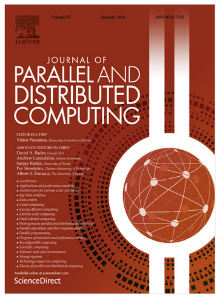
Accepted Manuscript



Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing

Jing Li, Xianmin Wang, Zhengan Huang, Licheng Wang, Yang Xiang

PII: S0743-7315(19)30262-X
DOI: https://doi.org/10.1016/j.jpdc.2019.04.003
Reference: YJPDC 4041

To appear in: *J. Parallel Distrib. Comput.*

Received date : 6 March 2018
Revised date : 1 February 2019
Accepted date : 1 April 2019

*Highlights (for review)

Highlights

1. A multi-secret sharing scheme with multi-level access structure was proposed, where the scheme does not need any trust party as a dealer.
2. The secret sharing scheme can share multiple secrets and each party only keeps a short share.
3. A decentralized multi-role e-voting protocol was designed based on the multi-level access structures.
4. The e-voting system achieves fast verification for the final election results and also does not need the authority center.

Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing

Jing Li[1*], Xianmin Wang[1], Zhengan Huang[1], Licheng Wang[2] and Yang Xiang[3,4]

1. School of Computer Science, Guangzhou University, Guangzhou, China.
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China.
3. State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xian 710071, China.
4. School of Software and Electrical Engineering, Swinburne University of Technology, Australia

Abstract

The cryptosystem-based data privacy preserving methods employ high computing power of cloud servers, where the main feature is to allow resource sharing and provide multi-user independent services. Therefore, to achieve the rapid allocation and release of resource sharing in cloud computing, decentralized cryptographic protocols need to be proposed for multi-user consensus systems. In this work, we first present a multi-secret sharing scheme with multi-level access structure, where the secret reconstruction algorithm satisfies the additive homomorphism. The secret sharing scheme needs no trusted third parties and any user can play the role of dealer. In the designing, multiple target secrets are independently shared, where each subset of users forms a sub access structure and shares one target secret only with a short secret share. This scheme is efficient and unconditionally secure.

Furthermore, based on the multi-level access structures, a decentralized multi-role e-voting protocol is designed using Chinese Remainder Theorem, where each role's election is associated with one sub-access structure. The voters employ a shared parameter to blind the sum of ballot values. Meanwhile, the e-voting scheme supports a public verification for the final election results. Compared with the existing e-voting protocols, our e-voting system does not require any authority center and the cloud server runs vote counting. And our e-voting scheme does not need any high-complexity computational cost operation such as module exponential operation, etc. Finally, the common feature of Blockchain and Ad Hoc networks is decentralized. Thus the main idea of this protocol without a trusted third party can be used to achieve a secure consensus among multiple nodes in Blockchain and Ad Hoc network, meanwhile, the consensus results can be verified.

Keywords:
Multi-secret sharing; Multi-role e-voting; Decentralized system; Cloud computing

1. Introduction

In 2006, the concept of cloud computing was proposed by Google at the Search Engine conference. The development of cloud computing quickly established a prairie "fire" and triggered the third wave of the information technology revolution. The computing model can provide usable, convenient, on-demand network access and access to configurable computing resource sharing pools [15, 26, 32], especially for Mobile Devices [9]. In outsourcing computing, the user's data and calculation are transplanted into an external, virtual cloud, then the computing and storage model simplifies the maintenance of information and reduces the cost of the user [22, 23]. To guarantee the security of sensitive data in such a semi-trusted model, the cryptosystems become effective techniques, which may require a trusted third party (or authority center). To realize rapid allocation and release of resource sharing, we mainly consider decentralized consensus mechanisms in multi-user cloud environment, such as mobile Ad Hoc network and Blockchain consensus [1, 19, 31].

Secret sharing is one primitive of multi-party computations, which is to distribute a secret among multiple participants and any authorized subset can recover the secret data. The collection of all authorized subsets is called an access structure, which supports the monotone ascending property [11]. The past three decades have seen a variety of secret sharing schemes (SSSs): In 1979, (t, n) threshold SSSs were designed by Shamir and Blakley based on Lagrange polynomial interpolation and projective geometry theory, respectively. In 1989, Brickell designed an ideal SSS based on vector space [4], realizing a general access structure [3, 14]. After then, verifiable SSSs were given in [6, 7, 8] for checking the validity of each participant. To improve the function of secret sharing schemes, dynamic SSSs [5, 21] were constructed, in which any member can join and leave the group and doesn't reveal any information about the secret. Besides, for the scheme efficiency, multiple secrets sharing schemes are designed within multipartite access structures [5, 11].

In particular, Hsu proposed a multi-secret sharing [11] based on monotone span programs (MSP) for general access structures, where each subset of participants shares a corresponding secret, called target secret. That is, the scheme is designed with respect to a family of access structures associated with multiple secrets. We note that the scheme can share n secrets at most, since the vector $\vec{r}$ hiding secrets only meets n linearly independent equations in the secret distribution phase [11], which can be used in attribute-based cryptosystems [33].

Most existing secret sharing schemes require trusted third parties (TTPs) to distribute secrets. However, considering the reliability and cost of TTP-s in practical applications, it is desired to construct SSSs without TTPs [27, 10, 25, 20]. In 1991, the first threshold secret sharing scheme without the assistance of any TTP was proposed by Pedersen [27]. And then a strong verifiable (n, t, n) SSS [10] was designed by Harn, in which participants check whether the verification polynomial is t-degree or not to decide the validity of the shares. Based on these SSSs, Liu presented a more efficient verifiable (n, t, n) SSS [25] that reduces the number of verification polynomials compared with Harn's SSS. In these schemes, each participant plays the role as a TTP and participates to generate a master secret, where the sub-secret is randomly chosen by each participant. Then the participant generates sub-shares and distributes its sub-secret to others participants based on Shamir′s SSS. Using the property of additive homomorphism [2], each participant is able to combine all received sub-shares into a master share. Therefore, the master secret can be recovered with knowledge of any t or more than t master shares. Note that a scheme realizes the (t, n) threshold structure, with n participants also acting as dealers simultaneously, so it is called (n, t, n) SSS. It is interesting to construct a more practical SSS for general access structure with no TTPs.

Considering some application scenarios, a SSS without TTPs can used into a decentralized consensus mechanisms. We will build an electronic voting (e-voting) protocol without any center authority (CA). Our goal is to make vote counting process more transparent and efficient, while allow voters to verify their election results. Furthermore, based on the multi-access structure SSSs without TTPs, we show the following situation for leader elections in an organization: One e-voting will be used to generate multiple leaders for managing different affairs. For example, a company needs to campaign three roles: a chairman, a general manager and two deputy general managers. It is unpractical to employ the direct sum of three parallel e-voting schemes for solving this problem, since such a method requires heavy computation cost and communication cost, meanwhile each voter will keep too much information. In this paper, we present a decentralized multi-role e-voting system based on a multi-secret sharing scheme (MSSS).

To solve this problem, we will construct a secure model for multi-role election without any authorized center. Based on a multi-access structure secret sharing scheme, each sub-access structure can be utilized to finish the election for one role, where each participant acts as a voter V_i and cloud server is the teller. Thus, the new e-voting model provides a multi-role election for different sets of candidates. In Figure 1, there are two sub-access structures–$\{V_1, V_2, V_3\}$ and $\{V_3, V_4, V_5\}$. Each sub-access structure shares a secret and V_i only carries one share. In the voting process for each sub-access structure, V_i uses his share to blind the vote and sends the blinded result to the cloud server. The cloud server aggregates all blinded results and returns the aggregated results to the corresponding sub-access structure. Finally, the parties recover their shared secret and get rid of blindness from the aggregated result, then each sub-access structure will obtain their own voting result.

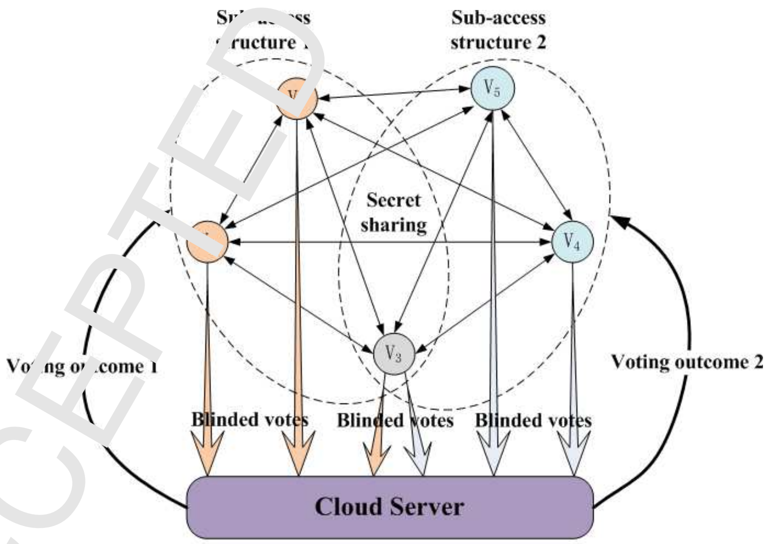


Figure 1: Multi-role E-voting based on MSSS

Our contributions. In this paper, we propose a multi-level multi-secret sharing scheme that realizes a family of access structures based on multi-target MSP. Due to the linear model of vector space, the secret reconstruction algorithm has a property of additive homomorphism. Thus, the participants can play the role of dealer to yield the shared secrets. Meanwhile, a sub-access structure has its target secret, thus the scheme supports multi-secret sharing and each participant keeps only one master share. Then, we prove that the scheme is unconditionally secure, where any subsets have no access to the secrets beyond its legal authority.

Furthermore, a multi-role e-voting system is designed based on the family of sub-access structures in the proposed MSSS. In the Setup phase, we use the Chinese Remainder Theorem (CRT) to select different prime module for each different candidate. Using this method, the e-voting system can achieve multi-role election among one collection of candidates, especially among disjoint collections of candidates. In the voting phase, the voters use a shared parameter to blind the sum of ballot values. Meanwhile, the e-voting scheme supports a public verification for the final election results, where any voter can check whether the sum of ballot values and the number of voters satisfy some fixed relation. Compared with the current e-voting protocols, our e-voting system supports public verification and does not need authority centers, that is, this scheme is decentralized.

The rest of this work is organized as follows: In Section 2, some basic definitions are reviewed. Section 3 presents an MSSS with no trusted third party. In Section 4, a decentralized multi-role e-voting system is proposed. Finally, conclusions are provided in Section 5.

2. Preliminaries

2.1. Access structure

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of participants. An access structure Γ is defined on $\mathcal{P}$ and Γ is a collection of all authorized subsets of $\mathcal{P}$ that satisfies monotone ascending property, then we only need to consider the minimum access structure.

2.2. Monotone span programs

Monotone span program (MSP) $\mathcal{M}(\mathcal{P}, \mathcal{F}, M, \psi)$ [16] involves a set of parties $\mathcal{P}$, a finite field $\mathcal{F}$, a matrix M over this field and a labeling map ψ, where M is a $d \times l$ matrix and ψ is a surjection from $\{1, \ldots, d\}$ to $\{P_1, \ldots, P_n\}$. Actually, MSP is a model for computing Monotone Boolean Function. Suppose that $\vec{v}$ is a target vector, if $\vec{v}$ can be linearly combined by the rows of M_A for

$A \subset \mathcal{P}$, where the row numbers of M_A are the preimages of all $P_i \in A$. Then Boolean function value $f(A) = 1$.

2.3. linear secret sharing

For a given an access structure Γ, constructing a linear secret sharing scheme (LSSS) on Γ is equivalent to obtaining an MSP. Generally, the target vector $\vec{v}$ is $(1, 0, \ldots, 0)$. If $A \in \Gamma$ and $P_i \in A$ for some i, then v can be linearly combined by M_i, that is, $v = \sum_{P_i \in A} a_i \cdot M_i$ for $a_i \in \mathcal{F}$. Let s be the shared secret. Randomly select a vector $\vec{w} = (s, w_1, w_2, \ldots, w_{l-1})$, each P_i will get his share y_i, where y_i is the inner product of M_i and $\vec{w}$. Thus, any authorized subset A can recover the secret as $s = \sum_{P_i \in A} a_i \cdot y_i$. Thus, a linear multi-secret sharing scheme [11] can be obtained based on multi-target vectors the corresponding m-tuple $\vec{\Gamma} = (\Gamma_1, \ldots, \Gamma_m)$ of access structures.

3. Multi-secret sharing scheme

Inspired by the multi-secret sharing scheme (MSSS) in [11], we present the construction of our MSSS with no trusted third party.

3.1. Description of MSSS

Setup : Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the participant set and $\Upsilon(\mathcal{P})$ be the power set of $\mathcal{P}$. Here, $|\Upsilon(\mathcal{P})|$ is 2^n. Then, the cardinality of the collection of the nonempty subsets of $\mathcal{P}$ is $2^n - 1$. Let $m = 2^n - 1$ and an m-tuple access structure be $\vec{\Gamma} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$, where Γ_l only contains the lth nonempty subset (we consider the minimum access structure). Let S_l denote the target secret associated with a sub-access structure Γ_l ($1 \leqslant l \leqslant m$). Thus, a multi-level access structure is well-defined.

Multi-target MSP : Let $\mathcal{F} = F_p^n$ for prime p. Randomly choose an $n \times n$ invertible matrix M. Let $u_i = M_i$, then each set of at most n vectors in $\{u_1, \ldots, u_n\}$ is linearly independent, where u_i is the adjoint vector of participant P_i and $V_i = \text{span}\{\vec{u}_i\}$.

Furthermore, let $\vec{v}_l = \sum_{\substack{P_i \in \Gamma_l \\ x_{i,l} \in F_p}} x_i \cdot \vec{u}_i$ $(l = 1, \ldots, m)$ be m target vectors, where coefficients $x_{i,l}$ are randomly chosen from field F_p. Then we can obtain a multi-target MSP $\mathcal{M}(\mathcal{F}, F_p, M, \psi)$, where $\psi(i) = P_i$ $(1 \leq i \leq n)$.

Note that, the matrix M, all target vectors and $x_{i,l}$ are public.

Secret sharing : The algorithm is composed of three stages:

- Master secret generation. Each participant P_i $(1 \le i \le n)$ selects a random vector $\vec{r}_i \in F_p^n$ and computes $S_{i,l} = \vec{r}_i \cdot \vec{v}_l$ for sub-access structure Γ_l $(l = 1, \ldots, m)$. Here, $S_{i,l}$ $(l = 1, \ldots, m)$ are sub-secrets determined by P_i. And m master secrets can be determined as $S_l = \sum_{i=1}^{n} S_{i,l}$, for $l = 1, \ldots, m$.
- Sub-share generation. Each participant P_i $(1 \le i \le n)$ computes and sends the inner product $s_{ij} = \vec{r}_i \cdot \vec{u}_j = \vec{r}_i \cdot M_j$ to P_j, for $j = 1, \ldots, n$. Meanwhile, P_i obtains n sub-shares, s_{ji} $(j = 1, \ldots, n)$.
- Master share generation. Participant P_i calculates the corresponding master share $s_i = \sum_{j=1}^{n} s_{ji}$.

Secret reconstruction : For any authorized subset $A \in \Gamma_l$ $(1 \le l \le m)$, since $\vec{v}_l = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i$, then the participants in A can reconstruct secret $S_l = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_i$ $(1 \le l \le m)$ (see the correctness proof of Theorem 1).

Note that in such an MSSS, each participant P_i $(1 \le i \le n)$ only needs to carry one master share s_i to be able to reconstruct multiple secrets by linearly combining the corresponding master shares. Table 1 and Table 2 present master secrets and master shares generation.

Table 1: Master secrets generation

	P_1	$\cdots$	P_n	Master secret
Γ_1	$S_{1,1}$	$\cdots$	$S_{n,1}$	$S_1 = \sum_{i=1}^{n} S_{i,1}$
Γ_2	$S_{1,2}$	$\cdots$	$S_{n,2}$	$S_2 = \sum_{i=1}^{n} S_{i,2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Γ_m	$S_{1,m}$	$\cdots$	$S_{n,m}$	$S_m = \sum_{i=1}^{n} S_{i,m}$

3.2. Correctness and Security

In this section, from the information theory, we will prove that our scheme is a perfect SSS, where Theorem 1 shows the correctness and Theorem 2 presents the privacy [11, 29].

Table 2: Master shares generation

	P_1	$\cdots$	P_n	Master share
P_1	s_{11}	$\cdots$	s_{n1}	$s_1 = \sum_{j=1}^{n} s_{j1}$
P_2	s_{12}	$\cdots$	s_{n2}	$s_2 = \sum_{j=1}^{n} s_{j2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
P_n	s_{1n}	$\cdots$	s_{nn}	$s_n = \sum_{j=1}^{n} s_{jn}$

Theorem 1. For any authorized subset $A \in \Gamma_l$ ($1 \leq l \leq m$), A can recover the shared secret.

Proof. Since $A \in \Gamma_l$, and the target vector $\vec{v}_l = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i$. Then we have the following equations:

$$S_{1,l} = \vec{r}_1 \cdot \vec{v}_l = \vec{r}_1 \cdot (\sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i) = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i(\vec{r}_1 \cdot \vec{u}_i) = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_{1i},$$
$$S_{2,l} = \vec{r}_2 \cdot \vec{v}_l = \vec{r}_2 \cdot (\sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i) = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i(\vec{r}_2 \cdot \vec{u}_i) = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_{2i},$$
$$\cdots$$
$$S_{n,l} = \vec{r}_n \cdot \vec{v}_l = \vec{r}_n \cdot (\sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i) = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i(\vec{r}_n \cdot \vec{u}_i) = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_{ni}.$$

Thus, the master secret S_l can be determined as

$$S_l = \sum_{i=1}^{n} S_{i,l} = S_{1,l} + \ldots + S_{n,l} \tag{1}$$
$$= \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_{1i} + \ldots + \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_{ni} \tag{2}$$
$$= \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot (\sum_{j=1}^{n} s_{ji}) \tag{3}$$
$$= \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_i. \tag{4}$$

where Eq. (3) follows from the property of additive homomorphism. Thus, any authorized subset $A \in \Gamma_l$ can recover the master secret S_l by calculating a linear combination of participants' master shares. □

Theorem 2. For any unauthorized subset $B \notin \Gamma_l$ and $A_l \not\subseteq B$ for $1 \leq l \leq m$, where $\Gamma_l = \{A_l\}$. Then, B fails to get any information about the shared secret S_l.

Proof. Suppose that $\vec{\Gamma} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$, $\vec{u}_i$ and $\vec{v}_l$ are defined in section 3.1, Since the vectors $\vec{u}_1, \ldots, \vec{u}_n$ are linearly independent and $A_l \not\subseteq B$. Then, $\vec{v}_l$ does not lie in $span\{u_j\}$ for P_j belongs to the unauthorized subset B. Otherwise, we have $\vec{v}_l = \sum_{\substack{P_j \in B \\ y_j \in F_p}} y_j \cdot \vec{u}_j$. Since $\vec{v}_l = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i$. Then, $\sum_{\substack{P_j \in B \\ y_j \in F_p}} y_j \cdot \vec{u}_j = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i$. This implies that $\vec{u}_1, \ldots, \vec{u}_n$ are linearly dependent, which is a contradiction. Thus, any unauthorized subset B fails to get any information about the shared secret S_l.

On the other hand, we want to illustrate the security from the information theory. We compute the information entropy $H(\mathcal{S}_l)$ of obtaining secret S_l with knowing its space $\mathcal{S}_l$ and the entropy $H(\mathcal{S}_l|B)$ of getting S_l with knowing $\mathcal{S}_l$ and shares for B. Suppose that $\vec{r}$ is an n-dimensional vector and there is a random number $S'_l \in \mathcal{S}_l$. For any unauthorized subset $B \notin \Gamma_l$, we can construct the following equations:

$$\begin{cases} \vec{v}_l \cdot \vec{r} = S'_l \\ \vec{u}_1 \cdot \vec{r} = s_1 \\ \quad \cdots \\ \vec{u}_i \cdot \vec{r} = s_i \\ \quad \cdots \\ \vec{u}_{|B|} \cdot \vec{r} = s_{|B|} \end{cases} \tag{5}$$

In the master shares generation phase, we have that $\vec{u}_i \cdot (\vec{r}_1 + \cdots + \vec{r}_n) = s_i$, for $i = 1, \ldots, n$. Thus, the following equations

$$\begin{cases} \vec{u}_1 \cdot \vec{r} = s_1 \\ \quad \cdots \\ \vec{u}_i \cdot \vec{r} = s_i \\ \quad \cdots \\ \vec{u}_{|B|} \cdot \vec{r} = s_{|B|} \end{cases} \tag{6}$$

have solutions. That is, $\vec{r} = \sum_{i=1}^{n} \vec{r}_i$. Meanwhile, since $\vec{v}_l \notin \bigcup_{B \in (\mathcal{A}_l)_{\max}} \sum_{P_i \in B} V_i$, we have that $Rank(\{\vec{u}_1, \ldots, \vec{u}_{|B|}\}) + 1 = Rank\ (\{\vec{u}_1, \ldots, \vec{u}_{|B|},\ \vec{v}_l\})$ and the rank of coefficient matrix is equal to that of augmented matrix. Eqs.(5) always have solutions with respect to any element $S'_l \in \mathcal{S}_l$. Therefore,

$$H(\mathcal{S}_l|B) = \sum_{S_l \in \mathcal{S}_l} Pr[S_l|B] \cdot \log Pr[S_l|B] = \sum_{i=1}^{p} \frac{1}{p} \log p = \log p = H(\mathcal{S}_l).$$

We see that the security of our scheme is proved from the aspect of information theory. That is, the scheme is unconditionally-secure without no assumption of intractable problem.

3.3. Efficiency analysis

The efficiency of our proposal is summarized in Table 3. NMO$_D$ denotes the number of module multiplication required by each participant in the distribution phase and NMO_R denotes the number of multiplication required in the reconstruction phase. NTS indicates the number of shared target secrets, NMS is the number of master shares for every participant, and NSS is the number of sub-shares sent from one participant to others.

• NMO_D: Since each one needs to perform n inner product operations between two n-dimension vectors, then each participant requires n^2 times multiplication.

• NMO_R: For l-th sub-access structure, secret reconstruction needs $|\Gamma_l|(\leq n)$ times multiplication (see Section 3.2).

• NTS: There are $m = 2^n - 1$ master secrets shared in the scheme (see Table 1).

• NMS: From Table 2, we see that each participant carries only one share that is combined by n sub-shares.

• NSS: In the distribution phase, each one sends $n - 1$ sub-shares to other $n - 1$ corresponding participants.

Table 3: Quantitative analysis on SSS

	NMO_D	NMO_R	NTS	NMS	NSS
Number	n^2	$\|\Gamma_l\|$	$2^n - 1$	1	$n - 1$

In summary, each participant only carries one master share for sharing multiple master (target) secrets. Furthermore, the scheme needs no trusted third party and it can be used to construct a decentralized e-voting protocol.

Table 4: Performance Comparison on SSS without TTPs

	SSS [10]	SSS [25]	SSS [20]	Our SSS
Access Structure	One-level	One-level	One-level	Multi-level
Multi-secret	No	No	Yes	Yes
Exponential computation	No	No	Yes	No

4. A multi-role e-voting system

Now we present a decentralized e-voting protocol for multi-role election.

4.1. Description of the e-voting system

Setup : Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a voter set, $m = 2^r - 1$ be the number of sub-voting protocols. Here, we continue to use the access structure and MSP constructed in Section 3. With respect to sub-access structure Γ_l $(1 \leq l \leq m)$, a sub-voting protocol can be correspondingly designed. Let $\mathcal{C}_l = \{C_{l,1}, C_{l,2}, \ldots, C_{l,k_l}\}$ be the set of k_l candidates for the l-th sub-protocol for $l \in \{1, \ldots, m\}$.

The cloud server broadcasts the values v_{yes}, v_{no} and v_0, such that $n^2 v_0 < n v_{no} < v_{yes}$, where v_{yes}, v_{no} and v_0 are assigned to the yes (Y) vote, the no (N) vote and the abstention (A) vote, respectively. Suppose that $k = \max\{k_l |\ l = 1, \ldots, m\}$. Then the cloud chooses a prime sequence $p_1, p_2, \ldots, p_k$, such that $p_\lambda > n \cdot v_{yes}$ and $\prod_{\lambda=1}^{k} p_\lambda < p$ (here, p is defined in above SSS).

Ballot Generation : This algorithm uses Chinese Remainder Theorem and the proposed secret sharing scheme.

- Each voter P_i $(1 \leq i \leq n)$ selects a random vector $\vec{r}_i \in F_p^n$ and computes $S_{i,l} = \vec{r}_i \cdot v_l$, for $l = 1, \ldots, m$. Then he generates his votes $b_{i,l,\lambda}$ for candidate $C_{l,\lambda}$ $(C_{l,\lambda} \in \mathcal{C}_l)$, where $b_{i,l,\lambda} \in \{v_{yes}, v_{no}, v_0\}$ and $\lambda = 1, \ldots, k_l$. P_i computes $B_{i,l}$ by using Chinese Remainder Theorem to solve k_l equations:

$$\{B_{i,l} \equiv b_{i,l,\lambda} \bmod p_\lambda,\ C_{l,\lambda} \in \mathcal{C}\}$$

- Then voter P_i broadcasts ballots $T_{i,l} = S_{i,l} + B_{i,l}$, where $S_{i,l}$ are blinding factors, for $l = 1, \ldots, m$ (see Table 5).
- Each voter P_i $(1 \leq i \leq n)$ sends the inner product $s_{ij} = \vec{r}_i \cdot \vec{u}_j$ to P_j, for $j = 1, \ldots, n$. Then each voter P_i receives s_{ji} and computes $s_i = \sum_{j=1}^{n} s_{ji}$.

Vote Counting : This algorithm mainly employs the secret reconstruction algorithm. At the same time, there is no need of an authority center for vote tallying.

- For the l-th sub-protocol, P_i $(P_i \in \Gamma_l,\ 1 \leq l \leq m)$ sends s_i to the cloud server without secret channels. Since $\vec{v}_l = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot \vec{u}_i$, then the cloud recovers $S_l = \sum_{\substack{P_i \in \Gamma_l \\ x_i \in F_p}} x_i \cdot s_i$ and computes $B_l = T_l - S_l$, where $T_l = \sum_{i=1}^{n} T_{i,l}$, $B_l = \sum_{i=1}^{n} B_{i,l}$.

- The numbers of Y, N and A votes, denoted by $x_{l,\lambda}$, $y_{l,\lambda}$ and $z_{l,\lambda}$ for candidate $C_{l,\lambda}$ $(1 \leq \lambda \leq k_l)$, can be computed by solving equation:

$$x_{l,\lambda} \cdot v_{yes} + y_{l,\lambda} \cdot v_{no} + z_{l,\lambda} \cdot v_0 \equiv B_l \pmod{p_\lambda},$$

where $n^2 v_0 < n v_{no} < v_{yes}$ and $x_{l,\lambda} + y_{l,\lambda} + z_{l,\lambda} = n$. Then the solution is

$$\hat{x}_{l,\lambda} \leftarrow B_l \bmod p_\lambda, \qquad x_{l,\lambda} \leftarrow \lfloor \hat{x}_{l,\lambda}/v_{yes} \rfloor;$$

$$\hat{y}_{l,\lambda} \leftarrow \hat{x}_{l,\lambda} \bmod v_{yes}, \qquad y_{l,\lambda} \leftarrow \lfloor \hat{y}_{l,\lambda}/v_{no} \rfloor;$$

$$\hat{z}_{l,\lambda} \leftarrow \hat{y}_{l,\lambda} \bmod v_{no}, \qquad z_{l,\lambda} \leftarrow \lfloor \hat{z}_{l,\lambda}/v_0 \rfloor.$$

- Finally, the voting outcome $x_{l,\lambda}$, $y_{l,\lambda}$, $z_{l,\lambda}$ and s_i is public. Each additional Y vote is 2 points, each additional A vote is 1 point and each additional N vote is 0 point. Hence, all parties can choose the winner according to the voting results. Furthermore, any one can check its validity: if $x_{l,\lambda} + y_{l,\lambda} + z_{l,\lambda} = n$ and $x_{l,\lambda}$, $y_{l,\lambda}$, $z_{l,\lambda}$ are integers, then there is no fraud.

Table 5: Quantitative analysis on SSS

	P_1	$\cdots$	P_n	Masked votes
Γ_1	$T_{1,1}$	$\cdots$	$T_{n,1}$	$T_1 = \sum_{i=1}^{n} T_{i,1}$
Γ_2	$T_{1,2}$	$\cdots$	$T_{n,2}$	$T_2 = \sum_{i=1}^{n} T_{i,2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Γ_m	$T_{1,m}$	$\cdots$	$T_{n,m}$	$T_m = \sum_{i=1}^{n} T_{i,m}$

To illustrate the e-voting protocol better, we give an example in appendix.

4.2. Discussion and analysis

Now we analyze some important properties for this new e-voting protocol.

• **Correctness.** The correctness holds based on Theorem 1 and Chinese Remainder Theorem.

• **Multi-role.** An e-voting protocol is said to be multi-use, if it can be used to simultaneously finish multiple roles in one election. In our e-voting system, each role can be chosen based on the corresponding sub-access structure.

Thus, on the basis of the family of access structures defined in MSSS, the e-voting model achieves multi-role election.

• **Decentralization.** The e-voting protocol does not need any trusted third party. The vote tallying is finished by the cloud server.

• **Anonymity.** Any unauthorized voter set or cloud servers cannot link a voter′s identity to the corresponding vote. For one reason, all voters blind their real votes. For another, the anonymity was ensured by homomorphic property. The cloud servers can only compute the final votes summation $B_l = T_l - S_l$, without the knowledge of single votes $B_{i,l}$ $(1 \leq i \leq n)$. And Theorem 3 below shows that the published parameters won't reveal the real votes. Thus, the proposed protocol supports the anonymity.

• **Uniqueness**. Each voter can throw only one vote. If there exists one malicious voter P_i, giving multiple votes, then $x_{l,\lambda} + y_{l,\lambda} + z_{l,\lambda} \neq n$. Thus, no dishonest voter can perform the election fraud by throwing multiple votes.

• **Public verifiability.** Since the ballots $T_{i,l}$ and parameters s_i are published for verification. Any party can check the validity of the outcome based on the Uniqueness.

Theorem 3. Suppose that parameters $T_{i,l}$, s_i $(i = 1, \ldots, n, l = 1, \ldots, m)$ published are defined as above, it holds that no one can obtain blinding factors $S_{i,l}$ $(i = 1, \ldots, n, l = 1, \ldots, m)$ from s_i and the real votes $B_{i,l}$ are unknown.

Proof. From Theorem 1, we see that the system of equations about $S_{i,l}$ $(i = 1, \ldots, n, l = 1, \ldots, m)$ as follows:

$$\begin{cases} S_{1,1} + S_{2,1} + \cdots + S_{n,1} = \sum_{\substack{P_i \in \Gamma_1 \\ x_{i1} \in F_p}} x_{i1} \cdot s_i \\ \cdots \\ S_{1,l} + S_{2,l} + \cdots + S_{n,l} = \sum_{\substack{P_i \in \Gamma_l \\ x_{il} \in F_p}} x_{il} \cdot s_i \\ \cdots \\ S_{1,m} + S_{2,m} + \cdots + S_{n,m} = \sum_{\substack{P_i \in \Gamma_m \\ x_{im} \in F_p}} x_{im} \cdot s_i \end{cases} \tag{7}$$

where x_{il} $(x_{il} \in F_p)$ are known. Because there are m equations and mn unknowns $(m < mn)$, no one can solve $S_{i,l}$ $(i = 1, \ldots, n, l = 1, \ldots, m)$. Thus, the public parameters does not reveal the real votes $B_{i,l}$. $\square$

Performance Comparison. The most existing e-voting protocols [17, 18, 28, 30] were proposed based on digital signature schemes, and those schemes used discrete logarithm and bilinear pairing operations, which need high-complexity computational cost. Compared with the most existing e-voting protocols, our protocol is constructed based on linear multi-secret sharing scheme (MSSS) and it only needs some additions and multiplications in the given finite field F_p. For example, the vote casting phase for one role election only requires $2n$ module multiplications, where n is the number of voters. Assume that p is about 160-bit for resisting exhaustive attacks and let $n < 100$, then the computational cost of this phase can be counted in Microseconds (μs). In [17], the running time of the vote casting phase was counted in Millisecond (ms). Secondly, based on the MSSS and Chinese Remainder Theorem, our scheme achieves a multi-role e-voting in one election, thus it has a higher utilization. In addition, compared with the traditional e-voting schemes, our scheme does not need an authority center. In other words, the tally phase can be outsourced to a cloud server for saving computational resources.

5. Conclusions

In this work, we construct a multi-secret sharing scheme based on multi-target MSP. The scheme does not require any trusted center, where each participant is also a dealer to generate master secrets together. Then, the scheme can be applied into a decentralized consensus system. Furthermore, based on the multi-target MSP, we design a multi-role e-voting model based on Chinese Remainder Theorem that can simultaneously achieve multiple roles in one election, without employing an authority center. Meanwhile, the protocol supports publicly verification for the voting outcome. In the future work, we will design more efficient e-voting protocols under different security models [12, 13] and apply the protocols to IoTs [24].

Acknowledgements

This work was supported by National Natural Science Foundation of China (Nos. 61472091, 61370194), Natural Science Foundation of Guangdong Province for Distinguished Young Scholars (No. 2014A030306020), Guangzhou scholars project for universities of Guangzhou (No. 1201561613), Science and Technology Planning Project of Guangdong Province, China (No. 2015B010129015), National Natural Science Foundation for Outstanding Youth Foundation (No. 61722203), National Key R&D Program of China (No. 2016YFN0800602), Shandong provincial Key R&D Program of China (No. 2018CXGC0701) and JSPS KAKENHI Grant Number JP15K00028.

[1] M. Ambrosin, P. Braca, M. Conti, et al. ODIN: Obfuscation-based privacy preserving consensus algorithm for Decentralized Information fusion in smart device Networks. 2017.

[2] J.C. Benaloh. Secret sharing homomorphisms: keeping shares of a secret, in: Advances in Cryptology, Proceedings of the Crypto86, 11-15 August, Santa Barbara, California, USA, LNCS, vol. 263, Springer-Verlag, Berlin, 1987: 251-260.

[3] J. Benaloh, J. Leichter, Generalized secret sharing and monotone functions, in: S. Goldwasser (Ed.), Advances in Cryptology, CRYPTO88, in: Lecture Notes in Computer Science, 1989, 403: 27-35.

[4] E.F. Brickell. Some Ideal Secret Sharing Schemes. Journal of Combinatorial Mathematics & Combinatorial Computing, 1989, 434: 468-475.

[5] A. Das, A. Adhikari, An efficient multi-use multi-secret sharing scheme based on hash function, Applied Mathematics Letters, 2010, 23: 993-996.

[6] M.H. Dehkordi, S. Mashhadi. An efficient threshold verifiable multi-secret sharing. Computer Standards & Interfaces, 2008, 30(3): 187-190.

[7] M.H. Dehkordi, S. Mashhadi. New efficient and practical verifiable multi-secret sharing schemes. Information Sciences, 2008, 178(9): 2262-2274.

[8] M.H. Dehkordi, S. Mashhadi. Verifiable secret sharing schemes based on non-homogeneous linear recursions and elliptic curves. Computer Communications, 2008, 31(9): 1777-1784.

[9] C. Gao, S. Lv, Y. Wei, Z. Wang, Z. Liu, X. Cheng. M-SSE: An Effective Searchable Symmetric Encryption with Enhanced Security for Mobile Devices. IEEE Access, 6: 38860-38869, 2018.

[10] L. Harn, C. Lin. Strong (n, t, n) verifiable secret sharing scheme, Information Sciences, 2010, 180: 3059-3064.

[11] C.F. Hsu, Q. Cheng, X.M. Tang, B. Zeng, An ideal multi-secret sharing scheme based on MSP, Information Sciences, 2011, 181: 1403-1409.

[12] Z. Huang, J. Lai, W. Chen, M. Raees-ul-Haq, L. Jiang. Practical public key encryption with selective opening security for receivers. Information Sciences, 2019, 478: 15-27.

[13] Z. Huang, J. Lai, W. Chen, T. Li, Y. Xiang. Data security against receiver corruptions: SOA security for receivers from simulatable DEMs. Information Sciences, 2018, 471: 201-215.

[14] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing general access structure. Electronics & Communications in Japan, 1989, 72(9): 56-64.

[15] L. Jiang, Y. Cheng, L. Yang, J. Li, H. Yan, X. Wang. A Trust-Based Collaborative Filtering Algorithm for E-Commerce Recommendation System. Journal of Ambient Intelligence and Humanized Computing, DOI: 10.1007/s12652-018-0928-7, 2018.

[16] M. Karchmer, A. Wigderson, On span programs, in: Proceedings of the Eighth Annual Conference on Structure in Complexity, San Diego, CA, 1993: 102-111.

[17] M. Kumar, C.P. Katti, P.C. Saxena. A Secure Anonymous E-Voting System Using Identity-Based Blind Signature Scheme. Information Systems Security. ICISS 2017. Lecture Notes in Computer Science, vol 10717. Springer.

[18] W. Jamroga, M. Knapik, D. Kurpiewski. Model Checking the SELENE E-Voting Protocol in Multi-agent Logics: Third International Joint Conference, E-Vote-ID 2018, Bregenz, Austria, October 2-5, 2018, Proceedings: Electronic Voting. Springer, 2018.

[19] K. Yeow, A. Gani, R.W. Ahmad, et al. Decentralized consensus for edge-centric interent of things: a review taxonomy and reserch issues. IEEE Access, 2017, 99: 1-1.

[20] J. Li, L. Wang, J. Yan, et al. A (k, t, n) verifiable multi-secret sharing scheme based on adversary structure. Ksii Transactions on Internet & Information Systems, 2014, 8(12): 4552-4567.

[21] H.Y. Lin and Y. Shiung. Dynamic multi-secret sharing scheme. Int. J. Contemp.math.Sciences, 2008, 3(1): 37-42.

[22] T. Li, Z. Huang, P. Li, Z. Liu, C. Jia. Outsourced Privacy-Preserving Classification Service over Encrypted Data. Journal of Network and Computer Applications, 2018, 106: 100-110.

[23] T. Li, W. Chen, Y. Tang, H. Yan. A Homomorphic Network Coding Signature Scheme for Multiple Sources and its Application in IoT. Security and Communication Networks, 2018, DOI: 10.1155/2018/9641273, 2018.

[24] T. Li, C. Gao, L. Jiang, W. Pedrycz, J. Shen. Publicly verifiable privacy-preserving aggregation and its application in IoT. Journal of Network and Computer Applications, 2018, 126: 39-44.

[25] Y.X. Liu, L. Harn, C.N. Yang, Y.Q. Zhang, Efficient (n, t, n) secret sharing schemes, Journal of Systems and Software, 2012, 85: 1325-1332.

[26] Y. Lyu, V.C.S. Lee, C.Y. Chow, et al. R-Sharing: Rendezvous for Personalized Taxi Sharing. IEEE Access, 2017, 99: 1-1.

[27] T.P. Pedersen. A threshold cryptosystem without a trusted party, in: Advances in Cryptology, Proceedings of the Eurocrypt'91, 8-11 April, Brighton, UK, LNCS, Springer-Verlag, Berlin, 1991, 547: 522-526.

[28] E.A. Quaglia, B. Smyth. Authentication with Weaker Trust Assumptions for Voting Systems. International Conference on Cryptology in Africa. Springer, 2018.

[29] C.E. Shannon and W. Weaver. The Mathematical Theory of Communication, The University of Illinois Press, Urbana, IL, 1949.

[30] S. Tamura, H.A. Haddad, N. Islam, et al. An Incoercible E-Voting Scheme Based on Revised Simplified Verifiable Re-encryption Mix-nets. Computer Science, 2015.

[31] Q. Xia, E.B. Sifah, K.O. Asamoah, et al. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access, 2017, 5: 14757-14767.

[32] J. Zhang, Z. Zhang. Secure and efficient data-sharing in clouds. Concurrency & Computation Practice & Experience, 2015, 27(8): 2125-2143.

[33] Y. Zhang, D Zheng, R.H. Deng, Security and privacy in smart health: Efficient policy-hiding attribute-based access control, IEEE Internet of Things Journal, 2018, 5(3): 2130-2145.

Appendix A. Toy example

We now give an example to show the process of the e-voting system.

- Multi-target access structure:

  Let $\mathcal{P}=\{P_1,P_2,P_3\}$ and $\Omega=\{\{P_1\},\{P_2\},\{P_3\},\{P_1,P_2\},\{P_1,P_3\},\{P_2,P_3\},\{P_1,P_2,P_3\}\}$. It can be seen that $n=3$, $m=7$, $\varphi:\{1,\dots,7\}\to\Omega$ and there are seven master secrets to be shared in such a 7-tuple $\vec{\Gamma}=\{\Gamma_1,\dots,\Gamma_7\}$ of access structures as follows:
  $(\Gamma_1)_{min}=\{\{P_1\}\}$, $(\Gamma_2)_{min}=\{\{P_2\}\}$, $(\Gamma_3)_{min}=\{\{P_3\}\}$, $(\Gamma_4)_{min}=\{\{P_1,P_2\}\}$, $(\Gamma_5)_{min}=\{\{P_1,P_3\}\}$, $(\Gamma_6)_{min}=\{\{P_2,P_3\}\}$, $(\Gamma_7)_{min}=\{\{P_1,P_2,P_3\}$

- Target-vector generation:

  Suppose that $p=6045133$ and $\overline{\mathrm{V}}=F_p^3$ with a basis $\{\vec{e}_1,\vec{e}_2,\vec{e}_3\}$, where $\vec{e}_1=(1,2,5)$, $\vec{e}_2=(3,7,10)$ and $\vec{e}_3=(4,1,9)$. Let $\vec{u}_1=\mathbf{v}(1)=(8,10,24)$ associated with P_1, $\vec{u}_2=\mathbf{v}(3)=(46,32,116)$ associated with P_2 and $\vec{v}_3=\mathbf{v}(4)=(77,46,189)$ associated with P_3. Let seven target vectors be as follows: $\vec{v}_1=\mathbf{v}(1)=(8,10,24)$, $\vec{v}_2=2\mathbf{v}(3)=(92{,}64{,}232)$, $\vec{v}_3=3\mathbf{v}(4)=(231{,}138{,}567)$, $\vec{v}_4=2\mathbf{v}(1)+\mathbf{v}(3)=(62{,}52,164)$, $\vec{v}_5=\mathbf{v}(1)+2\mathbf{v}(4)=(162,102,402)$, $\vec{v}_6=3\mathbf{v}(3)+2\mathbf{v}(4)=(292,188,726)$, $\vec{v}_7=4\mathbf{v}(1)+2\mathbf{v}(3)+3\mathbf{v}(4)=(355,242,895)$, where the coefficients in the expressions above are randomly chosen from field F_p.

We will give the continued example with respect to Γ_5 and Γ_6.

- Master secret generation:

  P_1, P_2 and P_3 selects $\vec{r}_1 = (7,4,13)$, $\vec{r}_2 = (11,3,6)$ and $\vec{r}_3 = (1,19,5)$, respectively. Then participant P_i computes $S_{i,l} = \vec{r}_i \cdot \vec{v}_l$ $(i = 1,\ldots,3,$ $l = 5,6)$ as $S_{1,5} = 6768$, $S_{1,6} = 12234$; $S_{2,5} = 4500$, $S_{2,6} = 8132$; $S_{3,5} = 4110$, $S_{3,6} = 7494$. Then master secrets are $S_5 = 15378$ and $S_6 = 27860$.

- Master share generation:

  Participant P_i computes sub-share $s_{ij} = \vec{r}_i \cdot \vec{u}_j$ $(i = 1,\ldots,3,$ $j = 1,\ldots,3)$ that $s_{11} = 408$, $s_{12} = 1958$ and $s_{13} = 3180$; $s_{21} = 262$, $s_{22} = 1298$ and $s_{23} = 2119$; $s_{31} = 318$, $s_{32} = 1234$ and $s_{33} = 1896$. Then master shares are $s_1 = 988$, $s_2 = 4490$ and $s_3 = 7195$.

- Master secret reconstruction:

  For master secret S_6 with respect to Γ_6 is determined as $S_6 = 3s_2 + 2s_3 = 3 \cdot 4490 + 2 \cdot 7195 = 27860$, where the coefficients "3" and "2" are obtained from the expression of target vector $\vec{v}_6$, while s_2 and s_3 are the master shares of participants P_2 and P_3, respectively.

Note that the above operations in MSSS are finished over field F_p.

- Public parameters for e-voting:

  Let the set of candidates be $\mathcal{C}_5 = \mathcal{C}_6 = \{C_1, C_2, C_3, C_4\}$. The central authority CA chooses $v_{yes} = 13$, $v_{no} = 4$, $v_0 = 1$ and then selects $p_1 = 41, p_2 = 43, p_3 = 47, p_4 = 53$ that can satisfy the conditions of $n \cdot v_{yes} < p_\lambda$ and $\prod_{\lambda=1}^{4} p_\lambda < p$.

- Ballot Generation:

  Each voter P_i generates his votes $b_{i,l,\lambda} \in \{1,4,13\}$ for C_λ $(l = 5,6,$ $\lambda = 1,\ldots,4)$, where

$$b_{1,5,1} = 4, \quad b_{1,5,2} = 13, \quad b_{1,5,3} = 13, \quad b_{1,5,4} = 1;$$

$$b_{2,5,1} = 13, \quad b_{2,5,2} = 4, \quad b_{2,5,3} = 13, \quad b_{2,5,4} = 1;$$

$$b_{3,5,1} = 1, \quad b_{3,5,2} = 13, \quad b_{3,5,3} = 13, \quad b_{3,5,4} = 4;$$

$$b_{1,6,1} = 1, \quad b_{1,6,2} = 13, \quad b_{1,6,3} = 13, \quad b_{1,6,4} = 1;$$

$$b_{2,6,1} = 13, \quad b_{2,6,2} = 13, \quad b_{2,6,3} = 13, \quad b_{2,6,4} = 1;$$

$$b_{3,6,1} = 13, \quad b_{3,6,2} = 13, \quad b_{3,6,3} = 4, \quad b_{3,6,4} = 1.$$

And then each voter uses Chinese Remainder Theorem to solve the corresponding equations. Hence, $B_{1,5} = 1226697 \bmod \hat{p}$, $B_{2,5} = 799718 \bmod \hat{p}$, $B_{3,5} = 1986656 \bmod \hat{p}$, $B_{1,6} = 5780199 \bmod \hat{p}$, $B_{2,6} = 3148731 \bmod \hat{p}$, $B_{3,6} = 2868414 \bmod \hat{p}$, here $\hat{p} = \prod_{\lambda=1}^{4} p_\lambda = 4391633$. Then P_1 publishes $T_{1,5}, T_{1,6}$, P_2 publishes $T_{2,5}, T_{2,6}$, and P_3 publishes $T_{3,5}, T_{3,6}$, where $T_{i,l} = S_{i,l} + B_{i,l}$ for $i = 1, 2, 3$, $l = 5, 6$.

- Vote Counting:

  The cloud server collects the needed shares from voters in Γ_l $(l = 5, 6)$ and recovers blinding factors S_5 and S_6 by master secret algorithm. Then $B_5 = 4007071 \bmod \hat{p}$, $B_6 = 2203531 \bmod \hat{p}$, and solve equations

$$x_{l,\lambda} \cdot v_{yes} + y_{l,\lambda} \cdot v_{no} + z_{l,\lambda} \cdot v_0 \equiv B_l \pmod{p_\lambda}$$

  for l = 5,6, $\lambda = 1, \ldots, 4$, where $3^2 v_0 < 3v_{no} < v_{yes}$ and $x_{l,\lambda} + y_{l,\lambda} + z_{l,\lambda} = 3$.

  Take the vote counting for candidate C_1 as an example: Cloud computes

$$\hat{x}_{5,1} = 18, \quad x_{l,\lambda} = 1;$$
$$\hat{y}_{5,1} = 5, \quad y_{5,1} = 1;$$
$$\hat{z}_{5,1} = 1, \quad z_{l,\lambda} = 1.$$

  by the description in vote counting. That is, C_1 gets 2+1+0=3 points. And other results can be obtained by the same method. Then cloud broadcasts points 3, 5, 6, 1 for candidates C_1, C_2, C_3, C_4 related to Γ_5; and points 1, 6, 5, 0 for candidates C_1, C_2, C_3, C_4 related to Γ_6. It can be seen that C_3 and C_2 are winners for two roles, respectively.

*Author Biography & Photograph

Author Biography

Jing Li received the B.S. degree from Inner Mongol Normal University in 2010, the M.S. degree from Shananxi Normal University in 2013 and PhD degree in Beijing University of Posts and Telecommunications. Currently, she works at Guangzhou University. Her research interests include cloud computing, applied cryptography and privacy-preserving, etc.

Xianmin Wang received his BS degree from Suzhou University, Jiangsu, China, in 2006, and his MS degree in computer science from Jiangxi University of Science and Technology, Jiang Xi, China, in 2013. He received the PhD degree in computer science in 2017 from Beihang University. Currently, he is working in the institution of School of computer science in Guangzhou University. His research interests include deep learning, image processing and understanding.

Zhengan Huang received his B.S. and M.S. degrees from Department of Mathematics, Sun Yat-sen University in 2009 and 2011, respectively, and his Ph.D. degree from Department of Computer Science and Engineering, Shanghai Jiao Tong University in 2015. He served as a security engineer in Huawei Technologies Co. Ltd. from 2015 to 2016. Currently, he is a PostDoc in Guangzhou University. His research interests include public-key cryptography and information security.

**Licheng Wang** received the B.S. degree from Northwest Normal University in 1995, the M.S degree from Nanjing University in 2001 and the PhD degree from Shanghai Jiao Tong University in 2007. His current research interests include modern cryptography, network security, trust management, etc. He is an associate professor in Beijing University of Posts and Telecommunications.

**Yang Xiang** received the Ph.D. degree in computer science from Deakin University, Australia. He is currently a Dean at the Digital Research & Innovation Capability Platform, Swinburne University of Technology. He is the director of the Network Security and Computing Lab (NSCLab). His research interests include network and system security, distributed systems, and networking. He is the Chief Investigator of several projects funded by the Australian Research Council. He serves as an Associate Editor of the IEEE Transactions on Computers, the IEEE Transactions on Parallel and Distributed Systems, Security and Communication Networks, and the Editor of the Journal of Network and Computer Applications.