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.

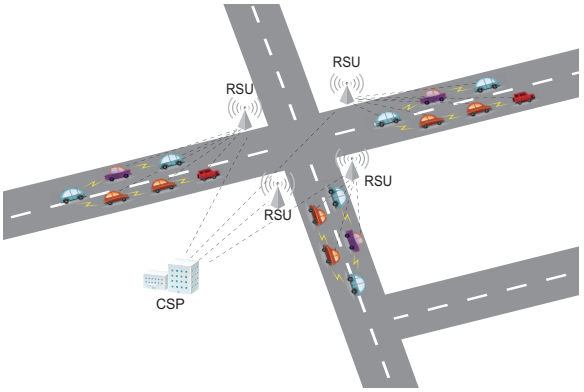

Fig. 1: Network Architecture of Privacy-preserving Location-based Service in VANETs

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