Information Sciences 329 (2016) 524–539

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

# Attacks to some verifiable multi-secret sharing schemes and two improved schemes

Yanhong Liu [a,c], Futai Zhang [a,b,*], Jie Zhang [a]

[a] School of Computer Science and Technology, Nanjing Normal University, Nanjing, China
[b] Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, Nanjing, China
[c] Heilongjiang Research Center for Labor Safety Science and Technology, Harbin, China

ARTICLE INFO

*Article history:*
Received 14 December 2011
Revised 1 December 2014
Accepted 16 September 2015
Available online 1 October 2015

*Keywords:*
Secret sharing
Verifiable multi-secret sharing scheme
Private channel
Shadow
RSA cryptosystem

ABSTRACT

Secret sharing plays an important role in protecting confidential information from being lost, destroyed, or falling into wrong hands. Verifiable multi-secret sharing enables a dealer to share multiple secrets among a group of participants such that the deceptive behaviors of the dealer and the participants can be detected. In this paper, we analyze the security of several recently proposed verifiable multi-secret sharing schemes. We show that these schemes cannot withstand some deceptive behaviors of the dealer, and hence fails to satisfy the basic requirement of secure verifiable secret sharing schemes. After that, we present two improved verifiable multi-secret sharing schemes. Our new schemes can not only resist cheating by the dealer or participants, but also remove the use of private channels.



## 1. Introduction

Secret sharing plays an important role in protecting important information from getting lost, destroyed, or falling into wrong hands. It has many practical applications, such as safeguarding very confidential information, opening a bank vault, launching a missile, etc. In 1979, the first $(t, n)$ threshold secret sharing schemes were proposed by Shamir [29] and Blakley [2] independently. In a $(t, n)$ threshold secret sharing scheme, a secret can be shared among $n$ participants such that $t$ or more participants can reconstruct the secret, but $t-1$ or fewer participants can not. In real applications, it is known that traditional secret sharing schemes like Shamir's and Blakley's cannot solve the following problems:

(1) Only one secret can be shared during one secret sharing process, they cannot be used to share multiple secrets simultaneously.
(2) The shadows of participants are not reusable. Once the secret has been reconstructed, all shadows will no longer be private.
(3) Deceptive behaviors of a dishonest dealer cannot be detected. A dishonest dealer may distribute a fake shadow to a certain participant, and then that participant would subsequently never obtain the true secret.
(4) Deceptive behaviors of a malicious participant cannot be prevented in the process of reconstruction. A malicious participant may provided a fake shadow to cheat the other participants to prevent them from reconstructing the true secret.
(5) Private channels are required for the communications between the dealer and participants.
(6) The dealer knows all shadows of participants. The shadows of participants are not reusable for different dealers.

* Corresponding author. Tel.: +86 25 85891990; fax: +86 13813945429.
*E-mail addresses:* angelpray@126.com (Y. Liu), ffttzhang@sina.com, zhangfutai@njnu.edu.cn (F. Zhang), 464516929@qq.com (J. Zhang).

http://dx.doi.org/10.1016/j.ins.2015.09.040
0020-0255/

To solve some of the above problems, the concepts of multi-secret sharing (MSS) [15,16] and verifiable secret sharing (VSS) [6] have been introduced. A number of multi-secret sharing schemes and verifiable secret sharing schemes [5,7–9,23,33,35] have been presented. Using multi-secret sharing schemes [4,13,22], the drawback in (1) can be removed. To deal with the drawback in (2), Jackson et al. [20] have further introduced multi-use secret sharing schemes. The difference is that the shadow kept by each participant in a multi-use scheme is reusable after secret reconstruction.

To overcome the problems both in (1) and (2), He and Dawson [15] proposed a MSS scheme. One year later, they [16] put forward a dynamic MSS scheme based on two-variable one-way function. Two other practical MSS schemes were presented by Chien et al. [5] in 2000 and Yang et al. [33] in 2004 respectively. Pang and Wang [23] pointed out although the reconstruction in Yang's scheme is easier than in Chien's scheme, more public values are required when $p < t$. They also demonstrated an improved scheme based on interpolation method. However, Li et al. [21] pointed out Pang el al.'s scheme needs to generate a polynomial of degree ($n$+$p$-1) in both the secret distribution and the secret reconstruction. And hence the efficiency is unfavorable when $p$ is very large. They presented a new $(t, n)$ threshold multi-secret sharing scheme using interpolation method. Some vulnerabilities of MSS schemes using polynomial interpolation were shown by Sahasranand et al. in [28]. They pointed out that a scheme based on interpolation method cannot be used to implement a $(k, t, n)$ scheme when the $k$ secrets to be distributed are inherently generated from a polynomial of degree less than $k-1$, and the scheme does not work if all of the secrets to be shared are the same, etc. Although the drawbacks in (1) and (2) may be eliminated in these MSS schemes, the problems in (3)–(6) still exist.

To do away with the drawback in (3), Chor et al. [6] have initiated the study of verifiable secret sharing (VSS). In a VSS scheme, participants are able to verify that their shadows are consistent, and cheating by a dishonest dealer can be detected. VSS is now a fundamental tool in cryptographic research [14]. In order to resolve the problem in (4), cheating immune secret sharing [24–26,34] and publicly verifiable secret sharing (PVSS) [31] were investigated. The PVSS scheme presented by Stadler can detect not only cheating by the dealer but also the cheating by any participants.

Taking the problems in (1)–(4) into consideration, Harn [13] has introduced a $(t, n)$ threshold verifiable multi-secret sharing (VMSS) scheme which can detect both malicious dealer and dishonest participants. In Harn's scheme, every participant keeps only one reusable shadow for sharing any set of secrets. However, Lin and Wu [22] pointed out that Harn's scheme suffered from the problems of large amount $(n!/((n-t)!\cdot t!))$ of modular exponentiations and running interactive verification protocol to verify the validity of shadows. Chen et al. [4] presented an alternative $(t, n)$ VSS scheme to avoid the disadvantages in Harn's scheme. However, Lin and Wu [22] showed that Chen et al.'s scheme is inefficient because the dealer has to record all participants' shadows and take $2n$ modular exponentiations to compute an $n$-dimensional verification vector for each shared secret. Lin and Wu put forward a $(t, n)$ threshold VMSS scheme (LW scheme) based on the intractability of factorization and the hardness of the discrete logarithm problem modulo a composite [22]. In [17], He and Wu have indicated that LW scheme can't resist cheating by participants, because a malicious participant can provide a fake subshadow to cheat other honest participants. An improvement of the LW scheme was given by Chang et al. [3]. The improved scheme not only successfully overcomes the drawbacks of LW scheme, but also is computationally more efficient than the other VMSS schemes. Unfortunately, Huang et al. [18] identified that Chang's VMSS scheme could not withstand conspiracy attack. They showed that any $t+1$ participants can conspire to compute the system's secret $\mathbf{R}$ or $\phi(N)$ with high probability. Subsequently, these malicious participants could reconstruct the shared secret independently.

In 2004, Yang et al. [33] proposed a relatively efficient multi-secret sharing scheme (YCH scheme). But Shao and Cao pointed out that this scheme does not enjoy the property of verifiability, and presented a modified scheme (SC scheme) [30] by adding the property of verifiability based on Feldman's [12] VSS scheme. Note that, in the SC scheme, all shadows are computed by the dealer and private channels are required for the dealer to distribute shadows to participants. So the problems in (5) and (6) remain unsolved. In 2006, Zhao et al. [35] introduced a practical verifiable multi-secret sharing scheme (ZZZ scheme) based on YCH scheme and Hwang–Chang's scheme (HC scheme) [19]. The verification phase of the ZZZ scheme is the same as that of the HC scheme. By making use of the techniques of public key cryptography [32], e.g. RSA cryptosystem [27] and Diffie–Hellman key agreement [10] method, the ZZZ scheme and HC scheme realized secret sharing without private channels. This property is particularly significant in applications where private channels are hard to set up. In these schemes, each participant chooses his secret shadow by himself. Hence the problems in (5) and (6) could be solved simultaneously. Similar to ZZZ scheme, the VMS schemes presented in [8,9] were also dealt with the problems in (5) and (6). For simplicity, we call the scheme in [8] MS scheme, the type 1 scheme in [9] the MS1 scheme, the type 2 scheme in [9] the MS2 scheme.

Although it was claimed that these schemes (ZZZ scheme, MS scheme, MS1 scheme, MS2 scheme) could identify cheating by both the dealer and the participants, unfortunately, we find that their claims are wrong.

In this paper, we analyze the security drawbacks of these verifiable multi-secret sharing schemes, including the ZZZ scheme, MS scheme, MS1 scheme, MS2 scheme. We demonstrate how a dishonest dealer can cheat a participant without being detected in all these schemes. So these schemes cannot withstand cheating by dishonest dealer.

In addition, taking into account all the problems (1) to (6) , we also propose two new verifiable multi-secret sharing schemes. Our new schemes have the following features:

(1) The dealer can arbitrarily give any set of secrets for sharing, and only one shadow, which is reusable, should be kept by each participant. This solves the problems in (1) and (2).
(2) Every participant can detect any cheating by the dealer. This solves the problem in (3).
(3) Every participant can detect the cheating by any other participants by using a non-interactive protocol. This solves the problem in (4).

(4) The dealer and the participants communicate through public channel. This solves the problem in (5).
(5) The dealer does not know each participant's shadow. The shadows of participants can be reusable for the different round of sharing. This solves the problem in (6).

With these features, our new schemes can be applied in many practical situations, such as authenticating an electronic funds transfer.

The rest of the paper is organized as follows. In Section 2 we revisit the concepts of RSA encryption scheme and homogeneous linear recursion (HLR) which will be building blocks in constructing our new VMSS schemes. Then we describe the security model for VMSS schemes. The security analysis and attacks on several verifiable multi-secret sharing schemes are shown in Section 3. Our new verifiable multi-secrets sharing scheme without a private channel is depicted in Section 4 followed by security analysis. In Section 5 we give performance analysis of our new VMSS schemes. Finally, Section 6 concludes our paper.

## 2. Preliminaries

### 2.1. RSA encryption scheme

RSA is one of the best known public-key encryption schemes named after its inventors Rivest, Shamir and Adleman [27]. It is is the first practical realization of public-key encryption scheme based on the notion of one-way trapdoor function introduced by Diffie and Hellman [10,11]. The security of RSA is based on the hardness of large integer factorization.

The RSA encryption scheme is specified as follows:

**Key setup:** A user Alice performs the following steps to generate her public and private keys.

1. choose two random prime numbers $p$ and $q$ such that $|p| \approx |q|$;
2. compute $N = pq$;
3. compute $\phi(N) = (p-1)(q-1)$;
4. choose a random integer $e < \phi(N)$ such that $\gcd(e, \phi(N)) = 1$, and compute the integer $d$ such that
$$ed \equiv 1 (\mathrm{mod}\ \ \phi(N));$$
5. publish $(N, e)$ as her public key, safely destroy $p$, $q$ and $\phi(N)$, and keep $d$ as her private key.

**Encryption:** To send a confidential message $m \in Z_N$ to Alice, the sender Bob creates the ciphertext $c$ as follows
$$c \leftarrow m^e (\mathrm{mod}\ \ N).$$

**Decryption:** To decrypt a ciphertext $c$, Alice computes
$$m \leftarrow c^d (\mathrm{mod}\ \ N).$$

### 2.2. Homogeneous linear recursion (HLR)

In this section we briefly introduce homogeneous linear recursion which forms the mathematical background of our second scheme. A detailed description of homogeneous linear recursion can be found in [1].

**Definition 1.** Let $t$ be a positive integer and $c_1, c_2, \ldots, c_t, a_1, a_2, \ldots, a_t$ be real numbers. A homogeneous linear recursion of degree $t$ is defined by the equations
$$[HLR]\begin{cases} u_0 = c_1, u_1 = c_2, \ldots, u_{t-1} = c_t, \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0 \quad (i \geq 0) \end{cases}$$
where $c_1, c_2, \ldots, c_t$ and $a_1, a_2, \ldots, a_t$ are constants.

**Definition 2.** We define the auxiliary equation for [HLR] to be
$$x^t + a_1 x^{t-1} + \cdots + a_t = 0.$$

We shall assume that the auxiliary equation has $t$ roots, which will certainly be the case if we work in the field $\mathbb{C}$ of complex numbers. However, the $t$ roots do not need to be distinct, and we shall suppose that the distinct values are $\alpha_1, \alpha_2, \ldots, \alpha_l$, occurring with multiplicities $m_1, m_2, \ldots, m_l$, respectively. In other words, the auxiliary equation can be rewritten as
$$(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\ldots(x-\alpha_l)^{m_l} = 0,$$
where $m_1 + m_2 + \cdots + m_l = t$.

**Lemma 1.** *Suppose sequence $\{u_i\}$ is defined by [HLR], and the auxiliary equation has roots $\alpha_1, \alpha_2, \ldots, \alpha_l$ with multiplicities $m_1, m_2, \ldots, m_l$. Then*
$$u_i = p_1(i)\alpha_1^i + p_2(i)\alpha_2^i + \cdots + p_l(i)\alpha_l^i,$$
*where, for $j = 1, 2, \ldots, l$, $p_j(i)$ is an expression of the form $A_0 + A_1 i + \cdots + A_{(m_j-1)} i^{(m_j-1)}$. In other words, $p_j(i)$ is a polynomial function of $i$ with degree at most $m_j - 1$.*

### 2.3. Security model of VMSS schemes

A $(t, n)$ VMSS scheme without private channels involves a dealer $D$ and a set $M = \{M_1, M_2, \ldots, M_n\}$ of $n$ participants. It is composed of the following 4 phases.

1. *Initialization*: The dealer sets up the system parameters which may include its private information and some public data authentically available to all participants. All participants choose their secret shadows and compute the corresponding public information respectively. Then each participant authenticates its identity and public information to the dealer. After that the dealer publishes the public parameters, the identities and public information of all participants.
2. *Construction*: For a set of secrets to be shared, the dealer $D$ computes subshadows and corresponding verification information for all participants. $D$ authentically publishes all verification information.
3. *Verification*: Each participant gets its subshadow from verification information. Then it checks the validity of its subshadow using the public information.
4. *Recovery*: $t$ or more participants cooperate to recover the shared secrets. Each of them supplies its subshadow to the others. They verify the validity of each subshadow. When at least $t$ valid subshadows are collected, they can compute all shared secrets using a predetermined algorithm.

With regard to the security, a $(t, n)$ VMSS scheme without private channels must satisfy the following requirements.

1. *Correctness*: If the dealer and the participants act honestly, any $t$ or more participants can reconstruct the secret correctly during the execution of the reconstruction algorithm.
2. *Verifiability*:
   - Any deceptive behavior of the dealer can be identified in the verification phase.
   - In the recovery phase, a dishonest participant who supplies a fake subshadow can be identified by the others.
3. *Privacy*: Any collusion of less than $t$ participants cannot obtain any of the shared secrets.

According to these security requirements, in the security model of VMSS schemes, we characterize three types of adversaries. One is a dishonest dealer who aims to cheat some participants by distributing to them invalid subshadows. We say a dishonest dealer succeeds if it distributes an invalid subshadow to a participant without being detected with a non-negligible probability. The second is a cheating participant who aims to submit a fake subshadow without being detected in the recovery phase. Such an adversary succeeds if it submits a fake subshadow without being detected with a non-negligible probability. Another is an adversary who is not the dealer but corrupts up to $t-1$ participants. An adversary of this kind gets complete control of up to $t-1$ corrupted participants and aims to extract some information of the shared secrets. We say such an adversary succeeds if it can get some information of the shared secrets other than those can be induced from public information and the information owned by the corrupted participants with a non-negligible probability.

**Definition 3.** A a $(t, n)$ VMSS scheme without private channels is said secure if it satisfies *Correctness* and no adversary can succeed with a non-negligible probability.

## 3. Security analysis and attacks to several verifiable multi-secret sharing schemes

### 3.1. Security analysis and attack on ZZZ scheme [35]

#### 3.1.1. Brief review of ZZZ scheme

- **Initialization phase**
  Let $P_1, P_2, \ldots, P_k$ denote $k$ secrets to be shared. Firstly, the dealer $D$ chooses two large strong primes, $p$ and $q$, computes $N = pq$. $D$ randomly chooses an integer $g$ from the interval $[N^{1/2}, N]$ such that $g$ is relatively prime to $p$ and $q$. $D$ publishes $\{g, N\}$.
  Let $M = \{M_1, M_2, \ldots, M_n\}$ be the set of participants. Each participant $M_i$ in $M$ randomly chooses an integer $s_i$ from the interval $[2, N]$ as her/his own secret shadow and computes $R_i = g^{s_i} \bmod N$, then $M_i$ provides $R_i$ and her/his identity information $ID_i$, to the dealer $D$. $D$ must ensure that $R_i \neq R_j$ for all $i \neq j$. Once $R_i = R_j$, $D$ should demand these participants to choose different secret shadows until $R_i's$ are different for $i = 1, 2, \ldots, n$. $D$ publishes $\{(ID_i, R_i)\}$.
- **Construction phase**
  The dealer $D$ performs the following steps
  (1) Randomly choose an integer $s_0$ from the interval $[2, N]$ such that $s_0$ is relatively prime to $(p-1)$ and $(q-1)$. Then $D$ computes $f$ such that $s_0 \times f = 1 \bmod \phi(N)$, where $\phi(N)$ is the Euler phi-function;
  (2) Compute $R_0 = g^{s_0} \bmod N$ and $I_i = R_i^{s_0} \bmod N$, $(i = 1, 2, \ldots, n)$;
  (3) Publish $\{R_0, f\}$.
  In case $k \leq t$,
  - Choose a prime $Q$ and construct $(t-1)$th degree polynomial $h(x) \bmod Q$,

$$h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q,$$

    where $0 < P_1, P_2, , P_k, a_1, a_2, \ldots, a_{t-k} < Q$;
  - Compute $y_i = h(I_i) \bmod Q$ for $i = 1, 2, \ldots, n$;

– Publish $(y_1, y_2, \ldots, y_n)$.

In case $k > t$,

– Choose a prime $Q$ and construct $(k-1)$th degree polynomial $h(x) \bmod Q$,

$$h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} \bmod Q,$$

where $0 < N, P_1, P_2, \ldots, P_k < Q$;

– Compute $y_i = h(I_i) \bmod Q$ for $i = 1, 2, \ldots, n$;

– Compute $h(i) \bmod Q$ for $i = 1, 2, \ldots, k-t$;

– Publish $\left(y_1, y_2, \ldots, y_n, h(1), h(2), \ldots, h(k-t)\right)$.

- **Recovery and verification phase**

Without loss of generality, suppose $t$ or more members $M_1, M_2, \ldots, M_t$ of $M$ collaboratively recover the secrets $P_1, P_2, \ldots, P_k$, they execute the following steps:

(1) $M_i$ supplies $I_i^{'} = R_0^{s_i} \bmod N$, where $s_i$ is the shadow of $M_i$;

(2) Anybody can verify the validity of $I_i^{'}$ provided by $M_i$: if $I_i^{'f} = R_i \bmod N$, then $I_i^{'}$ is true; otherwise $I_i^{'}$ is false and $M_i$ may be a cheater;

(3) Recover the secrets: The polynomial $h(x) \bmod Q$ can be uniquely determined as follows:

$k \le t$

$$\begin{aligned} h(x) &= \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - I_j^{'}}{I_i^{'} - I_j^{'}} \bmod Q \\ &= P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q. \end{aligned}$$

$k > t$

$$\begin{aligned} h(x) &= \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - I_j}{I_i - I_j} \prod_{l=1}^{k-t} \frac{x - l}{I_i - l} + \sum_{i=1}^{k-t} h(i) \prod_{j=1, j\neq i}^{k-t} \frac{x - j}{i - j} \prod_{l=1}^{t} \frac{x - I_l}{i - I_l} \bmod Q \\ &= P_1 + P_2 x^1 + \cdots + P_k x^{k-1} \bmod Q. \end{aligned}$$

*3.1.2. Analysis and attack to ZZZ scheme*

We notice that, when collaboratively reconstruct the shared secrets, only the validity of $I_i$ provided by each $M_i$ is checked using equation $I_i^f = R_i \bmod N$. But the consistence of $I_i$ with $y_i$ is not verified. Based on this observation, a dishonest dealer $D$ can cheat $M_i$ by using an invalid $y_i$ which is inconsistent with $I_i = R_i^{s_0} \bmod N$. The attack comes as follows:

In the **Construction phase**, the dishonest dealer $D$ performs:

In case $k \le t$

- $D$ chooses a prime $Q$ and construct $(t-1)$th degree polynomial $h(x) \bmod Q$,

$$h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q$$

where $0 < P_1, P_2, \ldots, P_k, a_1, a_2, \ldots, a_{t-k} < Q$;

- Assume $D$ wants to cheat participant $M_i$, he/she first randomly chooses $J_i \neq I_i$ and computes $y_i^{'} = h(J_i) \bmod Q$, correctly computes the other $y_j$ for $j = 1, 2, \ldots, n, j \neq i$;
- $D$ publishes $(y_1, y_2, \ldots, y_{i-1}, y_i^{'}, y_{i+1}, \ldots, y_n)$.

In case $k > t$

- $D$ chooses a prime $Q$ and construct $(t-1)$th degree polynomial $h(x) \bmod Q$,

$$h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q,$$

where $0 < P_1, P_2, \ldots, P_k, a_1, a_2, \ldots, a_{t-k} < Q$;

- Assume $D$ wants to cheat participant $M_i$, he/she first randomly chooses $J_i (J_i \neq I_i)$ and computes $y_i^{'} = h(J_i) \bmod Q$, correctly computes the other $y_j$ for $j = 1, 2, \ldots, n, j \neq i$;
- $D$ publishes $\left(y_1, y_2, \ldots, y_i^{'}, \ldots, y_n, h(1), h(2), \ldots, h(k-t)\right)$.

In the **Recovery and verification phase**, the honest $M_i$ will supply $I_i^{'} = R_0^{s_i} \bmod N$ which is really valid, since it does hold that $I_i^{'f} = R_i \bmod N$. As any participant can by no means find out $y_i^{'}$ is inconsistent with $I_i^{'} = R_0^{s_i} \bmod N$, i.e. $y_i^{'} \neq h(I_i)$, in the reconstruction phase, $M_i$ and his collaborators will use the fake $y_i^{'}$. As a result they will not recover the true secrets. In addition, when this happens, it is hard for the collaborators to identify which $y_i$ is fake.

**[Note]:** Obviously, such attacks can also be extended to MS scheme [8].

### 3.2. Security analysis and attacks to MS1 and MS2 schemes [9]

#### 3.2.1. Analysis and attack to MS1 scheme

For space limitation, we omit the description of the original MS1 scheme. Please refer to [9] for details. The security drawbacks of the MS1 scheme is similar to that of the ZZZ scheme. We notice that, when collaboratively reconstruct the shared secrets, only the validity of $I_i = f(r, s_i)$ provided by each $M_i$ is checked using equation $g^{I_i} = G_i \bmod p$. While the consistence of $I_i$ with the [∗MS1] homogeneous linear recursive formula is not verified. Based on this observation, in the generation of sequence $\{u_i\}$, a dishonest dealer $D$ can cheat $M_i$ by replacing the valid $I_i = f(r, s_i)$ with an invalid $I_i' = f(r, s_i')$, where $s_i' \neq s_i$. And any participants are not able to detect. The attack comes as follows:

$D$ randomly chooses $J_i (J_i \neq s_i)$ and computes:

$$\begin{cases} I_i' = f(r, J_i); \\ I_i = f(r, s_i); \\ G_i = g^{J_i} \bmod p. \end{cases}$$

If $1 \leq i \leq t$

- $D$ replaces the $I_i$ with the $I_i'$ to calculate the following [HLR] equations:

$$[*]\begin{cases} u_0 = I_1, u_1 = I_2, \ldots, u_{i-1}' = I_i', \ldots, u_{t-1} = I_t, \\ u_{j+t} + a_1 u_{j+t-1} + \cdots + a_t u_j = 0 \bmod q \quad (j \geq 0) \end{cases}$$

- $D$ computes $u_j$ for $t \leq j \leq n + k$;
- $D$ computes $y_j = I_j - u_{j-1}$ for $t < j \leq n$ and $r_j = P_j - u_{j+n}$ for $1 \leq j \leq k$;
- $D$ publishes $(r, G_1, G_2, \ldots, G_i, \ldots, G_n, r_1, r_2, \ldots, r_k, y_{t+1}, y_{t+2}, \ldots, y_n)$.

If $t < i \leq n$

- $D$ considers [HLR](Homogeneous linear recursion) which is defined by the equations

$$[*]\begin{cases} u_0 = I_1, u_1 = I_2, \ldots, u_{t-1} = I_t, \\ u_{j+t} + a_1 u_{j+t-1} + \cdots + a_t u_j = 0 \bmod q \quad (j \geq 0) \end{cases}$$

- $D$ computes $u_j, t \leq j \leq n + k$;
- $D$ replaces the $I_i$ with the $I_i'$ to compute $y_i' = I_i' - u_{i-1}$, correctly computes the other $y_j$ for $t < j \leq n, j \neq i$ and $r_j = P_j - u_{j+n}$ for $1 \leq j \leq k$.
- $D$ publishes $(r, G_1, G_2, \ldots, G_i, \ldots, G_n, r_1, r_2, \ldots, r_k, y_{t+1}, y_{t+2}, \ldots, y_i', \ldots, y_n)$.

Since $M_i$ cannot find out $I_i = f(r, s_i)$ is replaced with an invalid $I_i' = f(r, s_i')$ by $D$, in the reconstruction phase, he and his collaborators will use the subshadow $I_i = f(r, s_i)$ to recover the secrets. As a result they will fail to recover the true secrets. (Note that any $t$ or more honest participants without $M_i$ can recover the true secrets.) In addition, when this happens, it is hard for the collaborators to identify which $I_i = f(r, s_i)$ is replaced by $D$. This fact indicates that the MS1 scheme cannot withstand cheating by the dealer.

#### 3.2.2. Analysis and attack to MS2 scheme

For the complete description of the MS2 scheme, please refer to [9]. We notice that, when collaboratively reconstruct the shared secrets, only the validity of $I_i = R_0^{s_i} \bmod N$ provided by each $M_i$ is checked using equation $(I_i)^f = R_i \bmod N$, while the consistence of $I_i$ with the sequence $\{u_i\}$ generated from Homogeneous linear recursive formula [∗MS2] is not verified. Based on this observation, a dishonest dealer $D$ can cheat $M_i$ by replacing the valid $I_i = R_i^{s_0}$ with an invalid $I_i' = (J_i)^{s_0}$ $(J_i \neq R_i)$ in generating the sequence $\{u_i\}$ or $\{y_i\}$. The attack comes as follows:

$D$ randomly chooses $J_i (J_i \neq R_i)$ and computes:

$$\begin{cases} I_i' = (J_i)^{s_0} \bmod N; \\ I_i = (R_i)^{s_0} \bmod N. \end{cases}$$

If $1 \leq i \leq t$

- $D$ replaces the $I_i$ with the $I_i'$ to compute the following [HLR] equations:

$$[*]\begin{cases} u_0 = I_1, u_1 = I_2, \ldots, u_{i-1}' = I_i', \ldots, u_{t-1} = I_t, \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0 \bmod q \ (i \geq 0) \end{cases}$$

- $D$ computes $u_i$ for $t \leq i \leq n + k$;
- $D$ computes $y_i = I_i - u_{i-1}$ for $t < i \leq n$ and $r_i = P_i - u_{i+n}$ for $1 \leq i \leq k$;
- $D$ publishes $(R_0, f, r_1, r_2, \ldots, r_k, y_{t+1}, y_{t+2}, \ldots, y_n)$.

If $t < i \le n$

- $D$ considers the sequence $\{u_i\}$ which is defined by the formulas:

$$[*]\begin{cases} u_0 = I_1, u_1 = I_2, \ldots, u_{t-1} = I_t, \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0 \bmod q \ (i \ge 0) \end{cases}$$

- $D$ computes $u_i$ for $t \le i \le n + k$;
- $D$ replaces the $I_i$ with the $I_i'$ to compute $y_i' = I_i' - u_{i-1}$, correctly computes the other $y_j$ for $t < j \le n, j \ne i$ and $r_i = P_i - u_{i+n}$ for $1 \le i \le k$;
- $D$ publishes $(R_0, f, r_1, r_2, \ldots, r_k, y_{t+1}, y_{t+2}, \ldots, y_i', \ldots, y_n)$.

Since $M_i$ cannot find out $I_i = R_i^{S_0}$ is replaced by $D$ in the generation of sequence $\{u_i\}$ or $\{y_i\}$, in recovery phase, he and his collaborators will use the true $I_i$ that is inconsistent with sequence $\{u_i\}$ or $\{y_i\}$. As a result they will not recover the true secrets. (But any $t$ or more honest participants without $M_i$ can recover the true secrets.) In addition, when this kind of cheating occurs, it is hard for the collaborators to identify which $I_i = R_i^{S_0}$ is replaced by $D$. This fact indicates that the MS2 scheme also cannot withstand cheating by the dealer.

## 4. New VMSS schemes

To overcome the security drawbacks of the above analyzed VMSS schemes, we propose two new VMSS schemes in this section. By adding some consistence checking measures, our new schemes effectively get rid of the security flaws in ZZZ scheme, MS scheme, MS1 scheme, and MS2 scheme. Our first scheme is based on the ZZZ scheme introduced in [35] and Feldman's VSS scheme [12], and the second is based on the MS2 scheme [9]. The two new schemes can not only resist cheating by the dealer or participants, but also remove the use of private channels.

### 4.1. Description of our scheme 1

Let $D$ be the dealer, $M = \{M_1, M_2, \ldots, M_n\}$ be the set of participants, $t(< n)$ be the threshold.

- **Initialization phase**

In this phase, the dealer (denoted as $D$ ) first creates a public notice board (NB) which is used for storing necessary public information. The participants can access the information on NB. But the contents on the board can only be modified or updated by $D$. Let $\lambda$ be the security parameter. For our context, it should be chosen as the security parameter for a secure RSA cryptosystem.

Initialization of the dealer $D$, $D$ performs the following:

(1) Choose two large strong primes $p_0$ and $q_0$ $(p_0 > q_0)$ with bit-length $\lambda/2$ satisfying the requirement of a secure RSA public key cryptosystem [32], and compute $N = p_0 q_0$ of bit-length $\lambda$.
(2) Compute $\phi(N) = (p_0 - 1)(q_0 - 1)$ which is Euler's function, then safely destroy $p_0$, $q_0$.
(3) Choose primes $q$, $Q$ such that $Q|(q-1)$, and the bit-length of $Q$ is at least $\lambda/2$. Then randomly choose an element $g$ of $Z_q^*$ with order $Q$.
(4) $D$ publishes $(\lambda, N, Q, q, g)$ on NB.

Initialization of participants:

(1) Each $M_i$ with identity information $ID_i$ chooses two strong primes $p_i$ and $q_i$ $(p_i > q_i)$ of bit-length $\lambda/2$ , and computes $N_i = p_i q_i$ which satisfy $(N_i > N)$.
(2) $M_i$ computes $\phi(N_i) = (p_i - 1)(q_i - 1)$.
(3) $M_i$ randomly chooses an integer $e_i$ which is coprime to $\phi(N_i)$ and computes the integer $d_i$ such that $e_i d_i = 1 \pmod{\phi(N_i)}$.
(3) $M_i$ provides authentically $(ID_i, e_i, N_i)$ to $D$ through a public channel, and keeps his shadow $d_i$ secret.

$D$ puts $(ID_i, e_i, N_i), i = 1, 2, \ldots, n$, on NB.

**[Note]:** After the initialization phase, the information on NB can be reusable. The dealer $D$ does not know any participant's shadow, so the shadow can be reusable for multiple rounds of sharing even with different dealers.

- **Construction phase**

Let $P_1, P_2, \ldots, P_k$ be the $k$ secrets to be shared, $0 < P_i < Q, i = 1, 2, \ldots, k$. The dealer $D$ performs the following steps:

(1) In case $k \le t$
  (1) $D$ constructs a polynomial $f(x) \bmod Q$ of degree $(t-1)$:

$$f(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q.$$

  (2) $D$ generates subshadow $Y_i$ for participant $M_i$: $D$ randomly chooses $n$ different integers $C_1, C_2, \ldots, C_n$ such that $0 < C_i < Q, i = 1, 2, \ldots, n$ and computes $Y_i = f(C_i) \bmod Q$ for $i = 1, 2, \ldots, n$.
  (3) $D$ computes $H_i$ for $i = 1, 2, \ldots, n$,

$$H_i = Y_i^{e_i} \bmod N_i.$$

(4) $D$ computes $A_i$ for $i = 1, 2, \ldots, t$,

$$A_i = g^{P_i} \bmod q \quad (1 \le i \le k),$$
$$A_i = g^{a_{i-k}} \bmod q \quad (k < i \le t).$$

(5) $D$ publishes $(C_1, C_2, \ldots, C_n, H_1, H_2, \ldots, H_n, A_1, A_2, \ldots, A_t)$ on NB.

(2) In case $k > t$

(1) $D$ constructs a polynomial $f(x) \bmod Q$ of degree $(k-1)$:

$$f(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} \bmod Q.$$

(2) $D$ generates subshadow $Y_i$ for participant $M_i$, $D$ randomly chooses distinct integers $C_1$, $C_2$, $\cdots$, $C_n$ such that $0 < C_i < Q$, $i = 1, 2, \ldots, n$, and computes $Y_i = f(C_i) \bmod Q$ for $i = 1, 2, \ldots, n$.

(3) $D$ picks $k-t$ distinct minimum integers $\eta_1, \eta_2, \ldots, \eta_{k-t}$ from $\mathbb{Z}_Q^* - \{C_i \mid i = 1, 2, \ldots, n\}$, computes $f(\eta_i) \bmod Q$ for $i = 1, 2, \ldots, k-t$.

(4) $D$ computes $H_i$ for $i = 1, 2, \ldots, n$:

$$H_i = Y_i^{e_i} \bmod N_i.$$

(5) $D$ computes $A_i = g^{P_i} \bmod q$, $i = 1, 2, \ldots, k$.

(6) $D$ puts $\left(C_1, C_2, \ldots, C_n, H_1, H_2, \ldots, H_n, \eta_1, \eta_2, \ldots, \eta_{k-t}, f(\eta_1), f(\eta_2), \ldots, f(\eta_{k-t}), A_1, A_2, \ldots, A_k\right)$ on NB.

- **Verification phase**

Each participant $M_i$ gets his subshadow by computing $Y_i = (H_i)^{d_i} \bmod N_i$ for $i = 1, 2, \ldots, n$. The validity of subshadows and their consistence with the information published by $D$ on NB can be verified by each participant $M_i$ as follows.

(1) If $k \le t$, $M_i$ checks

$$g^{Y_i} \stackrel{?}{=} \prod_{l=0}^{t-1} (A_{l+1})^{(C_i)^l} \bmod q$$

(2) If $k > t$, $M_i$ checks

$$g^{Y_i} \stackrel{?}{=} \prod_{l=0}^{k-1} (A_{l+1})^{(C_i)^l} \bmod q$$
$$g^{f(\eta_j)} \stackrel{?}{=} \prod_{l=0}^{k-1} (A_{l+1})^{(\eta_j)^l} \bmod q, \quad j = 1, 2, \ldots, k-t$$

If $M_i$'s verification is successful, $M_i$ believes the subshadow $Y_i$ he has got is valid and is consistent with the public information on NB. If no participant fails in the verification, $D$ is thought honest.

Note that we add the consistency detection of all subshadows in the verification phase. This is necessary for preventing the dealer from distributing a fake subshadow to a participant. The weakness of the schemes attacked in the previous section is mainly due to lack of such a detection.

- **Recovery phase**

Suppose $t$ arbitrary participants $\{M_i\}_{i \in I}\left(I \subseteq \{1, 2, \ldots, n\}\right)$ pool their subshadows $Y_i$ to reconstruct the shared secrets. Each participant $M_i (i \in I)$ can check whether others' secret subshadows are valid and consistent by the following equations:

$$g^{Y_i} \stackrel{?}{=} \prod_{l=0}^{k-1} (A_{l+1})^{(C_i)^l} \bmod q, \quad j \in I.$$

Once $t$ valid subshadows are collected, the polynomial $f(x) \bmod Q$ can be uniquely determined as follows:

(1) If $k \le t$

$$f(x) = \left( \sum_{i=1}^{t} Y_i \prod_{j=1, j \ne i}^{t} \frac{x - C_j}{C_i - C_j} \right) \bmod Q$$
$$= P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q$$

(2) If $k > t$

$$f(x) = \left( \sum_{i=1}^{t} Y_i \prod_{j=1, j \ne i}^{t} \frac{x - C_j}{C_i - C_j} \prod_{l=1}^{k-t} \frac{x - \eta_l}{C_i - \eta_l} + \sum_{i=1}^{k-t} f(\eta_i) \prod_{j=1, j \ne i}^{k-t} \frac{x - \eta_j}{\eta_i - \eta_j} \prod_{l=1}^{t} \frac{x - C_l}{\eta_i - C_l} \right) \bmod Q$$
$$= P_1 + P_2 x + \cdots + P_k x^{k-1} \bmod Q$$

The structure of our scheme 1 is similar to that of the ZZZ scheme. The main difference lies in we use the RSA encryption system while the ZZZ scheme uses Diffie–Hellman key exchange. A comparison of the two scheme is shown in Fig. 1. In the ZZZ

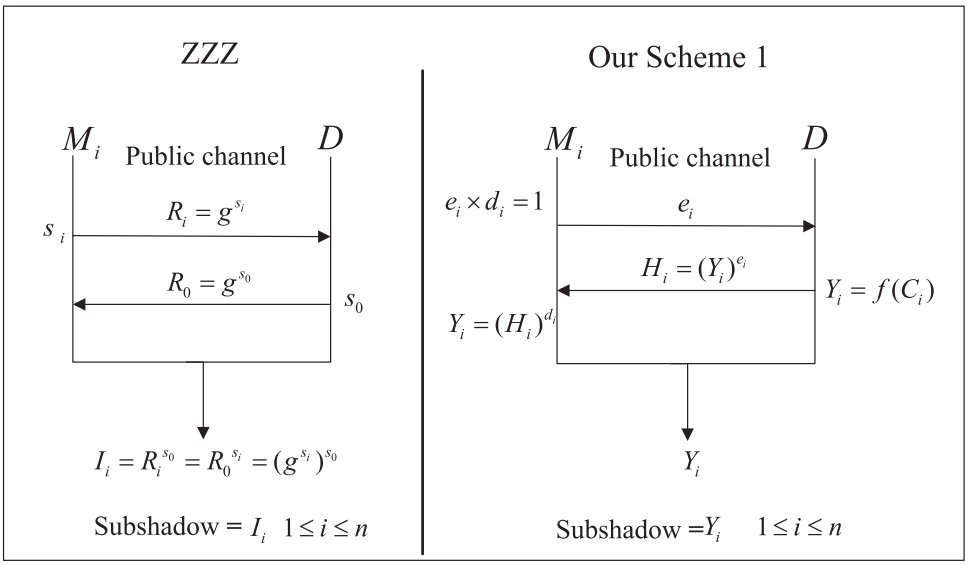


**Fig. 1.** The difference between our scheme 1 and ZZZ scheme.

scheme, participant $M_i$ chooses its secret shadow $s_i$ and computes its subshadow as $I_i = R_0^{s_i} \bmod N$ using the public information $R_0 = g^{s_0} \bmod N$ published by the dealer $D$. $M_i$ also sends $R_i = g^{s_i} \bmod N$ to $D$ as its public information corresponding to its secret shadow $s_i$. $D$ computes the subshadow of $M_i$ as $I_i = R_i^{s_0} \bmod N$ which is used in the computation of public information $y_i = h(I_i)$. While in our new scheme, participant $M_i$ generates a RSA public and private key pair $((e_i, N_i), d_i)$. It sets the private key $d_i$ as its secret shadow and computes its subshadow as $Y_i = H_i^{d_i} \bmod N_i$ using the public information $H_i = Y_i^{e_i} \bmod N_i$ published by the dealer $D$. Where $D$ computes the subshadow $Y_i$ of $M_i$ as $Y_i = f(C_i) \bmod Q$ from a publicly known $C_i \in Z_Q$. $D$ also publishes commitments to the coefficients of the polynomial $f(x)$. To compare the two scheme, please note in the ZZZ scheme, three modular exponentiation $I_i = R_0^{s_i} \bmod N$, $R_i = g^{s_i} \bmod N$, and $I_i = R_i^{s_0} \bmod N$ are needed for $M_i$ and $D$ to compute the same subshadow $I_i$ for participant $M_i$. Whereas in our new scheme, only two modular exponentiation $Y_i = H_i^{d_i} \bmod N_i$ and $H_i = Y_i^{e_i} \bmod N_i$ are needed for this purpose. More importantly, in the ZZZ scheme the dealer $D$ does not commit to the public information $y_i$. This weakness makes it possible for the dealer $D$ to cheat a participant $M_i$ by publishing a fake $y_i$ as pointed in our attack. While in our new scheme,this weakness is eliminated by requiring the dealer publishing commitment to the polynomial $f(x)$.

### 4.2. Security analysis

The security of our scheme 1 is based on the discrete logarithm problem and the large integer factorization problem which are assumed to be hard. We analyze the security of our scheme 1 from three aspects as formulated in the security model.

1. *Correctness*: If the dealer and the participants are honest, any $t$ or more participants can correctly reconstruct the set of secrets using the recovery algorithm. This can be proved by the following equations.
   - If $k \le t$

$$\begin{aligned} f(x) &= \left( \sum_{i=1}^{t} Y_i \prod_{j=1, j\neq i}^{t} \frac{x - C_j}{C_i - C_j} \right) \bmod Q \\ &= P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \bmod Q \end{aligned}$$

   - If $k > t$

$$\begin{aligned} f(x) &= \left( \sum_{i=1}^{t} Y_i \prod_{j=1, j\neq i}^{t} \frac{x - C_j}{C_i - C_j} \prod_{l=1}^{k-t} \frac{x - \eta_l}{C_i - \eta_l} + \sum_{i=1}^{k-t} f(\eta_i) \prod_{j=1, j\neq i}^{k-t} \frac{x - \eta_j}{\eta_i - \eta_j} \prod_{l=1}^{t} \frac{x - C_l}{\eta_i - C_l} \right) \bmod Q \\ &= P_1 + P_2 x + \cdots + P_k x^{k-1} \bmod Q \end{aligned}$$

2. *Verifiability*:
   The following theorem shows that the dealer can not pass through verification if he distributes inconsistent subshadows.

   **Theorem 1.** *Suppose the discrete logarithm in $Z_q^*$ with base g is intractable. Then the probability for the dealer successfully distributes a fake subshadow to any participant is negligible, and the success probability for a participant $M_i$ in submitting a fake subshadow in the recovery phase without being detected is also negligible.*

**Proof.** For any participant $M_i$, its valid subshadow is an element $Y_i \in Z_Q^*$ such that $Y_i = f(C_i) \bmod Q$, $g^{Y_i} = \prod_{l=0}^{t-1} (A_{l+1})^{(C_i)^l} \bmod q$, if $k \le t$; or $Y_i = f(C_i) \bmod Q$, $g^{Y_i} = \prod_{l=0}^{k-1} (A_{l+1})^{(C_i)^l} \bmod q$, $g^{f(\eta_j)} = \prod_{l=0}^{k-1} (A_{l+1})^{(\eta_j)^l} \bmod q$, $j = 1, 2, \ldots, k-t$, if $k > t$.

Without loss of generality, just consider the case $k \le t$. Assume that the dealer distributes an invalid subshadow $Y_i'$ to $M_i$ that passes the verification. Then $D$ has to find a $Y_i' \ne f(C_i)$ such that $g^{Y_i'} = \prod_{l=0}^{t-1} (A_{l+1})^{(C_i)^l} \bmod q$. As $g^{Y_i'} = \prod_{l=0}^{t-1} (A_{l+1})^{(C_i)^l} \bmod q$ implies the equation $Y_i' = f(C_i) \bmod Q$ holds with probability 1, we conclude that the probability for the dealer $D$ successfully cheats any participant is negligible. □

Now consider the success probability for a participant $M_i$ in submitting a fake subshadow in the recovery phase without being detected. Let $Y_i$ be $M_i$'s true subshadow obtained from the dealer. To successfully cheat in the recovery phase, $M_i$ has to find a $Y_i' \ne Y_i$, $Y_i' \in Z_Q^*$ such that $g^{Y_i'} = \prod_{l=0}^{t-1} (A_{l+1})^{(C_i)^l} \bmod q$. Since $g^{Y_i'} = \prod_{l=0}^{t-1} (A_{l+1})^{(C_i)^l} \bmod q$ implies $Y_i' = f(C_i) = Y_i \bmod Q$ with probability 1, we know that $M_i$'s success probability in submitting a fake subshadow in the recovery phase without being detected is negligible.

3. *Privacy*:

To demonstrate that no useful information about the set of shared secrets are revealed to an adversary corrupting at most $t-1$ participants, we give the following two theorems with brief proofs. The first one shows that the open commitments do not reveal any useful information about the set of secrets and the subshadows, and the second one implies the confidentiality of the set of shared secrets against an adversary who corrupts up to $t-1$ participants.

**Theorem 2.** *The adversary E can not get any useful information about* $\{P_1, P_2, \ldots, P_k\}$ *and the subshadows possessed by any participants from the public information under the assumptions that the RSA cryptosystem used in the system is secure, and the discrete logarithm problem in* $Z_q^*$ *with respect to the base g is intractable. i.e. the commitments* $A_i$, $i = 1, 2, \ldots, t$ *(or k), and* $H_i$, $i = 1, 2, \ldots, n$ *do not reveal any useful information about the set of secrets and the subshadows.*

**Proof.** In case $k \le t$, the public commitments are $A_i = g^{P_i} \bmod q$ for $i = 1, \ldots, k$, $A_i = g^{a_{i-k}} \bmod q$ for $i = k+1, \ldots, t$, $H_i = Y_i^{e_i} \bmod N_i$ for $i = 1, 2, \ldots, n$. While in case $k > t$, the public commitments are $A_i = g^{P_i} \bmod q$ for $i = 1, \ldots, k$, $H_i = Y_i^{e_i} \bmod N_i$ for $i = 1, 2, \ldots, n$. As computing the discrete logarithm to the base $g$ is difficult, the adversary can not derive any useful information about the secrets and the polynomial $f(x)$ from the open commitments. Secondly, to derive a subshadows $Y_i$ from $H_i$ without knowing $M_i$'s private key, one needs to break the RSA encryption scheme. So, the public information leaks no useful information about the set of shared secrets and the subshadows. □

**Theorem 3.** *An adversary corrupting up to* $t-1$ *participants cannot derive any subshadow kept by an honest participant and consequently cannot get useful information about the set of shared secrets.*

**Proof.** We learn that the adversary cannot get any useful information about the secret polynomial $f(x)$ from Theorem 2. Nevertheless according to the algorithm of construction, to acquire the subshadows of those honest participants, the adversary has no choice but compute $f(x)$ merely using the subshadows of the corrupted ones. Without loss of generality we suppose that the corrupted participants are $\{M_1, \ldots, M_{t-1}\}$. The adversary has to compute all coefficients of $f(x)$ from the following system of linear equations in $Z_Q$:

- If $k \le t$

$$\begin{cases} P_1 + P_2 C_1 + \cdots + P_k C_1^{k-1} + a_1 C_1^k + \cdots + a_{t-k} C_1^{t-1} = Y_1 \\ P_1 + P_2 C_2 + \cdots + P_k C_2^{k-1} + a_1 C_2^k + \cdots + a_{t-k} C_2^{t-1} = Y_2 \\ \vdots \\ P_1 + P_2 C_{t-1} + \cdots + P_k C_{t-1}^{k-1} + a_1 C_{t-1}^k + \cdots + a_{t-k} C_{t-1}^{t-1} = Y_{t-1} \end{cases}$$

i.e.

$$\begin{bmatrix} 1 & C_1 & \cdots & C_1^{k-1} & C_1^k & \cdots & C_1^{t-1} \\ 1 & C_2 & \cdots & C_2^{k-1} & C_2^k & \cdots & C_2^{t-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 1 & C_k & \cdots & C_k^{k-1} & C_k^k & \cdots & C_k^{t-1} \\ 1 & C_{k+1} & \cdots & C_{k+1}^{k-1} & C_{k+1}^k & \cdots & C_{k+1}^{t-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 1 & C_{t-1} & \cdots & C_{t-1}^{k-1} & C_{t-1}^k & \cdots & C_{t-1}^{t-1} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_k \\ a_1 \\ \vdots \\ a_{t-k} \end{bmatrix} = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_k \\ Y_{k+1} \\ \vdots \\ Y_{t-1} \end{bmatrix}$$

- If $k > t$

$$\begin{cases} P_1 + P_2C_1 + \cdots + P_kC_1^{k-1} = Y_1 \\ P_1 + P_2C_2 + \cdots + P_kC_2^{k-1} = Y_2 \\ \vdots \\ P_1 + P_2C_{t-1} + \cdots + P_kC_{t-1}^{k-1} = Y_{t-1} \\ P_1 + P_2\eta_1 + \cdots + P_k\eta_1^{k-1} = f(\eta_1) \\ \vdots \\ P_1 + P_2\eta_{k-t} + \cdots + P_k\eta_{k-t}^{k-1} = f(\eta_{k-t}) \end{cases}$$

i.e.

$$\begin{bmatrix} 1 & C_1 & C_1^2 & \cdots & C_1^{k-1} \\ 1 & C_2 & C_2^2 & \cdots & C_2^{k-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & C_{t-1} & C_{t-1}^2 & \cdots & C_{t-1}^{k-1} \\ 1 & \eta_1 & \eta_1^2 & \cdots & \eta_1^{k-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \eta_{k-t} & \eta_{k-t}^2 & \cdots & \eta_{k-t}^{k-1} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_t \\ P_{t+1} \\ \vdots \\ P_k \end{bmatrix} = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_{t-1} \\ f(\eta_1) \\ \vdots \\ f(\eta_{k-t}) \end{bmatrix}$$

These are systems of linear equations where the rank of coefficient matrices is less than the number of variables. That means it has at least $Q > 2^{\lambda/2}$ answers and the probability for the adversary to pick out the genuine $\{P_1, P_2, \ldots, P_k, a_1, \ldots, a_{t-k}\}$ are not more than $1/Q \le \lambda/2$. Accordingly the probability to calculate the subshadow of any uncorrupted participant is not more than $1/2^{\lambda/2}$, which is a negligible function of the security parameter $\lambda$. □

From the above analysis, we can draw the conclusion that our scheme 1 is a secure VMSS scheme.

### 4.3. Scheme 2

In this section we present another new VMSS scheme based on the homogeneous linear recursion, the RSA cryptosystem and the discrete logarithm problem. Let $D$ be the dealer, $M = \{M_1, M_2, \ldots, M_n\}$ be the set of participants, $t(t < n)$ be the threshold.

- **Initialization phase**

In this phase, the dealer $D$ first creates a public notice board (NB) which is used for storing necessary public information. The participants can access the information on NB. But the contents on the board can only be modified or updated by $D$.

Initialization of $D$:

(1) On input a security parameter $\lambda$, $D$ chooses two $\lambda/2$ bit strong primes $p_0$ and $q_0$ ($p_0 > q_0$), satisfying the requirement of a secure RSA public key cryptosystem [32], and computes $N = p_0q_0$.
(2) $D$ computes $\phi(N) = (p_0 - 1)(q_0 - 1)$, then safely destroy $p_0, q_0$.
(3) $D$ randomly chooses two primes $Q$, $q$, such that $Q|(q - 1)$, and the bit-length of $Q$ is at least $\lambda/2$. $D$ also selects an element $g$ of $Z_q^*$ with order $Q$ such that the discrete logarithm problem with base $g$ in $Z_q^*$ is infeasible.
(4) $D$ randomly chooses another integer $\alpha \neq 0$ and establishes the auxiliary equation:

$$(x - \alpha)^t = x^t + a_1x^{t-1} + \cdots + a_t = 0.$$

(5) $D$ publishes $(\lambda, N, Q, q, g, \alpha)$ on NB.

Initialization of participants:

(1) Each $M_i$ with identity information $ID_i$ chooses two strong primes $p_i$ and $q_i$ ($p_i > q_i$), satisfying the requirement of a secure RSA public key cryptosystem [32], and computes $N_i = p_iq_i$ which satisfy $(N_i > N)$.
(2) $M_i$ computes $\phi(N_i) = (p_i - 1)(q_i - 1)$.
(3) $M_i$ randomly chooses an integer $e_i$ which is coprime to $\phi(N_i)$ and computes the integer $d_i$ such that $e_id_i = 1 \pmod{\phi(N_i)}$.
(4) $M_i$ authentically provides $(ID_i, e_i, N_i)$ to $D$ through a public channel, and keeps his shadow $d_i$ secret.

$D$ puts $(ID_i, e_i, N_i)$, $i = 1, 2, \ldots, n$, on NB.

we note that, similar to scheme 1, the information on NB can be reusable after the initialization phase. The dealer $D$ does not know any participant's shadow, so the shadow can be reusable for multiple rounds of sharing even with different dealers.

- **Construction phase**

Let $P_1, P_2, \ldots, P_k \in Z_Q$ denote $k$ secrets to be shared. $D$ chooses at random an integer $a_i$ such that $Q > a_i$ for $i = 1, 2, \ldots, t$. Then $D$ performs the following steps to generate a subshadow $u_i$ for each participant $M_i$:

(1) Randomly choose $C_i \in \mathbb{Z}_Q^*$ for $i = 1, 2, \ldots, t$.

(2) Set up an [HLR] by the equations

$$[*]\begin{cases} u_1 = C_1, u_2 = C_2, \ldots, u_t = C_t, \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0 \bmod Q \quad (i \geq 1) \end{cases}$$

and compute $u_i$, $t < i \leq n + k$.

(3) Compute $Y_i = P_i - u_{n+i} \bmod Q$ for $i = 1, 2, \ldots, k$.

(4) Compute $H_i = (u_i)^{e_i} \bmod N_i$ and $T_i = g^{u_i} \bmod q$ for $1 \leq i \leq n$.

(5) Publish $(H_1, H_2, \ldots, H_n, T_1, T_2, \ldots, T_n, Y_1, Y_2, \ldots, Y_k)$ on NB.

- **Verification phase**

Each participant $M_i$ can get is subshadow by computing $u_i = (H_i)^{d_i} \bmod N_i$ for $i = 1, 2, \ldots, n$. The validity and consistence of $M_i$'s subshadow $u_i$ with the information published by $D$ on NB can be verified as follows:

$$T_{t+i} \prod_{j=1}^{t} (T_{t+i-j})^{a_j} \stackrel{?}{=} 1 \bmod q$$

$$T_i \stackrel{?}{=} g^{u_i} \bmod q$$

If $M_i$'s verification is successful, $M_i$ believes the subshadow $u_i$ he has got is valid and is consistent with the public information on NB. If no participant fails in the verification, $D$ is thought honest.

Similar to that in scheme 1, we add the consistency detection of all subshadows in the verification phase. This is necessary for removing the weakness of the schemes attacked in the previous section.

- **Recovery phase**

Assume that $t$ or more arbitrary participants $\{M_i\}_{i \in I}\big(I \subseteq \{1, 2, \ldots, n\}\big)$ pool together their subshadows $u_i$ to reconstruct the shared secrets. Each participant $M_i$ can check whether the subshadows provided by the others are valid by the following equations:

$$g^{u_j} \stackrel{?}{=} T_j \bmod q, \quad j \in I.$$

If there are at least $t$ valid subshadows, the shared secrets can be correctly reconstructed. Suppose they use $t$ valid subshadows $\{u_i | i \in J \subset I\}$, they can get the following simultaneous equations using Lemma 1 in Section 2:

$$z_0 + z_1 i + \cdots + z_{t-1} i^{t-1} = u_i \alpha^{-i} \bmod Q, \quad i \in J.$$

Solving the equations (or equivalently using the technique of Lagrange interpolation ), they get (in $Z_Q$) $z_0 = A_0, z_1 = A_1, \ldots, z_{t-1} = A_{t-1}$. Now, they have

$$u_i = (A_0 + A_1 i + \cdots + A_{t-1} i^{t-1}) \alpha^i \bmod Q, \quad \forall i \geq t.$$

Hence they can reconstruct the shared secrets:

$$P_i = Y_i + u_{n+i} \bmod Q, i = 1, 2, \ldots, k.$$

The difference between our scheme 2 and MS1 and MS2 schemes is shown in Fig. 2.

As seeing in Fig. 2, in scheme SM1, a participant $M_i$ chooses its secret shadow $s_i$, and encrypts it using the public key of the dealer $D$ and sends the cipher text to $D$. After that both $D$ and $M_i$ can computer the subshadow $I_i = f(r, s_i)$ for $M_i$. No information is provided for detecting whether the $I_i$ used in the [HLR] sequence is the same as the true subshadow of $M_i$. In scheme SM2, a participant $M_i$ chooses its secret shadow $s_i$, computes its subshadow as $I_i = R_0^{s_i} \bmod N$ using the public information $R_0 = g^{s_0} \bmod N$ published by the dealer $D$ and sends $R_i = g^{s_i} \bmod N$ to $D$ as its commitment to its secret shadow $s_i$. $D$ computes the subshadow of $M_i$ as $I_i = R_i^{s_0} \bmod N$ which is used in the generation of the [HLR] sequence. Three modular exponentiations are needed for the computation. No information for verifying whether correct $I_i$ is used in the computation of the [HLR] sequence. While in our scheme 2, $M_i$ selects its secret shadow $d_i$ and keeps it from the dealer. The subshadow of $M_i$ is encrypted using $M_i$'s public key corresponding to $d_i$ and is provided in the public information. Only two modular exponentiations are involved for the transmission of a subshadow. We require the dealer publish some information for verifying the consistence of participant's subshadow and the [HLR] sequence so that cheating behavior of the dealer can be detected.

### 4.4. Security analysis

The security of our scheme 2 is based on the discrete logarithm problem and the large integer factorization problem which are assumed to be hard.

1. *Correctness*: If the dealer and the participants are honest, any $t$ or more participants can reconstruct the set of the shared secrets in the recovery phase. This fact can be shown as follows.

Suppose $\{M_i, i \in I\}$ be a set of at least $t$ honest participants. Let $\{u_i, i \in I\}$ be their corresponding subshadows obtained from the honest dealer $D$. Using their subshadows, they can get the following equations

$$z_0 + z_1 i + \cdots + z_{t-1} i^{t-1} = u_i \alpha^{-i} \bmod Q, \quad i \in I.$$

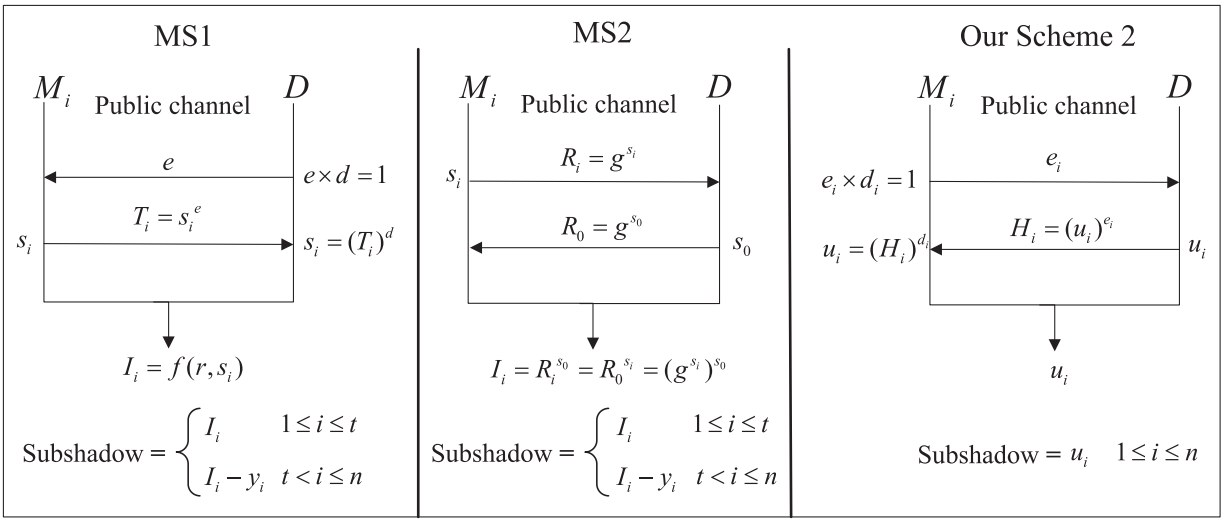


**Fig. 2.** The difference of our scheme 2 with MS1 and MS2 schemes.

Solving this system of equations (or using the technique of Lagrange interpolation), they get

$$u_i = (A_0 + A_1 i + \cdots + A_{t-1} i^{t-1})\alpha^i \bmod Q, \quad \forall i \ge t.$$

Hence they can reconstruct the shared secrets:

$$P_i = Y_i + u_{n+i} \bmod Q, i = 1, 2, \ldots, k.$$

2. *Verifiability*:
The following theorem shows that the dealer cannot pass through verification if he distributes inconsistent subshadows. And a dishonest participant is unable to submit a fake subshadow without being detected in the recovery phase.

**Theorem 4.** *The probability for the dealer successfully distributing a fake subshadow to any participant without being detected is negligible. At the same time, the probability for a dishonest participant submitting a fake subshadow without being detected in the recovery phase is negligible.*

**Proof.** Assume $M_i$'s valid subshadow is $u_i$, and the dealer successfully distributes a fake subshadow $u_i'$ to $M_i$. Then $T_i = g^{u_i} = g^{u_i'} \bmod q$, and $T_{t+i} \prod_{j=1}^{t} (T_{t+i-j})^{a_j} = 1 \bmod q$. Since $u_i, u_i' \in Z_Q$, this implies that the probability for $u_i' \neq u_i$ is negligible. Similarly, if a dishonest participant $M_i$ submits a fake subshadow $u_i'$ without being detected in the recovery phase, then we have $T_i = g^{u_i'} = g^{u_i} \bmod q$. Hence, $u_i' = u_i \bmod Q$ holds with probability 1. This means the probability for a participant $M_i$ successfully submitting a fake subshadow without being detected in the recovery phase is negligible. □

3. *Privacy*:

**Theorem 5.** *Assume that computing discrete logarithm in $Z_q^*$ is difficult and the RSA encryption scheme is secure. Then the public information $T_i$, $H_i$, $i = 1, \ldots, n$, do not reveal any useful information about the set of shared secrets and the subshadows of participants.*

**Proof.** We know that $T_i = g^{u_i} \bmod q$, $H_i = (u_i)^{e_i} \bmod N_i$ for $i = 1, \ldots, n$. As computing the discrete logarithm to the base $g$ is difficult, the adversary cannot derive any useful information about subshadows from the open commitments $T_1, T_2, \ldots, T_n$,. Second, Since $H_i$ is the RSA encryption of $M_i$'s subshadow $u_i$, to derive $u_i$ from $H_i$ the adversary $E$ has to break the RSA encryption scheme. Under the assumption that the RSA encryption scheme used in our construction is secure the adversary gets no useful information about $u_1, u_2, \ldots, u_n$ from $H_1, H_2, \ldots, H_n$. Without the knowledge of at least $t$ subshadows of the participants, the adversary cannot compute any of $u_{n+1}, u_{n+2}, \ldots, T_{n+k}$ due to the definition and properties of linear recursion sequence $u_j$. Hence the adversary gets no useful information about the set of shared secrets $u_{n+1} + Y_1, u_{n+2} + Y_2, \ldots, u_{n+k} + Y_k$ from public information. □

**Theorem 6.** *An adversary corrupts up to $t - 1$ participants cannot derive any subshadow kept by any honest participant and consequently cannot get any of the shared secrets.*

**Proof.** We learn that the adversary cannot get any useful information about the [HLR] from Theorem 5. Nevertheless according to the algorithm in the construction phase, to acquire the subshadows of those honest participants, the adversary has no choice but compute the [HLR] merely using the subshadows of the corrupted ones. Without loss of generality we suppose

**Table 1**
Analysis of computation cost.

| Scheme | Initialization | | Construction | Verification | Recovery |
|---|---|---|---|---|---|
| | Dealer $D$ | Each $M_i$ | Dealer $D$ | Each $M_i$ | Each $M_i$ |
| ZZZ | 0 | 1 | $n+1$ | – | $t$ |
| MS | $2n$ | 1 | 0 | – | $t-1$ |
| MS1 | $n$ | 1 | $n$ | – | $t-1$ |
| MS2 | 0 | 1 | $n+1$ | – | $t$ |
| Scheme 1 | 0 | 0 | $n+t,\ k \le t$ | $t+1,\ k \le t$ | $(t-1)(k+1)$ |
| Scheme 2 | 0 | 0 | $2n$ | 2 | $t-1$ |

that the corrupted participants are $\{M_1, \ldots, M_{t-1}\}$. The adversary has to compute the sequence $u_i$ of [HLR] from the following system of equations:

$$\begin{cases} u_1 = C_1, u_2 = C_2, \ldots, u_{t-1} = C_{t-1} \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0 \bmod Q, i = 1, 2, \ldots, n-t. \end{cases}$$

Namely, to compute any other subshadow $u_j$, the adversary should solve the following system of linear equations using the $t-1$ subshadow $u_1 = C_1, u_2 = C_2, \ldots, u_{t-1} = C_{t-1}$:

$$u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0 \bmod Q, i = 1, 2, \ldots, n-t$$

Note that this system of linear equations consists of $n-t$ equations, and there are $n-t+1$ variables $u_t, u_{t+1}, \ldots, u_n$. So the rank of the coefficient matrix is less than the number of variables. That means it has not less than $Q$ answers and the probability for the adversary to pick out the correct sequence $u_{t-1+i}$ $(i \ge 1)$ used in share distribution is not more than $1/Q$. Accordingly the probability to calculate the subshadow of any uncorrupted participant is not more than $1/Q$. As $Q > 2^{\lambda/2}$, this probability is not more than $1/2^{\lambda/2}$, which is a negligible function of the security parameter $\lambda$. □

From the above analysis, we know that our scheme 2 is a secure VMSS without private channels.

## 5. Performance analysis

### 5.1. Computation cost

In comparing the computational cost of our schemes with some other schemes of the same type, we list the amount of the most time consuming operations in each phase of these schemes. The most time consuming operations we consider here is modular exponentiation. Table 1 shows the main computational cost of our new schemes and the four schemes analyzed in Section 3.

As shown in Table 1, in the initialization and construction phases, our scheme 2 is the most efficient. While our scheme1 is slightly more efficient than MS and MS1 schemes (assume $n > k$), and less efficient than ZZZ and MS2 schemes. All the six schemes have almost the same computational cost in the recovery phase. Since we add consistence test to prevent cheating by the dealer, the verification phases of over new schemes require more modular exponentiations than in the other schemes. We note that such added computational cost is necessary for preventing cheating by the dealer. Without this distinctive feature of preventing cheating by the dealer, a so called verifiable secret sharing scheme will lose its real meaning for "verifiability". As demonstrated in Section 3, it is the lack of such tests that makes the other four schemes vulnerable to cheating by the dealers. As a whole, our new schemes are efficient and have a comparable computational cost with respect to similar existing verifiable multi-secret sharing schemes.

### 5.2. Communication cost

In Table 2, we list the communication cost in the initialization and construction phases of the six schemes, ZZZ scheme, MS scheme, MS1 scheme, MS2 scheme, and our new schemes. The communication cost of the six schemes in the recovery phase is almost the same. Table 2 indicates that our two new schemes are nearly as communication efficient as the other four schemes in the initialization phase, but slightly less efficient in the construction phase. This inefficiency is due to we require the dealer publish some redundant information for testing the consistence of the public information with the shadows and subshadows of participants. Our analysis in Section 3 reveals that the insecurity of the other four schemes is exactly resulted from lacking of such redundant information.

### 5.3. Main performance features

We also compare the main performance features of our new schemes with the other four schemes cited above. We consider six main functionalities of a VMSS scheme.

**Table 2**
Analysis of communication cost.

| Scheme | Initialization phase | | Construction phase |
|---|---|---|---|
| | $D$ Broadcast | $M_i$ to $D$ | $D$ Broadcast |
| ZZZ | $(g, N)$<br>$(ID_i, R_i),\ i = 1, 2, \ldots, n$ | $(ID_i, R_i)$<br>$i = 1, 2, \ldots, n$ | $(R_0, f), (y_1, y_2, \ldots, y_n),\ k \le t$<br>$(R_0, f), \big(y_1, \ldots, y_n, h(1), \ldots, h(k-t)\big),\ k > t$ |
| MS | $(e, N, g, p), (r, G_i),\ i = 1, 2, \ldots, n$<br>$(ID_i, T_i),\ i = 1, 2, \ldots, n$ | $(ID_i, T_i)$<br>$i = 1, 2, \ldots, n$ | $(y_1, y_2, \ldots, y_n),\ k \le t$<br>$(y_1, y_2, \ldots, y_n, h(1), h(2), \ldots, h(k-t)),\ k > t$ |
| MS1 | $(e, N, g, q, \alpha)$<br>$(ID_i, T_i),\ i = 1, 2, \ldots, n$ | $(ID_i, T_i)$<br>$i = 1, 2, \ldots, n$ | $(r, G_1, G_2, \ldots, G_n, r_1, r_2, \ldots, r_k, y_{t+1}, y_{t+2}, \ldots, y_n)$ |
| MS2 | $(N, g, q, \alpha)$<br>$(i, T_i),\ i = 1, 2, \ldots, n$ | $(i, T_i)$<br>$i = 1, 2, \ldots, n$ | $(R_0, f, r_1, r_2, \ldots, r_k, y_{t+1}, y_{t+2}, \ldots, y_n)$ |
| Scheme 1 | $(\lambda, N, Q, q, g)$<br>$(ID_i, e_i, N_i),\ i = 1, 2, \ldots, n$ | $(ID_i, e_i, N_i)$<br>$i = 1, 2, \ldots, n$ | $(C_1, \ldots, C_n, H_1, \ldots, H_n, A_1, \ldots, A_t),\ k \le t$<br>$\big(C_1, \ldots, C_n, H_1, \ldots, H_n, \eta_1, \ldots, \eta_{k-t}, A_1, \ldots, A_k, f(\eta_1), \ldots, f(\eta_{k-t})\big),\ k > t$ |
| Scheme 2 | $(\lambda, N, Q, q, g, \alpha)$<br>$(ID_i, e_i, N_i),\ i = 1, 2, \ldots, n$ | $(ID_i, e_i, N_i)$<br>$i = 1, 2, \ldots, n$ | $(H_1, H_2, \ldots, H_n, T_1, T_2, \ldots, T_n, Y_1, Y_2, \ldots, Y_k)$ |

**Table 3**
Performance features.

| Functionality | ZZZ scheme | MS scheme | MS1 scheme | MS2 scheme | Our scheme 1 | Our scheme 2 |
|---|---|---|---|---|---|---|
| 1 | NO | NO | NO | NO | YES | YES |
| 2 | YES | YES | YES | YES | YES | YES |
| 3 | YES | YES | YES | YES | YES | YES |
| 4 | YES | YES | YES | YES | YES | YES |
| 5 | YES | YES | YES | YES | YES | YES |
| 6 | YES | NO | NO | YES | YES | YES |

- Functionality 1: Resist cheating by the dealer $D$
- Functionality 2: Resist cheating by dishonest participants $M_i$
- Functionality 3: Without secret channel
- Functionality 4: Reconstruct multi-secrets parallelly
- Functionality 5: Reuse of the secret shadows
- Functionality 6: Reuse of the secret shadows for multiple rounds of sharing even with different dealers.

Table 3 shows that both of our new schemes possess all the six main performance features. While the other four schemes do not have functionality 1, i.e. the cannot resist cheating by a dishonest dealer. The MS scheme and MS1 scheme do not possess functionality 6. This means that the secret shadows of participants will useless after the recovery phase. So, the initialization of participants has to be executed in every round of sharing even if the group of participants is not changed. Our two new schemes effectively overcome this inconvenience. They allow participants reuse their secret shadows in different rounds of multi-secret sharing even with different dealers. In this way, a participant could run the initialization of participant only once, and could use the information generated in this execution of initialization in many rounds of multi-secret sharing no matter the dealers in these round of sharing are different. This feature enables the participants to greatly reduce the cost of initialization in multiple rounds of multi-secret sharing.

## 6. Conclusion

Verifiable multi-secret sharing schemes provide practical techniques for sharing multiple secrets in a group of participants so that cheating behavior of a dealer or a participant can be detected. They are important tools in keeping multiple secrets such as cryptographic keys, and in designing secure multi-party protocols. In this paper, we begin with re-analyze the security of four recently proposed VMSS schemes. Our analysis reveals that all these schemes are subject to cheating by dishonest dealers. So these schemes do not satisfy the basic security requirement of verifiable secret sharing schemes. We notice that the security drawback of these schemes is induced by lacking of the consistence test of the information published by a dealer with the subshadows of participants. Based on the analysis, we further put forward two improved VMSS schemes. In our new schemes, we require the dealer to publish some redundant information for the necessary consistence checking. The security analysis and performance analysis of our new schemes demonstrate that they are secure and efficient verifiable multi-secret sharing schemes withstanding cheating by the dealer or a participant, requiring no secret channels, allowing parallel reconstruct of multiple secrets and reuse of shadows in different rounds of sharing even with different dealers.

## Acknowledgments

The authors are very grateful to the anonymous reviewers and the editors for their valuable suggestions. This work is supported by National Natural Science Foundation of China (No.61170298), Natural Science Fund for Colleges and Universities in Jiangsu Province (No. 12KJD520007), NSF of Jiangsu Province of China (No. BK20130908), Program of Natural Science Research of Jiangsu Higher Education Institutions of China (Grant No.13KJD520006).

## References

[1] N.L. Biggs, Discrete Mathematics, revised ed., Oxford University Press, New York, 1989.
[2] G. Blakley, Safeguarding cryptographic keys, in: Proceedings of the AFIPS 1979 Nalt Conf, AFIPS Press, New York, 1979, pp. 313–317.
[3] T.Y. Chang, M.S. Hwang, W.P. Yang, An improvement on the Lin-Wu $(t, n)$ -threshold verifiable multi-secret sharing scheme, Appl. Math. Comput. 163 (2005) 169–178.
[4] L. Chen, C. D.Gollmann, J. Mitchell, P. Wild, Secret sharing with reusable polynomials, in: Proceedings of ACISP'97, 1997, pp. 183–193.
[5] H.Y. Chien, J.K. Jan, Y.M. Tseng, A Practical $(t, n)$ Multi-secret Sharing Scheme, IEICE Trans. Fundam. E83-A (12) (2000) 2762–2765.
[6] B. Chor, S. Goldwasser, S. Micali, et al., Verifiable secret sharing and achieving simultaneity, The presence Offaults: Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (FOCS), Washington, 1985, pp. 251–260.
[7] G.D. Crescenzo, Sharing one secret vs. sharing many secrets: tight bounds on the average improvement ratio, Theor. Comput. Sci. 295 (2003) 123–140.
[8] M.H. Dehkordi, S. Mashhadi, An efficient threshold verifiable multi-secret sharing, Comput. Standards Interfac. 30 (3) (2008) 187–190.
[9] M.H. Dehkordi, S. Mashhadi, New efficient and practical verifiable multi-secret sharing schemes, Inf. Sci. 178 (9) (2008) 2262–2274.
[10] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Info. Theory IT-22 (6) (1976) 644–654.
[11] W. Diffie, M. Hellman, Multiuser cryptographic techniques, in: Proceedings of AFIPS 1976 NCC, AFIPS Press, Montvale, N.J., 1976, pp. 109–112.
[12] P. Feldman, A practical scheme for non-interactive verifiable secret sharing [A], Proceedings of 28th IEEE Symposium on Foundations of Computer Science [C], IEEE, Canada, 1987.
[13] L. Harn, Efficient sharing (broadcasting) of multi-secret, in: IEEE Proceedings Computers and Digital Techniques, 142, 1995, pp. 237–240.
[14] L. Harn, C. Lin, Strong $(n, t, n)$ verifiable secret sharing scheme, Inf. Sci. 180 (16) (2010) 3059–3064.
[15] J. He, E. Dawson, Multistage secret sharing based on one-way function, Electron. Lett. 30 (1994) 1591–1592.
[16] J. He, E. Dawson, Multi secret-sharing scheme based on one-way function, Electron. Lett. 31 (2) (1995) 93–95.
[17] W.H. He, T.S. Wu, Comment on Lin-Wu $(t, n)$-threshold verifiable multisecret sharing scheme, IEEE Proc. Comput. Digit. Tech 148 (3) (2001) 139.
[18] M. Huang, J. Zhang, S. Xie, A Secure and Efficient $(t, n)$ Threshold Verifiable Multi-secret Sharing Scheme, LNCS 3802, Springer-Verlag Berlin Heidelberg, 2005, pp. 532–537. CIS 2005, Part II.
[19] R.J. Hwang, C.C. Chang, An on-line secret sharing scheme for multi-secrets, Comput. Commun. 21 (1998) 1170–1176.
[20] W.A. Jackson, K.M. Martin, C.M. O'Keefe, On sharing many secrets, in: Proceedings of the Asiacrypt'94, 1994, pp. 42–54.
[21] H.X. Li, C.T. Cheng, L.J. Pang, A new $(t, n)$-threshold multi-secret sharing scheme, in: Y. Hao, J. Liu, Y. Wang (Eds.), Computational Intelligence and Security, Springer-Verlag, Berlin, 2005, pp. 421–426.
[22] T.Y. Lin, T.C. Wu, $(t, n)$ threshold verifiable multi-secret sharing scheme based on factorization intractability and discrete logarithm module a composite problems, IEEE Proc. Comput. Digital Tech. 146 (1999) 264–268.
[23] L.J. Pang, Y.M. Wang, A New $(t, n)$ Multi-secret Sharing Scheme Based on Shamir's Secret Sharing, Appl. Math. Comput. 167 (2005) 840–848.
[24] J. Pieprzyk, X.M. Zhang, Constructions of Cheating Immune Secret Sharing, LNCS, 2288, Springer-Verlag, 2001, pp. 226–243. ICICS.
[25] J. Pieprzyk, X.M. Zhang, On cheating immune secret sharing, in: Discrete Mathematics and Theoretical Computer Science, 2004, pp. 253–264.
[26] R.D. Prisco, A.D. Santis, A Cheating Immune $(2, n)$-Threshold Visual Secret Sharing, (LNCS, 4116),, Springer, Berlin, 2006, pp. 216–228. SCN.
[27] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[28] K.R. Sahasranand, N. Nagaraj, S. Rajan, How not to share a set of secrets, Int. J. Comput. Sci. Inf. Security 8 (1) (2010) 234–237.
[29] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.
[30] J. Shao, Z.F. Cao, A new efficient $(t, n)$ verifiable multi-secret sharing (VMSS) based on YCH scheme, Appl. Math. Comput. 168 (2005) 135–140.
[31] M. Stadler, Public verifiable secret sharing, Proceeding of Advances in Cryptology -Eurocrypt'96, Springer-Verlag, Berlin, Germany, 1996.
[32] D.R. Stinson, Cryptography: Theory and Practice, second ed., Chapman & Hall, 2002.
[33] C.C. Yang, T.Y. Chang, M.S. Hwang, A $(t, n)$ Multi-secret Sharing Scheme, Appl. Math. Comput. 151 (2004) 483–490.
[34] X.M. Zhang, J. Pieprzyk, Cheating Immune Secret Sharing to Appear in The Third International Conference on Information and Communication Security (ICICS), LNCS, 2229, Springer-Verlag, 2001, pp. 144–149.
[35] J. Zhao, J.Z. Zhang, R. Zhao, A practical verifiable multi-secret sharing scheme, Comput. Stand. Interfaces 29 (1) (2007) 138–141.