# Verifiable Secret Sharing Based On Micali-Rabin's Random Vector Representations Technique

Haiou Yang and Youliang Tian
*(Corresponding author: Youliang Tian)*

School of Computer Science and Technology, Guizhou University
Guizhou Province, Guiyang, China
(Email: youliangtian@163.com)

*(Received Mar. 24, 2019; Revised and Accepted Nov. 16, 2019; First Online Jan. 29, 2020)*

## Abstract

Verifiable secret sharing is the core basic protocol of many cryptographic systems, which is widely used in secure communication in network environment. By now, there are many researches on verifiable secret sharing for threshold structure, which lacks generality and flexibility compared with general access structure. However it is difficult to realize verifiable secret sharing scheme for general access structures. Existing generalized verifiable secret sharing schemes are few and have low efficiency. In this paper, we propose a new verifiable secret sharing scheme of general access structure. We use knowledge commitment scheme based on bilinear pairing to ensure the security and concealment of public information, and adopt the Micali-Rabin's random vector representations technique to improve the the efficiency of verification process. Our security and performance analysis shows that the new scheme is more efficient and practical compared to existing similar schemes.

*Keywords: Bilinear Pairing; General Access Structure; Micali-Rabin's Random Vector Representations Technique; Verifiable Secret Sharing*

## 1 Introduction

Secret sharing is the basic protocol for constructing cryptographic schemes such as secure multiparty computation and digital signature, which is mainly used for the distribution, preservation and reconstruction of secret and key (or other secret information), to prevent loss, damage or been tampered of information. The fundamental idea of secret sharing is that secret is divided into multiple parts by one dealer and shared among different participants, and some subsets of participants can be used to reconstruct the secret, while others cannot reconstruct it and get no information about secret. Shamir [10] and Blakley [2] first proposed the (t,n) threshold secret sharing scheme based on Lagrange interpolation polynomial and mapping geometry theory respectively. Asmuth [1] proposed the threshold secret sharing scheme based on Chinese Remainder Theorem (CRT). Halper and Teague [6] combined game theory with secret sharing and proposed the concept of rational secret sharing for the first time, that is, all participants are rational rather than honest or malicious. TIAN [12] analyzed the distribution mechanism and reconstruction mechanism of secret sharing under the framework of game theory, and studied the problem of one secret sharing based on Bayesian game, which solved the cooperation of this kind of rational secret sharing system. But none of these schemes can properly detect and prevent the malicious behavior of dealers and participants. To address possible dishonesty among participants, Chor *et al.* [3] proposed the concept of verifiable secret sharing (VSS) based on large integer factor decomposition problem for the first time. Stadler [11] improved the Chor's scheme, and proposed the Publicly Verifiable Secret Sharing schemes (PVSS) based on discrete logarithm. TIAN [13] constructed a non-interactive public verifiable secret sharing using bilinear pairs on elliptic curves, and its information rate reached 2/3. Jhanwar [4] proposed a PVSS scheme and provided a formal proof for the IND-secrecy of his scheme, based on the $(t, n)$-multi-sequence of exponents Diffie-Hellman assumption. After that, a lot of achievements have been made in the research on secret sharing schemes. However, almost all of the above schemes are designed for threshold structure, the threshold secret sharing is only a special case of generalized secret sharing.

Threshold structure lack flexibility and are not applicable in some specific scenario compared with general access structure. For instance, the dealer share secret among participants $U_1, U_2, U_3, U_4$ and specify the two subsets of participants $\{U_1, U_2\}, \{U_2, U_3, U_4\}$ can reconstruct the secret. So (t,n) threshold secret sharing scheme is no longer applicable under this circumstance. In order to study the

secret sharing of general access structures with wider applicability, Ito *et al.* [8] first proposed a secret sharing scheme based on general access structure, that is, the cooperation of participants with any authorized subset can reconstruct the secret. Harn *et al.* [7] applied integer programming to the generalized secret sharing scheme. They stipulate authorized subsets and non-authorized subsets to try to find a reasonable share allocation scheme so as to achieve the general access structure with the traditional (t,n) threshold scheme, but the scheme was expensive and has low efficiency in calculation. In the existing secret sharing scheme of general access structure, either the correctness of secret shares cannot be verified, or the computational overhead is increased to achieve the verifiability of secret shares.

Therefore, we propose an efficient generalized verifiable secret sharing scheme based on Micali-Rabin's random vector representations technique. In view of the complexity of verification process and the low probability of verifying the correctness of computing result, we adopt Micali-Rabins random vector representation technique, based on Zero-Knowledge Proof(ZKPs), proposed by Micali and Rabin [9]. Zero Knowledge Proofs, proposed by Golddwasser [5], are one of the most remarkable innovations in information security, which refers to the ability of a prover to convince a verifier that a statement is true without providing any useful information to the verifier, has been widely used in the field of information security. Rabin [9] developed a novel secure and highly efficient way for verifying correctness of the output of a transaction while keeping input values secret, based on the ZKPs. Xin [15] proposed a new fair and rational delegation computation. Aiming at the complexity of the verification problem, they adopted the Micali-Rabin's random vector representation technique. Consequently, ZKPs is used to prove the correctness of the computing results, which provides a new direction for our research.

In this paper, a new generalized verifiable secret sharing (GVSS) scheme is proposed. The contributions of our proposed GVSS are as follows: First, we proposed a GVSS scheme based on the difficulty of Diffie-Hellman problem of bilinear pairings. In this scheme, secret shares are chosen by the participants themselves, effectively avoiding deception by the dealer. Also, compared with threshold schemes, this scheme can specify any authorized subsets to reconstruct secret, which greatly increases the flexibility of secret sharing and expands the application scenarios of the schemes. Second, on account of the comlexity of verification phase, we adopt Micali-Rabin's random vector representation technique, that is, the secret shares are represented by knowledge commitment scheme for bilinear pairing. When needs to verify the correctness of secret shares, it only needs to execute an efficiently process according to the public information on the bulletin board.

The rest of this paper is organized as follows. In Section 2 we give the relevant backgrounds. Our proposed GVSS is described in Section 3. In Section 4, we give security analysis of our proposed GVSS and the comparison of performance between our proposed GVSS and the VSS proposed by ZHANG [16] and Tsu-Yang [14]. Conclusion is given in Section 5.

# 2 Preliminaries

## 2.1 Bilinear Pairing

Let $G_1$ and $G_2$ be additive cyclic groups and multiplicative cyclic groups of order $q$, where $q$ is a big prime number. Assuming that discrete logarithm problems on group $G_1$ and $G_2$ are difficult. A map: $e : G_1 \times G_1 \to G_2$ with the following properties is called a bilinear pairing:

1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Z_q^*$.

2) Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

3) Computable: For all $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q) = 1$.

## 2.2 Knowledge Commitment Scheme Based on Bilinear Pairing

Let $P, Q \in G_1$ be two generators of group $G_1$. Nobody knows the the discrete log of $P, Q$ (anybody does not know the $n \in Z_q^*$ such that $Q = nP$). When making commitment to $s \in Z_q^*$, we just have to compute the commitment $COM(s) = e(P, Q)^s$. When revealing the commitment, only s needs to be disclosed, and the verifier can verify whether the commitments revealed by dealer are correct according to $COM(s) = e(P, Q)^s$.

## 2.3 Micali-Rabin's Random Vector Representations

We adopt the knowledge commitment scheme based on bilinear pairing by Tian [**?**], the equality is proved by zero knowledge proofs. The properties of the bilinear pairing satisfy the above assumption, and $F_q$ is a finite field and $q$ is a large prime number of 128bits.

**Definition 1.** *A random vector representation of $x$ is a vector $X = (u, v)$, where $u, v \in Z_q^*$, $u$ was randomly chosen, and $v = (x - u) mod q$. The value of the vector $X$ is $val(X) = (u + v) mod q$.*

**Definition 2.** *Commitment to vector $X = (u, v)$ is $COM(X) = (COM(u), COM(v))$, where $COM(u) = e(P, Q)^u$, $COM(v) = e(P, Q)^v$.*

**Definition 3.** *A list of commitments $COM(X^{(j)}), 1 \leq j \leq m$ are called value consistent if $val(X^{(j)}) = val(X^{(j+1)})$ for any $1 \leq j \leq m$.*

When needs to prove $COM(X), COM(Y)$ value consistent, where $X = (u_1, v_1), Y = (u_2, v_2)$, we will prove $val(X) = val(Y)$. Note that $val(X) = val(Y)$ if and only

if there exists $w \in Z_q^*$ such that $X = Y + (w, -w)$(If such an $w$ does not exist, the value is inconsistent). The prover randomly chooses $c \leftarrow \{1, 2\}$. Assume that $c = 1$, the prover reveals to verifier $u_1, u_2, -w$. The verifier computes $COM(u_1), COM(u_2)$, and compares to the posted first coordinates of $COM(X), COM(Y)$. The verifier next checks that $u_1$=$u_2 - w$ is true. Vice versa, assume that $c = 2$, the prover reveals to verifier $v_1, v_2, w$. The verifier computes $COM(v_1), COM(v_2)$ and compares to the posted second coordinates of $COM(X), COM(Y)$. The verifier next checks that $v_1 = v_2 + w$ is true. Apparently, the prover accepts an false formula with a probability of $\frac{1}{2}$.

**Lemma 1.** ***If more than*** $k$ ***commitments are false, then the probability that the verifier accepts is*** $(\frac{1}{2})^k$.

*Proof.* The probability that any $val(X^{(j)}) \neq val(X^{(j+1)})$ is not found to be wrong is at most $\frac{1}{2}$. So the probability that at least $k$ formulas are not found wrong is $(\frac{1}{2})^k$ with a randomly chosen value $c \leftarrow \{1, 2\}$. □

# 3 Scheme

This scheme assumes that the Dealer $D$ needs to share the secret $s$ between $n$ participants. Also, the scheme assumes the existence of a secure bulletin board(SBB), which is used to publish data and cannot be deleted or modified as soon as it is published. At the same time, the published data is visible to dealer and all participants. The scheme includes Distribution Phase, Verification Phase and Secret Reconstruction.

Initialization: Assume that $F_q$ is a finite field and $q$ is a large prime number, $G_1$ and $G_2$ are respectively additive cyclic groups and multiplicative cyclic groups of order $q$, $P, Q \in G_1$ are two generators of group $G_1$. The properties of the bilinear pairing satisfy the above assumption, and there are efficient algorithms for mapping $e : G_1 \times G_1 \rightarrow G_2$ on groups $G_1$ and $G_2$. $H : G_2 \rightarrow Z_q^*$ is the anti-collision hash function.

The secret distributor specifies the authorized subset. Assume that the participants set is $P = \{P_1, P_2, \cdots, P_n\}$, $\Gamma_0 = \{\delta_1, \delta_2, \cdots, \delta_n\}$ is the minimum access structure, $\delta_j = \{P_{1j}, P_{2j}, \cdots, P_{|\delta_j|j}\}$ is the authorized subset, which $|\delta_j|$ is the number of members in $\delta_j$. The secret distributor is $SD$, the secret reconstructor is $SR$, the shared secret is $s$.

## 3.1 Distribution Phase

**Step 1.** Each participant $P_{ij}$ randomly chooses $s_{ij} \in Z_q^*$, and computes $R_{ij} = e(P, Q)^{s_{ij}}$. And keeps $s_{ij}$ secretly, delivers $R_{ij}$ to $SD$.

**Step 2.** $SD$ randomly selects $s_0$, and computes $R_0 = e(P, Q)^{s_0}$. Then, chooses $a \in Z_q^*$ randomly and construct a $1st$ degree polynomial $f(x) = (s + ax) mod q$. Simultaneously, chooses $t$ different random numbers $d_1, d_2, \cdots, d_t$ to represent these $t$ authorized subsets in $\Gamma_0$ respectively. In succession, $SD$ computes $f(1)$, and for each authorized subset $\delta_j = \{P_{1j}, P_{2j}, \cdots, P_{|\delta_j|j}\}$ in $\Gamma_0$ computes $H_j = f(d_j) \oplus H(R_{1j}{}^{s_0}) \oplus H(R_{2j}{}^{s_0}) \oplus \cdots \oplus H(R_{|\delta_j|j}{}^{s_0})$. Finally, publish $R_0, f(1), H_1, H_2, \cdots, H_t, d_1, d_2, \cdots, d_t$ on the SBB.

## 3.2 Verification Phase

All participants of any authorized subset $\delta_j$ can cooperate to reconstruct the secret s. Assume that the participants of $\delta_j = \{P_{1j}, P_{2j}, \cdots, P_{|\delta_j|j}\}$ reconstruct the secret $s$.

**Step 3.** Each participant $P_{ij}$ computes $R_{ij'} = R_0^{s_{ij}}$ based on the public information $R_0$ on the SBB. And each participant $P_{ij}$ posts on the SBB $3k$ rows of $R_{ij}{}'$: $COM(R_{1j'}^{(h)})$, $\cdots$, $COM(R_{|\delta_j|j'}^{(h)})$, $1 \leq h \leq 3k$. The $3k$ rows of SBB use the Micali-Rabin's random vector representations technique $COM(R_{1j'}^{(h)}) = (COM(u_{ij'}^{(h)}),\ COM(v_{ij'}^{(h)}))$, where $R_{1j'}^{(h)} = (u_{ij'}^{(h)}, v_{ij'}^{(h)})$, $val(R_{1j'}^{(h)}) = (u_{ij'}^{(h)} + v_{ij'}^{(h)}) \bmod q$, $1 \leq h \leq 3k$.

**Step 4.** To begin with, $P_{ij}$ randomly chooses half of the commitments from the $3k$ rows of $R_{ij'}$, $P_{ij}$ secretly reveals $R_{ij'}$ and commitment values $R_{1j'}^{(h)} = (u_{ij'}^{(h)}, v_{ij'}^{(h)})$ to $SR$.

Next, determines the value of $c \leftarrow \{1, 2\}$ by flipping a coin, opening a part of the remaining commitments value. Assume that $c = 1$, $P_{ij}$ secretly reveals the commitments $COM(u_{ij'}^{(h)}), COM(u_{ij'}^{(h+1)})$ and $-w$ to $SR$, where $w = (u_{ij'}^{(h+1)} - u_{ij'}^{(h)}) \bmod q$. Assume that $c = 2$, $P_{ij}$ secretly reveals the commitments $COM(v_{ij'}^{(h)}), com(v_{ij'}^{(h+1)})$ and $w$ to $SR$, where $w = (v_{ij'}^{(h+1)} - v_{ij'}^{(h)}) \bmod q$.

**Step 5.** At first, $SR$ privately received commitment values $R_{1j'}^{(h)} = (u_{ij'}^{(h)}, v_{ij'}^{(h)})$ and $R_{ij'}$ sent by $P_{ij}$. $SR$ first verify that the equation $val(R_{ij'}) = (u_{ij'}^{(h)} + v_{ij'}^{(h)}) \bmod q$ is correct.

Next, $SR$ performs a value consistent check on the remaining commitment values. Assume that received $c = 1$, $SR$ opens the commitment value $COM(u_{ij'}^{(h)}), COM(u_{ij'}^{(h+1)})$ and $-w$, then verifies that the equation $COM(u_{ij'}^{(h)}) = (COM(u_{ij'}^{(h+1)}) + (-w)) \bmod q$ is correct. If received $c = 2$, $SR$ opens the commitment value $COM(v_{ij'}^{(h)}), COM(v_{ij'}^{(h+1)})$ and $w$, then verifies that the equation $v_{ij'}^{(h)} = (u_{ij'}^{(h+1)} + w) \bmod q$ is correct. Apparently, only opened half of the commitment values at one time, from lemma 1, it can be seen that the probability of the participants accepting an false equation is $\frac{1}{2}$, if more than $k$ commitments are false, then the probability that the participants accept is $(\frac{1}{2})^k$.

### 3.3 Secret Reconstruction

**Step 6.** And then $SR$ received the verified $R_{ij'}$. With these values, $SR$ can compute $H_{j'} = H_j \oplus H(R_{1j'}) \oplus H(R_{2j'}) \oplus \cdots \oplus H(R_{|\delta_j|j'})$. With the two coordinate points $(1, f(1)), (d_j, H_{j'})$, $SR$ can reconstruct $f(x) = xf(1) - xH_{j'} - d_j f(1) + H_{j'}(1 - d_j)^{-1}$. At last, the shared secret can be recovered by computing $s = f(0) \bmod q$.

## 4 Scheme Analysis

### 4.1 Security Analysis

**Theorem 1.** ***If the $R_{ij'}$ received by the secret recuperator $SR$ are verified by the Micali-Rabin's random vector representations technique, then $R_{ij'}$ is the correct and has not been modified. Then this new scheme is verifiable.***

*Proof.* In the verification phase, by adopting the Micali-Rabin random vector representations technique, each participant $P_{ij}$ committed $3K$ rows: $COM(R_{1j'}^{(h)}), \cdots, COM(R_{|\delta_j|j'}^{(h)}), 1 \le h \le 3k$ to the $R_{ij'}$ on the SBB. In the verification phase, $SR$ verify half of the commitments $u_{ij'}^{(h)}, v_{ij'}^{(h)}$ and $R_{ij'}$ sent by $P_{ij}$(That is to verify that $val(R_{ij'}^{(h)}) = (u_{ij'}^{(h)} + v_{ij'}^{(h)})$modq is equal). If verification fails, $SR$ reject $R_{ij'}$ sent by the dealer. If it's verified, $SR$ performed a value consistent check on the remaining commitment values, that is verified $COM(u_{ij'}^{(h)}) = (COM(u_{ij'}^{(h+1)}) + (-w)) \bmod q$ or $v_{ij'}^{(h)} = (u_{ij'}^{(h+1)} + w) \bmod q$. According to Lemma 1, if more than $k$ commitment values are wrong, the probability of $SR$ accepting the wrong results is $(\frac{1}{2})^k$. To sum up, the $R_{ij'}$ verified by Micali-Rabin's random vector representations technique is the correct and has not been modified, this scheme is verifiable. □

**Theorem 2.** ***The knowledge commitment scheme based on bilinear pairing meets the requirements of complete hiding and computational binding.***

*Proof.* Assume that there exists $s' \in Z_q^*$ and $s' \neq s$ such that $COM(s') = COM(s)$(that is, the dealer can open the commitment in two ways). Assume that $s = s' + t, 0 < t < q$, that is $e(P,Q)^{s'} = e(P,Q)^s$. Because $P, Q \in G_1$ are two generators of group $G_1$, and $q$ is the big prime order on group $G_1$, so $qP = 0, qQ = 0$(0 is the point at infinity of the group $G_1$). We get $e(s'P, Q) = e(sP, Q)$ from $e(P,Q)^{s'} = e(P,Q)^s = e(sP,Q) = e(s'P,Q)$, so we have $sP = s'P$. So there exists $sP - s'P = tP = 0$ with $s = s' + t, 0 < t < q$. But, $0 < t < q$, this contradicts $P$ with order $q$, so it has to be $s = s'$, that is, the dealer only can open the commitment in one way. So the scheme meets the requirement of computational binding. □

Also $COM(s) = e(sP, Q) = e(P, sQ)$, it is not computationally feasible for an attacker to try to get the specifics of the commitment, since the calculation of Diffie-Hellman problem (CDHP) of bilinear pairings are hard to work out. In conclusion, the knowledge commitment scheme based on bilinear pairing meets the requirements of complete hiding and computational binding.

**Theorem 3.** ***It is assumed that the calculation of Diffie-Hellman problem (CDHP) of bilinear pairings are difficult to be solved, then the proposed scheme is of security.***

*Proof.* In the verification phase, the attackers try to get the $s_0$ and $s_{ij}$ from the commitments $R_0$ and the commitments of $3k$ rows $COM(R_{1j'}^{(h)}), \cdots, COM(R_{|\delta_j|j'}^{(h)}), 1 \le h \le 3k$ posted on the SBB, they have to solve $R_0 = e(P,Q)^{s_0}$, $COM(u_{ij'}^{(h)}) = e(P,Q)^{u_{ij'}^{(h)}}$ and $COM(v_{ij'}^{(h)}) = e(P,Q)^{v_{ij'}^{(h)}}$. However, the discrete logarithm problem(DLP) on the elliptic curve and the calculation of Diffie-Hellman problem (CDHP) of bilinear pairings are difficult to be solved. So it's not computationally feasible to get the specifics of the commitments. □

At the same time, the participant $P_{ij}$ tries to distribute false $R_{ij'}$ to $SR$ in the verification phase, that is $COM(R_{ij'}{}') = COM(R_{ij'})$, where $R_{ij'}{}' \neq R_{ij'}, R_{ij'}R_{ij'}{}' \in Z_q^*$. However, according to theorem 2, the knowledge commitment scheme based on bilinear pairing meets the requirement of computational binding, the dealer only can open the commitment in one way. So $P_{ij}$ cannot send a false $R_{ij'}$ to $SR$. Also, the secret shares $s_{ij}$ of each participant $P_{ij}$ in this scheme are chosen by the participants themselves, avoiding the distributor's deception.

### 4.2 Performance Analysis

This section briefly analyzes the performance of the proposed scheme by comparing it with the existing scheme. $T_e$ denotes the time of executing a bilinear pairing, $T_m$ denotes the time of executing a scalar of multiplication in $G_1$, $T_exp$ denotes the time of executing an exponentiation in $G_2$, $T_p$ denotes the time of computing the polynomial value. The time of executing a modular addition operation in $Z_q^*$ and one-way hash function are negligible compared with $T_e$ and $T_m$. Therefore, we just consider those time-consuming operations $T_e$, $T_m$, $T_exp$, $T_p$, other computational overhead is ignored.the computational efficiency as shown in Table 1.

The above mentioned, $|\delta_j|$ denotes the number of members in authorized subset, hence $|\delta_j| \ll n$. Therefore, performance analysis shows that in our scheme, with the adoption of Micali-Rabin's random vector representations technique, the verification process is much less computationally intensive. Compared with the above two schemes, the computational costs in the distribution phase has also been significantly improved.

Table 1: Comparison of computational costs

| Schemes | Distribution Phase | Verification Phase | Reconstruction Phase |
|---|---|---|---|
| *TIAN's scheme[8]* | $(3n+t)G_1$ | $tT_{\exp}+G_1+(t+1)T_e$ | $3tT_m+2tT_e$ |
| *ZHANG's scheme[14]* | $(n+1)T_m+2tT_{\exp}$ | $tT_e+n(t+1)T_{\exp}$ | $tT_m$ |
| *Tsu-Yang's scheme[15]* | $nT_e+(4n+t)T_m$ $+nT_{\exp}+nT_p$ | $(n+3)T_e+n(t+1)T_m$ $+nT_{\exp}+ntT_p$ | $tT_m$ |
| *TIAN's scheme[8]* | $(n+1)T_e+nT_{\exp}$ | $6k\lvert\delta_j\rvert T_e+\lvert\delta_j\rvert T_{\exp}$ | $T_m$ |

### 4.3 Simulation Analysis

For the generalized verifiable secret sharing based on Micali-Rabin's random vector representation technique proposed in this paper, simulation analysis was carried out in combination with the actual scenario. All data were the average of the experimental results for 10 times. The execution performance of the secret distribution process is shown in Figure 1. It can be seen that the execution time is linear with the change of the number of people. Because as the number of people increases, the number of operations of bilinear pairing and exponentiation increases. As can be seen from Figure 2, as the sub-secret is verified by Micali-Rabin's random vector representation technique in the verification phase, the calculation time of the secret verification process is less affected by the number of participants, and the calculation time of the secret reconstruction process does not change much with the number of people. In general, the scheme has good application value in practical application scenarios.

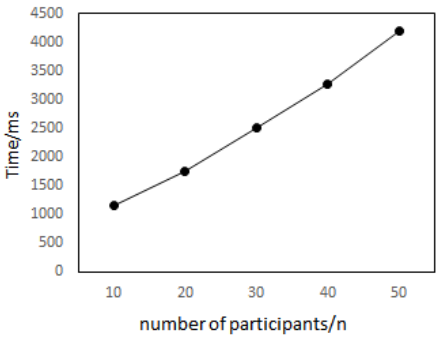


Figure 1: The curve of secret distribution calculations as the number of people changes

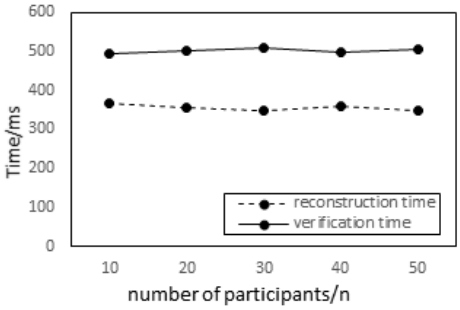


Figure 2: The curve of calculation costs as the number of people changes in the verification phase, and the curve of secret reconstruction calculations as the number of people changes

## 5 Conclusions

The (t,n) threshold secret sharing scheme has certain limitations in practical application, so it is of great application value to study the secret sharing of general access structure. This paper proposes a verifiable secret sharing scheme based on general access structure. Firstly, our scheme adopts the knowledge commitment scheme based on the bilinear pairing to guarantee the concealment and security of public information. Secondly, our scheme adopts Micali-Rabin's random vector representations technique, which greatly improves the efficiency of the verification phase. Finally, by analyzing the security and performance of the scheme, the scheme satisfies the feature of verifiable secret sharing and is more efficient than the existing schemes. The next work is to design a efficient secret sharing scheme with general access structure that can be publicly verified and applied to suitable application scenarios.

## Acknowledgments

This work is supported by Key Projects of the Union Fund of the National Natural Science Foundation of China under Grant No. U1836205; The National Natural Science Foundation of China under Grant No. 61772008; The Science and Technology Top-notch Talent Support Project in Guizhou Province Department of Education under Grant No.Qian Education Combined KY word [2016]060; The Guizhou Province Science and Technology Major Special Plan No. 30183001; The Guizhou Provincial Science and Technology Plan Project under Grant No. [2017]5788; The Ministry of Education-China Mobile Research Fund Project under Grant No. MCM20170401; The Guizhou University Fostering Project No. [2017]5788; Research on Block Data Fusion Analysis Theory and Security Management Model of Data Sharing Application (No. U1836205); Research on Key Technologies of Blockchain for Big Data Applications (Grant No. [2019]1098).

## References


[1] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208-210, 1983.

[2] G. R. Blakley, "Safeguarding cryptographic keys," *IEEE Computer Society Digital Library*, vol. 22, no. 11, pp. 612-613, 1979.

[3] B. Chor and S. Goldwasser and S. Micali and B. Awerbuch, " Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Foundations of Computer Science*, pp. 383-395, 1985.

[4] Y. Gan and L. Wang and P. Pan and Y. Yang, "Publicly verifiable secret sharing scheme with provable security against chosen secret attacks," *International Journal of Distributed Sensor Networks*, pp. 1-9, 2013.

[5] S. Goldwasser and S. Micali and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186-208, 1989.

[6] J. Halpern and V. Teague, "Rational secret sharing and multiparty computation: Extended abstract," *The 36th Acm Symposium on Theory of Computing*, pp. 623-632, 2004.

[7] L. Harn and C. Hsu and M. Zhang and T. He and M. Zhang, "Realizing secret sharing with general access structure," *Information Sciences*, vol. 367-368, pp. 209-220, 2016.

[8] M. Ito and A. Saito and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electronics and Communications in Japan Part Iii-fundamental Electronic Science*, vol. 72, no. 9, pp. 56-64, 1989.

[9] M. O. Rabin and Y. Mansour and S. Muthukrishnan and M. Yung, "Strictly-black-box zero-knowledge and efficient validation of financial transactions," in *International Colloquium Conference on Automata*, pp. 738-749, 2012.

[10] A. Shamir, "How to share a secret," *Communications of The ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[11] M. Stadler, "Publicly verifiable secret sharing," in *Theory and Application of Cryptographic Techniques*, pp. 190-199, 1996.

[12] Y. L. Tian and J. Katz J. F. Ma and C. G. Peng, "One-time rational secret sharing scheme based on Bayesiangame," *Wuhan University Journal of Nature Science*, vol. 16, pp. 430-434, 2011.

[13] Y. Tian and C. Peng, "publicly verifiable secret sharing schemes using bilinear pairings," *International Journal Network Security*, vol. 14, no. 3, pp. 142-148, 2012.

[14] T. Wu and Y. Tseng, "A pairing-based publicly verifiable secret sharing scheme," *Journal of Systems Science and Complexity*, vol. 24, no. 1, pp. 186-194, 2011.

[15] Y. Xin and M. O. Rabin, "Fair and rational delegation computation protocol," *Journal of Software*, vol. 29, no. 7, pp. 1953-1962, 2018.

[16] F. Zhang, "Efficient and information-theoretical secure verifiable secret sharing over bilinear groups," *Chinese Journal of Electronics*, vol. 23, no. 1, pp. 13-17, 2014.


## Biography

**Haiou Yang** biography. He received the B.Sc. degree in Information Management and System from Dalian Commuication University in 2017. He is now a postgraduate student at Guizhou University. His research interests include Security, Cloud computing and Cryptographic protocols.

**Youliang Tian** biography. He received the B.Sc. degree in Mathematics and Applied Mathematics in 2004 and the M.Sc. degree in Applied Mathematics from Guizhou University in 2009. He received the Ph.D. degree in cryptography from Xidian University in 2012. In the years 2012 to 2015, he was a Postdoctoral Associate at the State Key Laboratory for Chinese Academy of Sciences. He is currently a professor and Ph.D. supervisor at College Of Computer Science and Technology, GuiZhou University. His research interests include algorithm game theory, cryptography and security protocol.