,h})(1 - f_{jud,2}(m_{i,h}, m_{j,h})) \\ &(1 - f_{jud,3}(m_{i,h}, m_{j,h})) + (1 - f_{jud,1}(m_{i,h}, m_{j,h})) \\ &f_{jud,2}(m_{i,h}, m_{j,h})(1 - f_{jud,3}(m_{i,h}, m_{j,h}))) \end{aligned} \tag{14}$$

such that

$$f_{jud}(m_i, m_j) = \begin{cases} 1, m_i > m_j, \\ 0, otherwise. \end{cases} \tag{15}$$

In our case, owing to the property of full homomorphism of our proposed MSOC and the fact that both the bit decomposition (i.e. the ciphertext of power of 2 can be also generated by senders Sen_i or Sen_j) and the recursive judging polynomial calculation only require multivariate polynomial evaluation, the cloud SER can calculate the judging polynomial $f_{jud}(m_i, m_j)$ in the encrypted domain namely $C_{f_{jud}(m_i,m_j)} = f_{jud}(C_{m_i}, C_{m_j})$, by exploiting the algorithm $MSOC.Evl(PPR, f_{jud}, sk_{f,ser}, sk_{f,csp}, C_{m_i}, C_{m_j})$.

TABLE 2: Notation Description for LPPA

Notation	Description
$m_{i,j}$	The j-th LBS message generated by vehicular user U_i
$Index_{i,j}$	The message identifier of $m_{i,j}$
$(x_{i,j}, y_{i,j})$	The coordinates denoting the location where LBS message $m_{i,j}$ is collected
$t_{i,j}$	The time when LBS message $m_{i,j}$ is collected
$R_{i,k,j}$	The rating of vehicular user U_i on user U_k's j-th LBS message $m_{k,j}$
$S(U_i, U_t)$	The similarity between vehicular users U_i and U_t
$RED_{k,j'}$	The redundancy factor denoting whether the $j^{'}$-th LBS message $m_{k,j'}$ of vehicular user U_k is redundant
$PR_{i,k,j'}$	The predicted rating of vehicular user U_i on LBS message $m_{k,j'}$
T_a	The threshold for LBS message filtering

LSCP.Dec is the same as **MSOC.Dec**. If the decryption result $f_{jud}(m_i, m_j) = 1$, the receiver decides $m_i > m_j$; otherwise, $m_i \leq m_j$.

5.2 The Proposed LPPA

In this subsection, based on our proposed MSOC and LSCP, a lightweight privacy-preserving authentication protocol LPPA for location-based services in VANETs is proposed, by devising an efficient information filtering system in the encrypted domain. It is assumed that there exist n_u vehicular users $U_i(i = 1, 2, \cdots, n_u)$ in district $s(s = 1, 2, \cdots, n_d)$ managed by RSU_s. To efficiently achieve fine-grained encrypted LBS message access control and permit the authorized vehicular users to successfully decrypt LBS services, a ciphertext-policy attribute-based encryption (CP-ABE) is adopted, which is composed of the algorithms $ABE.Setup(1^\lambda), ABE.KeyGen(MSK, S), ABE.Enc(PPAR, m, \mathbb{A}), ABE.Dec(PPAR, C, SK)$. For LBS message authentication, an existentially unforgeable secure signature scheme Λ under adaptively chosen message attack is also adopted, which is composed of the algorithms $\Lambda.KeyGen(1^\lambda), \Lambda.Sign(sk, m), \Lambda.Verify(pk, m, \sigma)$. Table 2 shows the notations used in LPPA. The proposed LPPA comprises the following four algorithms: **Setup**, **LBS Message Generation**, **LBS Message Filtering** and **LBS Message Decryption and Verification**, which are presented as follows.

Setup: On input 1^λ where λ is the security parameter, it runs the algorithm $MSOC.Setup(1^\lambda)$ to generate pairs of public key and secret key $(pk_{f,RSU_s}, sk_{f,RSU_s})$, $(pk_{f,csp}, sk_{f,csp})$ and (pk_{f,U_i}, sk_{f,U_i}) respectively for the $RSU_s(s = 1, 2, \cdots, n_d)$, the CSP and each vehicular user $U_i(i = 1, 2, \cdots, n_u)$, where f, f^{-1} on $\{0,1\}^{2\lambda}$ is a pair of one-way trapdoor permutations. $H_0, H_1 : \{0,1\}^* \rightarrow \{0,1\}^{2\lambda}$ are cryptographic hash functions. It also runs $ABE.Setup(1^\lambda)$ to generate public parameter $PPAR_{ABE}$ and master secret key MSK_{ABE}. The public parameters are $PPR = (pk_{f,RSU_s}, pk_{f,csp}, pk_{f,U_i}, PPAR_{ABE}, H_0, H_1)$ and the secret keys are $sk_{f,RSU_s}, sk_{f,csp}, sk_{f,U_i}, MSK_{ABE}$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

respectively kept private by RSU_s, CSP, U_i and the system.

LBS Message Generation: Without loss of generality, it is assumed that each vehicular user U_i generates its j-th LBS message $m_{i,j}(i = 1,2,\cdots,n_u; j = 1,2,\cdots,n_i)$ associated to the tuple $Info_{i,j} = (U_i, U_i, Index_{i,j}, x_{i,j}, y_{i,j}, t_{i,j}, r_{i,i,j})$ where $Index_{i,j}$, $(x_{i,j}, y_{i,j})$,$t_{i,j}$ and $r_{i,i,j}$ denote the message identifier of $m_{i,j}$, the coordinates of the location and the time the message $m_{i,j}$ is collected, and the rating of user U_i on its generated LBS message $m_{i,j}$. It is assumed that each U_i rates its own messages with the highest score, namely $r_{i,i,j} = 5$ where the rating values range from 1 to 5 as integers. A rounding function is applied on the location coordinates and the time to guarantee $(x_{i,j}, y_{i,j}, t_{i,j})$ to be integers for cryptographic exploitation. Let $r_{i,k,j}(k = 1,2,\cdots,n_u)$ be the user U_i's rating on user U_k's j-th message $m_{k,j}(j = 1,2,\cdots,n_k)$. In the following two cases that U_i has not received $m_{k,j}$ from other users or that U_i decides $m_{k,j}$ as redundant LBS message, the rating $r_{i,k,j}$ is set to 0. Each vehicular user U_i and RSU_s respectively generates (pbk_i, pvk_i) and (pbk_s, pvk_s) by exploiting the algorithm $MSOC.KeyGen(PPR)$. It also derives $sk_{ABE,i}, (pk_{\Lambda,i}, sk_{\Lambda,i})$ for user U_i, by running $ABE.KeyGen(MSK_{ABE}, S_i)$ and $\Lambda.KeyGen(1^\lambda)$ where S_i is the attribute set of user U_i.

1) Each U_i generates the encrypted LBS message for $m_{i,j}$

$$\begin{aligned}
&C_{i,j} = ABE.Enc(PPAR_{ABE}, m_{i,j}, \mathbb{A}),\\
&\sigma_{i,j} = \Lambda.Sign(sk_{\Lambda,i}, C_{i,j}),\\
&C_{Loc_{i,j,x}} = MSOC.Enc(PPR, pbk_i, pvk_i, x_{i,j}),\\
&C_{Loc_{i,j,y}} = MSOC.Enc(PPR, pbk_i, pvk_i, y_{i,j}),\\
&C_{t_{i,j}} = MSOC.Enc(PPR, pbk_i, pvk_i, t_{i,j}), \quad (16)
\end{aligned}$$

where $\mathbb{A}$ is the access policy permitting that the authorized LBS users can successfully decrypt the underlying LBS message $m_{i,j}$, and broadcasts $Info_{i,j} = (U_i, U_i, Index_{i,j}, C_{i,j}, \sigma_{i,j}, C_{Loc_{i,j,x}}, C_{Loc_{i,j,y}}, C_{t_{i,j}})$ in its neighborhood.

2) Each vehicular user U_i initializes and updates a table T_i by storing the encrypted tuples $Info_{l,j} = (U_i, U_l, Index_{l,j}, C_{Loc_{l,j,x}}, C_{Loc_{l,j,y}}, C_{t_{l,j}}, C_{R_{i,l,j}})(l = 1,2,\cdots,n_u; j = 1,2,\cdots,n_l)$ associated to $m_{l,j}$ as the j-th LBS message it generated itself if $l = i$ or accepted as the j-th generated LBS message from other vehicles U_l if $l \neq i$, where

$$C_{R_{i,l,j}} = MSOC.Enc(PPR, pbk_i, pvk_i, R_{i,l,j}) \quad (17)$$

is the ciphertext of its rating $R_{i,l,j}$ on each LBS message $m_{l,j}$ located in table T_i. Then, for each tuple in table T_i, user U_i randomly selects $r^i_{l,j,x}, r^{i,'}_{l,j,x}, r^i_{l,j,y}, r^{i,'}_{l,j,y}, r^i_{l,j,t}, r^{i,'}_{l,j,t} \in_R \{0,1\}^{2\lambda}$ with the conditions that $r^i_{l,j,x}, r^i_{l,j,y}, r^i_{l,j,t} \in \mathbb{Z}^*_T$ and $r^{i,'}_{l,j,x}, r^{i,'}_{l,j,y}, r^{i,'}_{l,j,t} \in \mathbb{Z}_{T_l}$, where T, T_l are the temporary public keys of CSP and user U_l, re-encrypts it as

$$\begin{aligned}
&C^i_{l,j,x} = f_{pk_{f,RSU_s}}(r^i_{l,j,x}),\\
&C^i_{l,j,y} = f_{pk_{f,RSU_s}}(r^i_{l,j,y}), C^i_{l,j,t} = f_{pk_{f,RSU_s}}(r^i_{l,j,t}),\\
&C^{i,'}_{l,j,x} = f_{pk_{f,csp}}(r^{i,'}_{l,j,x}),\\
&C^{i,'}_{l,j,y} = f_{pk_{f,csp}}(r^{i,'}_{l,j,y}), C^{i,'}_{l,j,t} = f_{pk_{f,csp}}(r^{i,'}_{l,j,t}),\\
&C^{i,'}_{Loc_{l,j,x}} = r^i_{l,j,x} r^{i,'}_{l,j,x} C_{Loc_{l,j,x}},\\
&C^{i,'}_{Loc_{l,j,y}} = r^i_{l,j,y} r^{i,'}_{l,j,y} C_{Loc_{l,j,y}},\\
&C^{i,'}_{t_{l,j}} = r^i_{l,j,t} r^{i,'}_{l,j,t} C_{t_{l,j}}. \quad (18)
\end{aligned}$$

Finally, user U_i constructs table $T^{'}_i$ comprising the tuples $Info^{'}_{i,l,j} = (U_i, U_l, Index_{l,j}, C^{i,'}_{Loc_{l,j,x}}, C^{i,'}_{Loc_{l,j,y}}, C^{i,'}_{t_{l,j}}, C_{R_{i,l,j}})$ and sends $T^{'}_i$ to the RSU_s. Note that the blinding factors $r^i_{l,j,x}, r^i_{l,j,y}, r^i_{l,j,t}$ and $r^{i,'}_{l,j,x}, r^{i,'}_{l,j,y}, r^{i,'}_{l,j,t}$ are respectively adopted in the re-encryption to achieve the interest pattern privacy of vehicular users (i.e. please refer to Sec. 6.2 for the security proof).

LBS Message Filtering: The roadside unit $RSU_s(s = 1,2,\cdots,n_d)$ predicts the rating in the encrypted domain for each vehicular user $U_i(i = 1,2,\cdots,n_u)$ currently travelling in district s on LBS message $m_{k,j'}$ which U_i has not rated before.

1) For each LBS message $m_{k,j'}(k = 1,2,\cdots,n_u; j' = 1,2,\cdots,n_k)$ as the j'-th message generated by user U_k, for each tuple in $T^{'}_i$ sent by user U_i, RSU_s computes the function

$$\begin{aligned}
&F_{dist}(Info_{k,j'}, Info_{l,j})\\
&= (Loc_{k,j',x} - Loc_{l,j,x})^2 + (Loc_{k,j',y} - Loc_{l,j,y})^2\\
&+(t_{k,j'} - t_{l,j})^2 \quad (19)
\end{aligned}$$

in the encrypted domain by exploiting the algorithm

$$\begin{aligned}
C_{Dist_{k,j',l,j}} = MSOC.Eval(&PPR, F_{dist}, sk_{f,RSU_s},\\
&sk_{f,csp}, T^{'}_k, T^{'}_i), \quad (20)
\end{aligned}$$

where $T^{'}_k$ is the table maintained and updated by user U_k.

Note that to evaluate on the re-encryption ciphertexts (i.e. we take $C^{i,'}_{Loc_{l,j,x}}$ in the updated table $T^{'}_i$ for example), the CSP firstly deciphers $r^{i,'}_{l,j,x} = f^{-1}_{sk_{f,csp}}(C^{i,'}_{l,j,x})$, computes $C^{i,csp}_{Loc_{l,j,x}} = ((r^{i,'}_{l,j,x})^{-1} C^{i,'}_{Loc_{l,j,x}})\ mod\ N_l$, and $C^{i,ser,bld}_{Loc_{l,j,x}} = p^{-1}p(C^{i,csp}_{Loc_{l,j,x}})^q_q + q^{-1}q(C^{i,csp}_{Loc_{l,j,x}})^q_q + r^{i,csp}_{l,j,x} N\ mod\ T$, where $r^{i,csp}_{l,j,x} \in_R \{0,1\}^\lambda$. Afterwards the RSU_s is also required to compute $r^i_{l,j,x} = f^{-1}_{sk_{f,RSU_s}}(C^i_{l,j,x})$ and execute an additional deblinding operation that $C^{i,ser}_{Loc_{l,j,x}} = r^{-1}_l (r^i_{l,j,x})^{-1} C^{i,ser,bld}_{Loc_{l,j,x}}$ where r_l is the blinding factor adopted to encrypt $Loc_{l,j,x}$ by the algorithm $MSOC.Enc$ in Eqn. (16) and can be decrypted by RSU_s using its secret key sk_{f,RSU_s}. The same operations are required to be performed on other re-encryption ciphertexts both in the updated table $T^{'}_i$ and $T^{'}_k$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

Then, RSU_s computes

$$C_{T_d} = MSOC.Enc(PPR, pbk_s, pvk_s, T_d), \quad (21)$$

where T_d is the threshold to decide whether an LBS message is redundant, and for each tuple in table $T_i^{'}$ associated to user U_l's j-th LBS message accepted by user U_i, compares $Dist_{k,j^{'},l,j}(l = 1, 2, \cdots, n_u; j = 1, 2, \cdots, n_l; j^{'} = 1, 2, \cdots, n_k)$ and T_d, namely evaluating the judging polynomial $f_{jud}(Dist_{k,j^{'},l,j}, T_d)$ in the encrypted domain by exploiting the algorithm

$$\begin{aligned} C_{f_{jud,k,j^{'},l,j}} &= LSCP.Comp(PPR, f_{jud}, sk_{f,RSU_s}, \\ & sk_{f,csp}, C_{Dist_{k,j^{'},l,j}}, C_{T_d}). \end{aligned} \quad (22)$$

2) RSU_s computes the similarity $S(U_i, U_t)(i, t = 1, 2, \cdots, n_u)$ between users U_i and U_t

$$S(U_i, U_t) = \frac{(\sum_{j=1}^{\sum_{l=1}^{n_u} n_l} R_{i,l,j} R_{t,l,j})^2}{\sum_{j=1}^{\sum_{l=1}^{n_u} n_l} R_{i,l,j}^2 \sum_{j=1}^{\sum_{l=1}^{n_u} n_l} R_{t,l,j}^2} \quad (23)$$

in the encrypted domain, by performing the algorithm

$$\begin{aligned} C_{S(U_i,U_t)} &= MSOC.Evl(PPR, S(U_i, U_t), sk_{f,RSU_s}, \\ & sk_{f,csp}, T_i^{'}, T_t^{'}), \end{aligned} \quad (24)$$

where $T_t^{'}$ is the table maintained and updated by user U_t. Then, it predicts user U_i's rating on LBS message $m_{k,j^{'}}$, by computing

$$PR_{i,k,j^{'}} = RED_{k,j^{'}} \frac{\sum_{t=1,t\neq i}^{n_u} R_{t,k,j^{'}} S(U_i, U_t)}{\sum_{t=1,t\neq i}^{n_u} S(U_i, U_t)} \quad (25)$$

in the encrypted domain through performing the algorithm

$$\begin{aligned} C_{PR_{i,k,j^{'}}} &= MSOC.Evl(PPR, PR_{i,k,j^{'}}, sk_{f,RSU_s}, \\ & sk_{f,csp}, C_{RED_{k,j^{'}}}, T_t^{'}, C_{S(U_i,U_t)}), \end{aligned} \quad (26)$$

where $C_{RED_{k,j^{'}}} = \prod_{j=1}^{\sum_{l=1}^{n_u} n_l} C_{f_{jud,k,j^{'},l,j}}$ is the encrypted redundancy factor. Finally, RSU_s transmits all the encrypted prediction ratings $C_{PR_{i,k,j^{'}}}(k = 1, 2, \cdots, n_u; j^{'} = 1, 2, \cdots, n_k)$ to vehicular user U_i.

LBS Message Decryption and Verification: While receiving a newly-arriving LBS message $m_{k,j^{'}}$, vehicular user U_i firstly recovers the prediction rating by performing

$$PR_{i,k,j^{'}} = MSOC.Dec(PPR, sk_{f,U_i}, C_{PR_{i,k,j^{'}}}), \quad (27)$$

and compares it to the predefined threshold T_a. If $PR_{i,k,j^{'}} = 0$, U_i considers LBS message $m_{k,j^{'}}$ to be duplicate to the messages she/he has accepted, discards and prevents it from being further broadcasted in the neighborhood; if $0 < PR_{i,k,j^{'}} < T_a$, user U_i considers LBS message $m_{k,j^{'}}$ as a useless but not redundant one without further authentication and transmit it to other vehicles in her/his neighborhood; otherwise, U_i decides LBS message $m_{k,j^{'}}$ as a useful one and verifies the signature by performing the algorithm $\Lambda.Verify(pk_{\Lambda,k}, C_{k,j^{'}}, \sigma_{k,j^{'}})$. If it fails, U_i discards LBS message $m_{k,j^{'}}$ and stop it from further transmission; otherwise, U_i accepts and recovers $m_{k,j^{'}}$ by performing the ABE decryption algorithm $m_{k,j^{'}} = ABE.Dec(PPAR_{ABE}, SK_{ABE,i}, C_{k,j^{'}})$. Finally, U_i gives a rating $R_{i,k,j^{'}}$ on LBS message $m_{k,j^{'}}$ and adds the tuple $(U_i, U_k, j^{'}, C_{Loc_{k,j^{'},x}}, C_{Loc_{k,j^{'},y}}, C_{t_{k,j^{'}}}, C_{R_{i,k,j^{'}}})$ into its table T_i by performing Step 2) in the algorithm **LBS Message Generation**.

Remark:(Aggregated LBS bundles) It is noted that the techniques of aggregate signature and multi-signature [6] can be exploited by each vehicular user to compress all her/his accepted LBS messages originally generated and signed by different users, into a single bundle (i.e. the useless but not duplicate LBS messages can also be aggregated into a single bundle in the same way). Then, the specific vehicular user rates on both the accepted and the useless but not redundant LBS bundle, and each $RSU_s(s = 1, 2, \cdots, n_d)$ can predict the ratings on the bundles for other users based on their similarities in Eqn. (25). The communication cost on each vehicular user would be further reduced (i.e. please refer to Sec. 7.2 for performance evaluation).

6 Security Proof

In this section, we firstly give the formal security proof of our proposed multi-key secure outsourced computation scheme MSOC. Then, based on the primitive of MSOC, we elaborate that our proposed lightweight privacy-preserving authentication protocol LPPA for location-based services in VANETs achieves the security goals.

6.1 Security for the Proposed MSOC

Before giving the security proof, we present the correctness of our MSOC that serves the primitive of LPPA. In Eqn. (7), by exploiting Chinese Remainder Theorem and Euler's Theorem [29], we have

$$\begin{aligned} & C_F^{CSP,1} = C_F^{bld} \ mod \ N \\ & = r^{deg_F - deg_j} \sum_{j=1}^{K} a_j \prod_{l=1}^{n} (C_{l,SER}^{"})^{t_{l,j}} \ mod \ N \\ & = r^{deg_F} \sum_{j=1}^{K} a_j \prod_{l=1}^{n} (p^{-1} p m_{l,q}^{q} + q^{-1} m_{l,p}^{p} + r_{i,csp} N)^{t_{l,j}} \\ & \quad mod \ N \\ & = r^{deg_F} \sum_{j=1}^{K} a_j (p^{-1} p (\prod_{l=1}^{n} m_l^{t_{l,j}})_q^q + q^{-1} q (\prod_{l=1}^{n} m_l^{t_{l,j}})_p^p) \\ & \quad mod \ N \\ & = r^{deg_F} (p^{-1} p (\sum_{j=1}^{K} a_j \prod_{l=1}^{n} m_l^{t_{l,j}})_q^q + q^{-1} q (\sum_{j=1}^{K} a_j \prod_{l=1}^{n} m_l^{t_{l,j}})_p^p) \\ & \quad mod \ N \\ & = r^{deg_F} \sum_{j=1}^{K} a_j \prod_{l=1}^{n} m_l^{t_{l,j}} = r^{deg_F} F(m_1, m_2, \cdots, m_n). \end{aligned}$$

Therefore, the authorized receiver possessing the secret key $sk_{f,rec}$ can successfully recover $F(m_1, m_2, \cdots, m_n) = r^{-deg_F} C_F^{CSP,1}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

We firstly give the security proof of the data privacy of the subset of uncorrupted senders $N_{Sen} \setminus T$ in our proposed MSOC against the collusion attack between the CSP, the subset of corrupted senders T and malicious receivers. We also take input privacy to detail the security proof and the proofs for the output privacy and the collusion with the cloud server can be similarly derived.

Theorem 1: (**Data Privacy for MSOC**) Let $\mathcal{A}$ be a malicious adversary defeating the CCA2 security for data privacy of our proposed MSOC with a nonnegligible advantage defined as $\epsilon^{'}$,$^{ploy(\lambda)}$, where $poly(\lambda)$ refers to the total number of queries made to the oracles and λ is the security parameter. There exists a simulator $\mathcal{B}$ who can use $\mathcal{A}$ to invert the one-way trapdoor permutation f with the nonnegligible probability ϵ that:

$$\epsilon \geq \epsilon^{'},^{poly(\lambda)} - \frac{poly(\lambda)}{2^{\lambda-1}}. \tag{28}$$

Proof: We take input privacy to detail the security proof. Intuitively, although the adversary $\mathcal{A}$ considered as the collusion between the CSP, the malicious receiver and a subset of corrupted senders holds secret key $sk_{f,csp}$ that can be used to compute $N_i = f^{-1}_{sk_{f,csp}}(C_{i,csp})$ and $C^{'}_{i,i'} = C_{i,i'} \ mod \ N_i = r_i m_{i,i'} \ mod \ N_i$, the input $m_{i,i'}$ cannot be derived without the knowledge of r_i encrypted in $C_{i,ser} = f_{pk_{f,ser}}(r_i)$. Therefore, we can reduce the CCA2 security for input privacy to the inverse of one-way trapdoor permutation f without secret key $sk_{f,ser}$ and the proof is given by contradiction. In the initialization phase, the system performs $(f, f^{-1}) \leftarrow \mathcal{G}(1^{\lambda}), y_i = f_{pk_{f,ser}}(r_i)$ and the simulator $\mathcal{B}$ tries to solve $r_i = f^{-1}_{sk_{f,ser}}(y_i)$. The adversary $\mathcal{A}$ is given the public parameter PPR, the secret keys $sk_{f,csp}, sk_{f,rec}$ of the corrupted CSP and the corrupted receiver and all the temporary secret key pvk_{CSP}, pvk_i of the corrupted CSP and all corrupted senders $Sen_i \in T$. There are two oracles, namely $\mathcal{O}^{H_0}$ and $\mathcal{O}^{Dec}$. $\mathcal{B}$ can perform the simulations by answering the queries from the adversary as follows. For the collusion between the CSP, malicious receivers and a subset of corrupted senders, we mainly focus on the ciphertext components $C_{i,ser}, C_{i,i'}, C^{'}_{i,ser}$ in C_{Sen_i}.

$\mathcal{O}^{H_0}$ **Query**. If a query $r_i \parallel C_{i,1} \parallel \cdots \parallel C_{i,n_i}$ to $\mathcal{O}^{H_0}$ satisfies $f(r_i) = y_i$, then $\mathcal{B}$ outputs r_i and halts; otherwise, it returns a random element $Str_0 \in_R \{0,1\}^{2\lambda}$ as the response to the adversary and remains the triple $(r_i, C_{i,1} \parallel \cdots \parallel C_{i,n_i}, Str_0)$ in the H_0-list.

$\mathcal{O}^{Dec}$ **Query**. To answer the query $s^{'} \parallel d^{'} \parallel h^{'}$ to $\mathcal{O}^{Dec}$ where $d^{'} = \cup_{i'=1}^{n_i} C_{i,i'}$, the simulator $\mathcal{B}$ firstly checks if there exists a triple $(r_i, d^{'}, h^{'})$ in the H_0-list. If it does, the simulator $\mathcal{B}$ further checks whether $s^{'} = f_{pk_{f,ser}}(r_i)$ holds. If not, the simulator $\mathcal{B}$ returns invalid; otherwise it computes and returns $C^{'}_{i,i'} = r_i^{-1} d^{'}$ to the adversary $\mathcal{A}$ and $\mathcal{A}$ computes $m_i = C^{'}_i \ mod \ N_i$.

Then, the adversary $\mathcal{A}$ submits two challenge plaintexts $m_{i,i',0}, m_{i,i',1}$ associated to an uncorrupted sender $Sen_i \in N_{Sen} \setminus T$ of the same size $|m_{i,i',0}| = |m_{i,i',1}| = 2\lambda$, and the simulator $\mathcal{B}$ randomly selects $\beta \in \{0,1\}$ and returns the encryption of $m_{i,i',\beta}$ as the challenge ciphertext $c^*_{i,i'}$. After receiving $c^*_{i,i'}$, $\mathcal{A}$ can continue to make queries to the oracles $\mathcal{O}^{H_0}$ and $\mathcal{O}^{Dec}$ with the restriction that $c^*_{i,i'}$ cannot be queried to the decryption oracle $\mathcal{O}^{Dec}$ in the adaptive query phase.

To explain the interaction perfectly simulates the real environment of the adversary $\mathcal{A}$ running with its oracles, we study the following events. Let S be the event that for some ciphertext $s^{'} \parallel d^{'} \parallel h^{'}$, $\mathcal{A}$ made some query $r_i \parallel d^{'}$ to the oracle $\mathcal{O}^{H_0}$ satisfying $f(r_i) = s^{'}$. Then, we further let R be the event that $\mathcal{A}$ made some query $s^{'} \parallel d^{'} \parallel h^{'}$ to the decryption oracle $\mathcal{O}^{Dec}$ where $h^{'} = H_0(r_i \parallel d^{'})$ holds without making any query $(f^{-1}_{sk_{f,ser}}(s^{'}) \parallel d^{'})$ to the H_0-oracle $\mathcal{O}^{H_0}$. Let $poly(\lambda)$ be the total number of oracle queries made by the adversary $\mathcal{A}$. Then, we can conclude that

$$\begin{aligned} & Pr[\mathcal{A}^{Suc}] \\ &= Pr[\mathcal{A}^{Suc}|R]Pr[R] + Pr[\mathcal{A}^{Suc}|\bar{R} \wedge S]Pr[\bar{R} \wedge S] \\ &+ Pr[\mathcal{A}^{Suc}|\bar{R} \wedge \bar{S}]Pr[\bar{R} \wedge \bar{S}] \\ &\leq poly(\lambda)2^{-\lambda} + Pr[S] + \frac{1}{2}, \end{aligned}$$

since $Pr[R] \leq \frac{poly(\lambda)}{2^{\lambda}}$ and $Pr[\mathcal{A}^{Suc}|\bar{R} \wedge \bar{S}] = \frac{1}{2}$ can be straightforwardly derived. Finally, it is observed that the probability of simulator $\mathcal{B}$ to fail in behaving like the adversary $\mathcal{A}$ in inverting the one-way trapdoor permutation f can be bounded by $Pr[R]$. Therefore,

$$\epsilon \geq \epsilon^{'},^{poly(\lambda)} - \frac{poly(\lambda)}{2^{\lambda-1}},$$

which is also non-negligible. Therefore, theorem 1 holds. □

Theorem 2: (**Security for the Whole Protocol**) The proposed MSOC securely implements the functionality Fun, namely for every real world adversary $\mathcal{A}$, there exists an ideal world adversary $\mathcal{S}$ with access to $\mathcal{A}$ in a black-box manner such that for all input vectors $\vec{m}$, we have $Ideal_{Fun,\mathcal{S}}(\vec{m}) \approx_c Real_{MSOC,\mathcal{A}}(\vec{m})$.

Proof: Based on the data privacy (indistinguishability) proved in Theorem 1, we prove this theorem when the server is corrupted via a series of hybrid games, by using an ideal/real paradigm. The proofs for other cases of a corrupted CSP, corrupted sender, corrupted receiver and their collusion can be analogously derived.

Game 0. This is the real world execution of our proposed MSOC.

Game 1. Instead of executing **MSOC.Dec** where the honest receiver uses its secret key, we run the simulator $\mathcal{S}_{MSOC.Dec}$ interacting with the adversary $\mathcal{A}$. Owing to the data privacy (i.e. we mean output privacy here) of our proposed MSOC, if the ideal decryption functionality is correctly emulated, the joint output is computationally indistinguishable in a real world execution of our proposed MSOC with the adversary $\mathcal{A}$, and in a ideal world execution with the adversary $\mathcal{S}_{MSOC.Dec}$.

Game 2. In this game, by replacing computing $\hat{y} = MSOC.Dec(PPR, \hat{sk}_{f,rec}, C_F)$, the joint output is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

computed by $\hat{y} = F(\hat{m_1}, \hat{m_2}, \cdots, \hat{m_n})$ where $\hat{m_i} = m_i$ for all honest inputs from honest senders $Sen_i \in N_{Sen} \setminus T$ and $\hat{m_i}$ from the corrupted set of senders $Sen_i \in T$ are the data inputs from the adversary $\mathcal{A}$. We claim that Game 1 and Game 2 are identically distributed, since a semi-honest adversary $\mathcal{A}$ must strictly follow the protocol specification with the inputs and randomness that it captures.

Game $3.k.k^{'}(k = 1, 2, \cdots, n - |T|; k^{'} = 1, 2, \cdots, n_k)$. Without loss of generality, it is assumed that the uncorrupted set of senders is $N_{Sen} \setminus T = \{Sen_1, Sen_2, \cdots, Sen_{n-|T|}\}$. In Game $3.k.k^{'}$, we change the ciphertext component in C_{Sen_k} such that it now encrypts 0 instead of encrypting $m_{k,k'}$. Formally speaking, we have

$$\{C_{Sen_j} \leftarrow MSOC.Enc(PPR, pbk_j, pvk_j, 0)\},$$
$$when\ j < k \vee (j = k \wedge j^{'} \leq k^{'});$$
$$\{C_{Sen_j} \leftarrow MSOC.Enc(PPR, pbk_j, pvk_j, m_{j,j'})\},$$
$$when\ j > k \vee (j = k \wedge j^{'} > k^{'}).$$

We let Game 2 be Game 3.1.0 and claim that the view of $\mathcal{A}$ in Game $3.k.k^{'}(k = 1, 2, \cdots, n - |T|; k^{'} = 1, 2, \cdots, n_k)$ is indistinguishable from its view in Game $3.k.(k^{'} - 1)$ since Theorem 1 tells us that the input privacy of our proposed MSOC achieves CCA2 security of indistinguishability. On the other hand, since we have run the simulator $\mathcal{S}_{MSOC.Dec}$ in Game 1 instead of the real decryption, the secret key pvk_i is only adopted to encrypt C_{Sen_j}.

Now, we have proved that the joint output in Game 0 is computationally indistinguishable from the joint output in Game $3.(n - |T|).n_{n-|T|}$ that is precisely $Ideal_{Fun,\mathcal{S}}(\vec{m})$. Note that Game 0 is defined to be $Real_{MSOC,\mathcal{A}}(\vec{m})$, therefore we arrive at the conclusion that $Ideal_{Fun,\mathcal{S}}(\vec{m}) \approx_c Real_{MSOC,\mathcal{A}}(\vec{m})$. □

6.2 Security for the Proposed LPPA

Our proposed lightweight privacy-preserving authentication scheme LPPA for LBS in VANETs achieves location privacy, interest privacy and interest pattern privacy.

For location privacy, both the position coordinate $(x_{i,j}, y_{i,j})$ and time $t_{i,j}$ of vehicular user U_i's j-th generated LBS message $m_{i,j}(i = 1, 2, \cdots, n_u; j = 1, 2, \cdots, n_i)$ are encrypted using the algorithm $MSOC.Enc$ by Eqn. (16) in the **LBS Message Generation** phase. Owing to the fact that the data privacy (i.e. input privacy) of $MSOC.Enc$ has been proved to be CCA2 secure against the CSP (or the cloud server), the subset of corrupted senders and the malicious receiver, the location privacy can be well protected.

For the same reason that the rating $R_{i,l,j}$ of vehicular user U_i on user U_l's j-th generated LBS message $m_{l,j}(l = 1, 2, \cdots, n_u; j = 1, 2, \cdots, n_l)$ is encrypted by $MSOC.Enc$ in Eqn. (17), the interest privacy can also be well protected.

To achieve interest pattern privacy, it is required for vehicular user U_i to re-encrypt the ciphertext of position coordinate $C_{Loc_{l,j,x}}, C_{Loc_{l,j,y}}$ and the time $C_{t_{l,j}}$ of her/his accepted LBS message $m_{l,j}$ in Eqn. (18). Taking $C^{i,'}_{Loc_{l,j,x}} = r^i_{l,j,x} r^{i,'}_{l,j,x} C_{Loc_{l,j,x}}$ for example, two blinding factors $r^i_{l,j,x}$ and $r^{i,'}_{l,j,x}$ are adopted to re-encrypt $C_{Loc_{l,j,x}}$. Although RSU_s and the CSP can respectively decipher the randomness $r^i_{l,j,x}$ and $r^{i,'}_{l,j,x}$, under the assumption that RSU_s is not permitted to collude with the CSP, the unique ciphertext $C_{Loc_{l,j,x}}$ would be re-encrypted by different randomnesses $r^i_{l,j,x}$ and transferred into different ciphertexts from the view of the CSP. On the other hand, since the randomness $r^{i,csp}_{l,j,x}$ is adopted in the CSP's re-encryption $C^{i,ser,bld}_{Loc_{l,j,x}} = p^{-1}p(C^{i,csp}_{Loc_{l,j,x}})^q_q + q^{-1}q(C^{i,csp}_{Loc_{l,j,x}})^q_q + r^{i,csp}_{l,j,x} N \ mod\ T$ under the unique modulus N, without the knowledge of N, RSU_s can neither distinguish whether two ciphertexts $C^{i,ser,bld}_{Loc_{l,j,x}}$ and $C^{k,ser,bld}_{Loc_{l,j,x}}(k \neq i)$ correspond to the same $Loc_{l,j,x}$. Therefore, the interest pattern privacy is well protected.

TABLE 3: Efficiency Comparison for Secure Multiparty Outsourced Computation

		Computational Complexity	Communication Complexity
López-Alt's scheme [18]	Sender	$O(n_i)$	$O(n_i)$
	Cloud	$O(n + K2^{deg_F})$	$O(n + 2^{deg_F})$
	CSP	$O(n)$	$O(n)$
	Receiver	$O(2^{deg_F})$	$O(2^{deg_F})$
Our Proposed MSOC	Sender	$O(1)$	$O(n_i)$
	Cloud	$O(n + Kdeg_F)$	$O(n)$
	CSP	$O(n)$	$O(n)$
	Receiver	O(1)	O(1)

7 Performance Evaluation

In this section, we evaluate the performance of our proposed efficient multi-key secure outsourced computation scheme MSOC and lightweight privacy-preserving authentication protocol LPPA.

7.1 Efficiency Comparison of the Proposed M-SOC

Theoretical Analysis We give a theoretical efficiency analysis of our proposed MSOC in the aspects of computational complexity and communication complexity, compared to the representative work [18] among all the state-of-the-art exploiting public key FHE. Owing to the fact that López-Alt et al. [18] proved that it is impossible to achieve program obfuscation of non-interaction with the clients in the single server setting, for comparison convenience with our proposed MSOC, a modified version of [18] in the two non-colluding server setting is exploited. Table 3 demonstrates the efficiency comparison between López-Alt's secure multiparty outsourced computation [18] implemented by Brakerski's public key FHE [19] and our proposed MSOC.

It is observed that the computational complexity of any one-way trapdoor permutation (i.e. the most significant component contributing to the computational cost) on each sender Sen_i's end in our MSOC is $O(1)$, which is significantly reduced from $O(n_i)$ that is required for López-Alt's scheme [18] exploiting Brakerski's FHE [19]. The reason is that Brakerski's public key FHE [19] is needed to be performed on each message (data input) $m_{i,i'}(i' = 1, 2, \cdots, n_i)$ of sender Sen_i in [18]; while in our

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

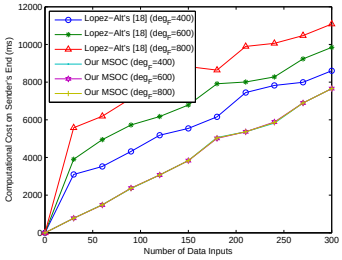


Fig. 2: Computational Cost Comparison on Sender's End of MSOC

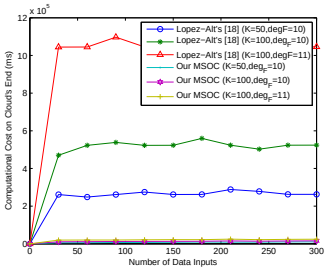


Fig. 3: Computational Cost Comparison on Cloud's End of MSOC

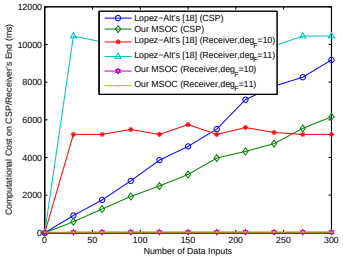


Fig. 4: Computational Cost Comparison on CSP/Receiver's End of MSOC

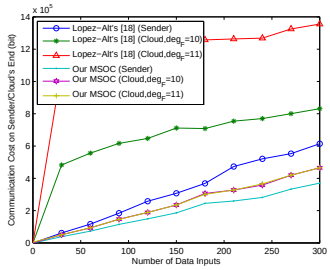


Fig. 5: Communication Cost Comparison on Sender/Cloud's End of MSOC

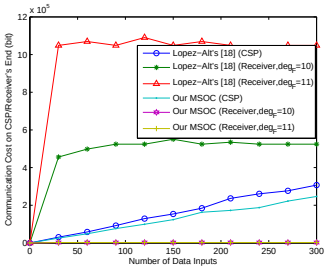


Fig. 6: Communication Cost Comparison on C-SP/Receiver's End of MSOC

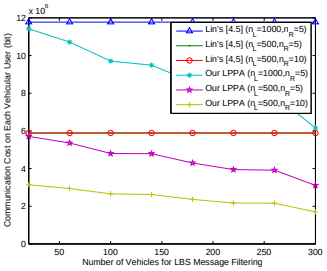


Fig. 7: Communication Cost Comparison of LPPA

MSOC, to encrypt all n_i messages, the underlying one-way trapdoor permutation f is computed only twice, namely $C_{i,ser} = f_{pk_f,ser}(r_i), C_{i,csp} = f_{pk_f,csp}(N_i)$ in Eqn. (3), independent to the number of messages n_i held by Sen_i.

It also shows the computational overhead of the cloud in our MSOC is $O(n + Kdeg_F)$, considerably less than $O(n + K2^{deg_F})$ in [18] where $n = \sum_{i=1}^{n_S} n_i, K, deg_F$ respectively denote the total number of messages (data inputs) from all n_S senders, the number of items in multivariate polynomial $F(x_1, x_2, \cdots, x_n) = \sum_{j=1}^{K} a_j \prod_{l=1}^{n} x_l^{t_{l,j}}$, and the degree of F. The reason is that our MSOC requires to execute n multiplicative blinding in addition to $K(deg_F - 1)$ multiplications for function evaluation in the encrypted domain; while López-Alt's scheme [18] requires n multiplicative blinding and $K2^{deg_F}$ multiplications for function evaluation in the worst case (i.e. each item $Item_j (j = 1, 2, \cdots, K)$ is of degree deg_F). The computational overhead of the CSP in our MSOC and López-Alt's scheme [18] are both $O(n)$ to re-encrypt all n messages (data inputs) under the unique set of public key for function evaluation.

Finally, the computational overhead of the receiver in our MSOC is $O(1)$, also dramatically lower than $O(2^{deg_F})$ required in [18] for the reason that the decryption in [18] using Brakerski's public key FHE [19] requires the inner product on the ciphertext vector of size 2^{deg_F} that evaluates 2^{deg_F} multiplications; while in our MSOC, only 2 one-way trapdoor permutations, 1 modular exponentiation and 1 multiplication are needed, independent to the degree of the outsourced function F.

On the other hand, the communication complexity on the cloud's end and the receiver's ends of our MSOC are respectively $O(n)$ and $O(1)$ that are significantly reduced from $O(n + 2^{deg_F})$ and $O(2^{deg_F})$ in López-Alt's scheme [18] adopting Brakerski's public key FHE [19], since each ciphertext multiplication on Brakerski's public key FHE [19] would double the size of the ciphertext, leading to a high communication complexity. Since López-Alt's scheme [18] incurs an exponential complexity, it is only appropriate for the outsourced function with the degree $deg_F = O(log\lambda)$ where λ is the security parameter.

Extensive Evaluation Results We conduct the extensive evaluation to demonstrate the performance of our proposed MSOC in the aspects of computational cost and communication cost on the sender's, the cloud's and the receiver's ends. All the experiments are implemented by exploiting PBC [27] and MIRACL libraries [28] running on Linux platform with 2.93GHz processor. Let the security parameter be $\lambda = 512$. In our proposed MSOC, we respectively set $|p_i| = |q_i| = |s_i| = |p| = |q| = |s| = 512$ and $|N_i| = |N| = 1024, |T_i| = |T| = 1536$. The one-way trapdoor permutations $f_{pk_f,ser}, f_{pk_f,csp}$ and $f_{pk_f,rec}$ are respectively implemented by RSA on $\mathbb{Z}_{N_i}^*$ and $\mathbb{Z}_N^*$; while in López-Alt's scheme [18] adopting Brakerski's public key FHE [19], we set $|q_B| = 512, p_B = 4096$.

Fig. 2 demonstrates that the computational cost on the sender's end of our MSOC is dramatically reduced to López-Alt's scheme [18] as the number of messages (data inputs) increases. The sender's computational cost of [18] also increases as the degree of the outsourced function deg_F increases from 400, 600 to 800, since each user in Brakerski's public key FHE [19] including the sender is required to generate a secret key vector of the form $\vec{s} = (1, s, s^2, \cdots, s^{deg_F})$ and the evaluated function F must be known in advance; while in our MSOC, it remains constant regardless of the variation on deg_F. Fig. 3 shows that the computational cost on the cloud's end is considerably less than [18] as the number of the items K and the function degree deg_F respectively increase from 50 to 100 and 10 to 11. Fig. 4 shows that the computational cost on the CSP's and receiver's ends are considerably saved compared to López-Alt's scheme [18]. Especially, the computational cost of the receiver in our MSOC is constant and independent to the degree of the function deg_F which increases from 10 to 11.

Fig. 5 and Fig. 6 demonstrate that the communication

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2923156, IEEE Transactions on Information Forensics and Security

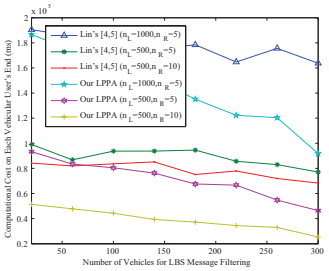


Fig. 8: Computational Cost Comparison of LPPA

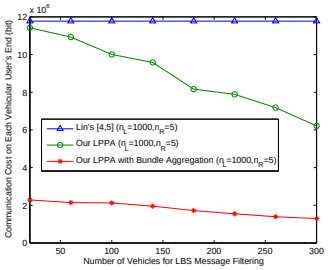


Fig. 9: Communication Cost Comparison for LBS Bundle Aggregation of LPPA

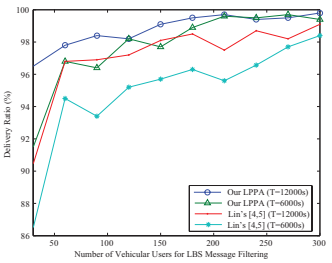


Fig. 10: Delivery Ratio Comparison of LPPA

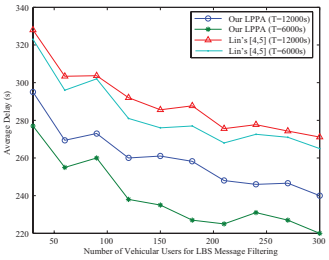


Fig. 11: Average Delay Comparison on LPPA

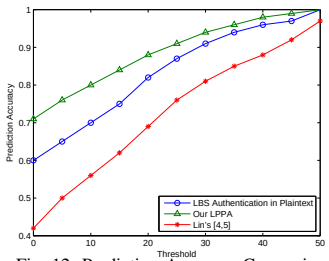


Fig. 12: Prediction Accuracy Comparison

cost on the sender's, cloud's, CSP's and receiver's ends are all significantly reduced from López-Alt's scheme [18]. The reason is that López-Alt's scheme [18] requires $O(K2^{deg_F})$ multiplications in $\mathbb{R}_{q_B}$ to evaluate the multivariate polynomial F with K items of degree deg_F and results in that the size of the ciphertext would be doubled in $\mathbb{R}_{q_B}$ each time a ciphertext multiplication is evaluated; while in our MSOC, the ciphertext size of the function evaluation result is independent to deg_F, namely the number of required ciphertext multiplications.

7.2 Efficiency Comparison of the Proposed LPPA

In this subsection, we perform a series of custom simulations using a Java simulator. The performance evaluations are mainly operated to demonstrate the efficiency improvement in both aspects of the computational cost and communication cost of our proposed lightweight privacy-preserving authentication scheme LPPA for LBS in VANETs, compared to the state-of-the-art [4,5]. The detailed simulation settings and results are presented in the following.

We consider a typical VANET where n vehicular users with their equipped OBUs are uniformly deployed in a 8000m $\times$ 8000m area. A set of 8 social spots are randomly distributed in this area where the RSUs with the transmission range of 1000m are appropriately deployed. The transmission range of each vehicle is 300m. In simulation, each vehicular user randomly arrives 4-8 frequently visited social spots along the shortest path at the average velocity of 10 m/s and stays at most 4 mins before driving to another. The simulation lasts 6000s/12000s and the vehicular users of the size $n_u = 50, 100, \cdots, 300$ are uniformly distributed in 6 groups. For each case, we run the simulation 500 times and derive the average results. In our simulation, the CP-ABE [26], the short signature scheme Λ [25] and the aggregate signature scheme [6] are exploited for implementation of LPPA.

Fig. 7 demonstrates that the communication cost of each vehicular user in our LPPA is dramatically lower than the existing work [4,5] as the LBS message generation rate increases from $n_L = 500$ to 1000. The reason is that distinguishing from [4,5] where duplicate messages with different message identifiers are possible to be authenticated multiple times, our LPPA reduces the authentication overhead from the sender's aspect where an LBS message would be checked for its redundancy and utility in Eqn. (24) before it is authenticated. Specifically, the vehicular user discards the duplicate LBS contents without broadcasting (i.e. $PR_{i,k,j'} = 0$ since the redundancy factor $RED_{k,j'}$=0), which optimizes the communication cost. On the other hand, it also shows that the communication cost on each vehicular user decreases as the number of vehicles increases. The reason is that more vehicular users collaborate in filtering duplicate LBS messages; while the number distinguished LBS messages would not increase accordingly since all vehicles in the same geographically social group share the same set of LBS messages. Finally, it is noted that the communication cost of each vehicular user in our LPPA decreases as the number of RSUs increases from $n_R = 5$ to 10, since there exist more RSUs participating in privacy-preserving LBS message recommendation by evaluating Eqn. (24) in the encrypted domain.

Fig. 8 shows that the computational cost on each vehicular user is also considerably reduced compared to [4,5], as the number of LBS message generation rate increases from $n_L = 500$ to 1000. The reason is that in our LPPA, each vehicular user only authenticates the valuable LBS messages (i.e. $PR_{i,k,j'} \geq T_a$), which eliminates the computational cost to authenticate redundant LBS messages (i.e. $PR_{i,k,j'} = 0$) or useless LBS messages ($0 < PR_{i,k,j'} < T_a$). It also demonstrates that the computational cost on each vehicular user decreases as the number of vehicular users increases. The reason is that the more users rate on their accepted LBS messages, the more precise each $RSU_s(s = 1, 2, \cdots, n_d)$ would predict the ratings of each vehicular user on her/his received LBS messages.

Consequently, more redundant or useless LBS messages would be correctly identified and discarded/transmitted in the neighborhood without taking effort for authentication.

Fig. 9 demonstrates that the communication cost for bundle aggregation in our LPPA is significantly saved compared to [4,5] and our LPPA without bundle aggregation, since a batch of LBS messages are aggregated into a single bundle for delivery and authentication. Fig. 10 and Fig. 11 illustrate that the delivery ratio and average delay of our LPPA are respectively higher and lower than the existing work [4,5] as the number of vehicular users and the simulation time respectively increase. The reason is that the communication bandwidth would be more likely taken to deliver only distinctive LBS messages without redundancy, when more vehicular users participate in LBS message filtering for a long period of time. Fig. 12 demonstrates the prediction accuracy comparison among our LPPA, Lin's schemes [4,5] and the LBS authentication in plaintext. It is observed that all prediction accuracy increase as threshold T_a increases, since more redundant or useless LBS messages for vehicular user U_i would be filtered with a larger threshold T_a. More importantly, the prediction accuracy of our LPPA is much higher than the corresponding protocol in plaintext and Lin's schemes [4,5]. The reason is that in our LPPA, two cryptographic hash functions H_0, H_1 are adopted to guarantee the integrity of ciphertexts in the underlying building block MSOC; while the adversary in the corresponding protocol in plaintext can fabricate or forge the location coordinates, the time and the ratings on the generated LBS messages, which leads to a lower prediction accuracy. In Lin's schemes [4,5] without effective prediction mechanisms, LBS messages are only filtered by message identifiers where LBS messages with different identifers are likely associated to the same content and redundant to vehicular users.

8 Conclusions

In this paper, an efficient multi-key secure outsourced computation scheme MSOC without exploiting public key FHE is firstly proposed. Then, based on MSOC, an efficient and secure comparison protocol LSCP is devised, without the interaction between the server and the users. Furthermore, a lightweight privacy-preserving authentication protocol LPPA is proposed for LBS in VANETs, by eliminating duplicate and useless encrypted LBS messages before authentication. Finally, formal security proof shows that the our proposed LPPA achieves vehicular user's location privacy, interest privacy and interest pattern privacy, and the extensive simulation results verify its efficiency and practicability.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China (Grant No. 61602180, 61632012 and 61672239), in part by Natural Science Foundation of Shanghai (Grant No. 16ZR1409200) and in part by China Postdoctoral Science Foundation (Grant No. 2017M611502).

References

[1] M. Raya and J. P. Hubaux *A security of vehicular ad hoc networks*, In Proc. SASN, Alexandria, VA, Nov. 2005.

[2] U.S. Department of Transportation, *National highway traffic safty administration*, in Veh. Safty Commu. Project, Final Report, Apr. 2006.

[3] M. Whaiduzzaman, M. Sookhak, A. Gani and R. Buyya, *A survey on vehicular cloud computing*, Journal of Network and Computer Applications, vol. 40, pp. 325-344, 2014.

[4] X. Lin, X. Sun, X. Wang, C. Zhang, P. H. Ho and X. Shen, *TSVC: Timed efficient and secure vehicular communications with privacy preserving*, IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987-4998, 2008.

[5] X. Lin and X. Li, *Achieving efficient cooperative message authentication in vehicular ad hoc networks*, IEEE Trans. Veh. Technol., vol. 62, no. 7, pp. 3339-3348, 2013.

[6] A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum, *Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing*, In ACM CCS 2007, pp. 276-285.

[7] 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, 2007.

[8] J. Zhou, X. Lin, X. Dong and Z. Cao, *PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system*, IEEE Transactions on Parallel and Distributed Systems, 26(6): 1693-1703, 2015.

[9] C. Zhang, X. Lin, R. Lu and P. H. Ho, *RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks*, In Proc. IEEE ICC, Beijing, China, May 2008, pp. 1451-1457.

[10] X. Lin, *Secure and privacy-preserving vehicular communications*, Ph.D. dissertation, Univ. Waterloo, Department of Electrical and Computer Engineering, Waterloo, ON, Canada, 2008.

[11] R. Lu, X. Lin, X. Liang and X. Shen, *A dynamic privacy-preserving key management scheme for location based services in VANETs*, IEEE Trans. on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127-139, 2012.

[12] P. Fan, J. F. Haran, J. Dillenburg, and P. C. Nelson, *Cluster-based framework in vehicular ad-hoc networks*, ADHOC-NOW 2005, LNCS 3738, pp.32-42, 2005.

[13] A. Daeinabi, A. Ghaffar, P. Rahbar and A. Khademzadeh, *VWCA: An efficient clustering algorithm in vehicular ad hoc networks*, Journal of Network and Computer Applications, vol. 34, no. 1, pp. 207-222, Jan. 2011.

[14] R. Lu, X. Lin, T. H. Luan, X. Liang, X. Li, L. Chen and X. Shen, *PReFilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks*, In Proc. IEEE INFOCOM '12, Orlando, Florida, USA, Mar. 25-30, 2012.

[15] Q. Tang and J. Wang, *Privacy-preserving context-aware recommender systems: analysis and new solutions*, In ESORICS 2015, LNCS 9327, pp. 101-119, 2015.

[16] S. Badsha, X. Yi, I. Khalil and E. Bertino, *Privacy preserving user-based recommender system*, In ICDCS'17, 2017.

[17] X. Liu, K.K.R Choo, R.H. Deng, R. Lu and J. Weng, *Efficient and privacy-preserving outsourced calculation of rational numbers*, IEEE Transactions on Dependable and Secure Computing, 15(1): 27-39, 2018.

[18] A. López-Alt, E. Tromer and V. Vaikuntanathan, *On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption*, In STOC'12, 2012.

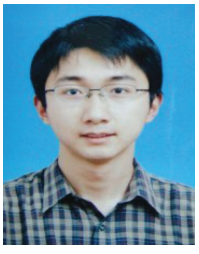
[19] Z. Brakerski and V. Vaikuntanathan, *Fully homomorphic encryption from ring-lwe and security for key dependent messages*, In CRYPTO'11, 2011.

[20] X. Liu, R.H. Deng, K.K.R. Choo and J. Weng, *An efficient privacy-preserving outsourced calculation toolkit with multiple keys*, IEEE Transactions on Information Forensics and Security, 11(11): 2401-2414, 2016.

[21] W. Ding, Z. Yan and R.H. Deng, *Secure encrypted data deduplication with ownership proof and user revocation*, ICA3PP 2017, LNCS 10393, pp. 297-312, 2017.

[22] J. Zhou, X. Dong, Z. Cao and A.V. Vasilakos, *Secure and privacy preserving protocol for cloud-based vehicular DTNs*, IEEE Transactions on Information Forensics and Security, 10(6): 1299-1314, 2015.

[23] A. Peter, E. Tews and S. Katzenbeisser, *Efficiently outsourcing multiparty computation under multiple keys*, IEEE Transactions on Information Forensics and Security, 8(12): 2046-2058, 2013.
[24] X. Liu, B. Qin, R.H. Deng and Y. Li, *An efficient privacy-preserving outsourced computation over public data*, IEEE Transactions on Services Computing, 10(5): 756-770, 2017.
[25] D. Boneh, H. Shacham and B. Lynn,*Short signatures from the weil paring*, J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.
[26] B. Waters, *Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization*, In PKC'11, 2011.
[27] B. Lynn, *PBC library*, http://crypto.stanford.edu/pbc/.
[28] *Multiprecision integer and rational arithmetic c/c++ library*, http://www.shamus.ie/.
[29] M. Bellare and P. Rogaway, *Random oracles are practical: A paradigm for designing efficient protocols*, In Proc. ACM CCS '93.
[30] M. Bellare, D. Micciancio and B. Warinschi, *Foundations of group signatures: formal definition, simplified requirements and a construction based on general assumptions*, In: EUROCRYPT 2003.
[31] K. Lauter, M. Naehrig and V. Vaikuntanathan, *Can homomorphic encryption be practical?* In: ACM CCS, 2011.
[32] E. Bresson, D. Catalano and D. Pointcheval, *A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications*, In: ASIACRYPT 2003.
[33] R. A. Brualdi, *Introductory Combinatorics (Fourth Edition)*, China Machine Press 2009.
[34] C. Wang, Y. Zheng, J. Jiang and K. Ren, *Toward privacy-preserving personalized recommendation services*, Engineering (2018), doi:https://doi.org/10.1016/j.eng.2018.02.005.



Jun Zhou received the Ph.D. degree in computer science with the Trusted Digital Technology Laboratory, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. He is currently an associate professor of computer science in East China Normal University. His research interests mainly include ciphertext access control and secure outsourced computation in cryptography and information security. He is a member of the IEEE.

Zhenfu Cao (SM'10) received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from the Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively. He was exceptionally promoted to Associate Professor in 1987, became a Professor in 1991, and is currently a Distinguished Professor with East China Normal University, China. Since 1981, over 400 academic papers have been published in journals or conferences. His research interests mainly include number theory, cryptography, and information security. He serves as a member of the Expert Panel of the National Nature Science Fund of China. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, and the Special Allowance by the State Council in 2005. He was a corecipient of the 2007 IEEE International Conference on Communications-Computer and Communications Security Symposium Best Paper Award in 2007. He is the Leader of the Asia 3 Foresight Program (61161140320), and the key project (61033014) of the National Natural Science Foundation of China.

Zhan Qin is a 100 Talent Professor at Zhejiang University, China. He obtained a Ph.D. from the State University of New York at Buffalo in 2017. His current research interests focus on data privacy, secure computation, crowdsourcing data security and smart grid security. He is a member of the IEEE.

Xiaolei Dong is a Distinguished Professor in East China Normal University. After her graduation with a doctorate degree from Harbin Institute of Technology in 2001, she pursued her post-doctoral study in SJTU from September 2001 to July 2003. She joined the Department of Computer Science and Engineering, SJTU, in 2003. In 2014, she joined East China Normal University, where she is currently a Distinguished Professor. Her primary research interests include number theory, cryptography, and trusted computing. Her Number Theory and Modern Cryptographic Algorithms project received the first prize of the China University Science and Technology Award in 2002. Her New Theory of Cryptography and Some Basic Problems project received the second prize of the Shanghai Nature Science Award in 2007. Her Formal Security Theory of Complex Cryptographic System and Applications project received the second prize of the Ministry of Education Natural Science Progress Award in 2008. She hosts a number of research projects supported by the National Basic Research Program of China (973 Program), and the special funds on information security of the National Development and Reform Commission, and the National Natural Science Foundation of China.

Kui Ren received the PhD degree from the Worcester Polytechnic Institute. He is currently a professor of computer science and technology and the director of the Institute of Cyberspace Research, Zhejiang University. He has published more than 200 papers in peer-reviewed journals and conferences. His current research interest spans cloud and outsourcing security, wireless and wearable systems security, and mobile sensing and crowdsourcing. He is an IEEE fellow, a member of the ACM, and a past board member of the Internet Privacy Task Force, State of Illinois. He received several Best Paper Awards, including IEEE ICDCS 2017, IWQoS 2017, and ICNP 2011. He received the IEEE CISTC Technical Recognition Award in 2017, the UB Exceptional Scholar Award for Sustained Achievement in 2016, the UB SEAS Senior Researcher of the Year Award in 2015, the Sigma Xi/IIT Research Excellence Award in 2012, and the NSF CAREER Award in 2011. He currently serves on the editorial boards of the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Service Computing, the IEEE Transactions on Mobile Computing, IEEE Wireless Communications, and the IEEE Internet of Things Journal.