New Efficient and Practical v-Fairness (t, n) Multi-Secret Sharing Schemes

Wenjie Yang, Futai Zhang

Abstract

Secret sharing plays an important role in protecting confidential information among all participants. A fairness secret sharing scheme assures that a dishonest participant cannot get any advantages over the honest ones in the process of secret reconstruction. Though there are many secret sharing schemes available in the literature, most of them do not satisfy the requirement of fairness. In this paper, we focus on v-fairness (t, n) multi-secret sharing schemes which are (t, n) threshold multi-secret sharing schemes with the feature of fairness even if there are v < t/2 dishonest participants. We show security weaknesses in an existing v-fairness (t, n) multi-secret sharing scheme, and then present two new v-fairness (t, n) multi-secret sharing schemes. Our new schemes are not only secure, but also remove the need for private channels.

Keywords: Secret Sharing Scheme, Multi-Secret Sharing Scheme, Fair Multi-Secret Sharing Scheme

1. Introduction

Secret sharing plays an important role in safeguarding cryptographic keys, protecting confidential information from getting lost, destroyed, or falling into wrong hands. It is a basic tool in designing secure protocols, and has been an interesting research branch of modern cryptography. Blakley and Shamir initiated the study of secret sharing in 1979[1,2]. They put forward the first (t, n) threshold secret sharing schemes independently. In their context, a (t, n) threshold secret sharing scheme is a mechanism to divide a secret S into n shadows for n participants, such that the secret S can be reconstructed when pooling together at least t valid shadows. After the pioneering work of Blakley and Shamir, a great deal of attention has been paid to the study of secret sharing. By now, many secret sharing schemes are available in the literature[13,12,3,4,5,6,7,24,25]. A careful observation reveals that when put into practical use, many of the earlier secret sharing schemes are subject to the following weaknesses:

(1) In each of the secret sharing process, only one secret can be shared such that the efficient of the early scheme is very lower.

(2) The shadow of the previous schemes is not reused in order to share different secrets. In other words, once the shared secret has been reconstructed, all shadows by the participant will no longer be confidential to everyone. Therefore, if the dealer want to again share some secrets, he/she must redistribute the shadow hold by the participants.

(3) In the previous scheme, both the dealer who is responsible for distributing the shadow and the participants who receive the shadow should be required to be honest in order to correctly recovery those shared secrets. If a malicious dealer distribute a fake shadow to a certain participant or a dishonest participant provide an invalid shadow in the reconstruction phase, the early schemes are very difficult to stop cheating to the other honest participants and achieve the fairness.

Later, several multi-secret sharing (MSS) schemes were presented to solve the first problem. In such schemes, several secrets can be shared during one secret sharing process[10,11]. In order to overcome the problems 1 and 2, He and Dawson proposed two MSS schemes to share multiple secrets in 1994[10] and in 1995[11] respectively. In their schemes, one-way functions were used to avoid disclosing the secret shadows. A pair of MSS schemes were introduced by Chien et al.[12] in 2000 and Yang et al.[3] in 2004 respectively. The former is based on the systematic block codes and matrices, and the latter is based on the Shamir's secret sharing. To solve the problem 3, Chor et al. proposed the
New Efficient and Practical v-Fairness (t, n) Multi-Secret Sharing Schemes
Wenjie Yang, Futai Zhang

In recent years, some practical verifiable (t, n) threshold multi-secret sharing schemes\cite{3,4,5,6,7} were presented. These schemes make use of public key cryptography to supply verifiability. We notice that all of these schemes fail to satisfy the requirement of fairness. The reason is that, though these schemes do provide methods to detect and identify cheaters, they have no methods to prevent the cheaters to get some advantages over the honest participants. Namely, when a dishonest participant cooperate with t-1 honest ones in the reconstruction phase, all of them can identify the cheater after providing their shadows, but no one except the cheater may get the shared secret. Tompa and Woll considered fairness in secret sharing in \cite{8}. They presented a secret sharing scheme by hiding the secret in a sequence $S_1, S_2, \ldots, S_t$ In their scheme, a cheater cannot obtain the secret if all participants release their own shadows simultaneously. However, it is difficult to make all participants provide their true shadows simultaneously in the practical applications. In 1995, Lin and Harn\cite{14} introduced a fair (t, n) secret sharing scheme using a similar technique. In their scheme, t participants do not need to release their shadows simultaneously for reconstructing the secret. However, a cheater still has a probability of $1/k$ to obtain the secret.

To our knowledge, the first truly fair secret sharing scheme was put forward by Lee and Laih\cite{15} up until 1997. In their v-fairness (t, n) secret sharing scheme, the honest participants and the cheaters have the same probability to obtain the secret and the cheaters can also be detected. Besides, their scheme is tolerant of $v$ cheaters among $t$ participants, where $v < t/2$. Although fairness is well guaranteed, we find that Lee and Laih's scheme is inefficient. In their scheme, each participant is required keep three shadows to reconstruct only one secret. To improve the efficiency, Hwang et al. \cite{9} presented a modified scheme which requires each participant to keep two shadows. In 2011, Yung-Cheng Lee et al. advanced a simple $(v, t, n)$-fairness secret sharing scheme\cite{16} requiring only one shadow for each participant.

In the above mentioned fair secret sharing schemes, only one secret can be shared during one secret sharing process. Very recently, the first v-fairness (t, n) threshold secret sharing scheme which shares multiple secrets during one secret sharing process was proposed by Jen-Ho Yang et al.\cite{17}. The scheme is a one time scheme and requires secure channels between the dealer and the participants. So, once the secret has been reconstructed, the dealer must redistribute a fresh shadow over a secure channel to every participant.

In this paper, at first we analyze a security weakness of the v-fairness (t, n) threshold multi-secret sharing scheme of Jen-Ho Yang et al.\cite{17}. Then we come up with two new v-fairness (t, n) multi-secret sharing schemes. In our schemes each participant obtain her/his masked shadow by an agreement with the dealer and there is not any need for a secure channel. What's more, the shadow of each participant can be reused for different sharing processes with different dealer. These features make our new schemes practical in real applications.

The rest of the paper is organized as follows: We first review the preliminaries used in our scheme in \textbf{Section 2}. In \textbf{Section 3} we briefly analyze Jen-Ho Yang et al.'s scheme. In \textbf{Section 4}, we propose our new schemes. In \textbf{Section 5} and \textbf{Section 6}, we give security analysis and performance analysis of our new schemes. Finally we present our conclusions in \textbf{Section 7}.

2. Preliminary

**Definition:** The fairness of a secret sharing scheme requires that:

1. If all participants (both the honest participants and the cheaters) honestly released their correct shadows in the recovery phase, these shared secrets can be obtained by any participants who want to recovery those secrets.

2. If some dishonest participants provide incorrect shadows in the recovery phase, either both the honest participants and the cheaters get the shared secrets, or both of them cannot obtain the shared secrets. In other words, even if there are some cheaters providing incorrect shadows, the honest participants and the cheaters still have the same probability to obtain the shared secrets.

3. If the dealer is a dishonest dealer, he cannot cheat some designed participants by distributing the incorrect shadows or publishing some malicious information.
A v-fairness \((t, n)\) multi-secret sharing scheme denotes a \((t, n)\) threshold multi-secret sharing scheme with the feature of fairness even if there are \(v\) dishonest participants, provided that at most \(v < t/2\).

**Discrete Logarithm (DL) Problem:** Let \(G\) be a finite cyclic multiplicative group of the prime order \(p\), the DL problem in \(G\) is that given \(g, h \in G\) to find an integer \(a \in \mathbb{Z}_p\) such that \(h = g^a\). We define the advantage of an algorithm \(B\) in solving the DL problem in \(G\) by \(\text{Adv}_B = \Pr[B(p, G, g, h) = a]\).

**Discrete Logarithm (DL) Assumption in \(G\):** The DL assumption is that \(\text{Adv}(B)\) is negligible for all efficient algorithm \(B\) in polynomial time.

### 3. Security Analysis of Jen-Ho Yang et al.’s Scheme

In this section we briefly review Jen-Ho Yang et al.’s v-fairness \((t, n)\) multi-secret sharing scheme[17]. Then, we analyze and point out that their scheme has some weaknesses in security.

#### 3.1. Review of Jen-Ho Yang et al.’s Scheme

In their scheme, there is a trusted dealer who initializes the parameters and distributes the shadows to the participants. The scheme is divided into two phases, the secret sharing phase and the secret reconstruction phase. Please refer to [17] for the detailed description of the scheme.

#### 3.2. Analysis of Jen-Ho Yang et al.’s Scheme

In the scheme, the dealer shares \(k\) secrets \((S_1, S_2, \ldots, S_k)\) in an \(n\)-participant group, and only \(t\) out of \(n\) participants can recover these secrets. Note that each participant must keep two shadows for recovering the secrets in their scheme and the communication between the dealer and each participant needs a private channel.

We notice that, in the above scheme the polynomials \(f_a(x), f_b(x)\) and \(f_c(x)\) are lack of constant terms. Thus \(t-1\) correct shadows can reconstruct \(f_a(x)\) and \(t-1\) correct shadows can reconstruct \(f_b(x)\) respectively. So, the scheme cannot withstand \(v < t/2\) cheaters when \(t - v - 1 \leq v\). And \(t-1\) (not the threshold \(t\)) honest participants are enough to recover all shared secrets. For example, let, \(n = 7\), \(t = 3\), \(v = 2\), where \(t - v - 1 \leq v\). According to the scheme, in the secret sharing phase, the dealer will generate \(f_a(x) = a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4\), \(f_b(x) = b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4\), \(f_c(x) = c_1 x + c_2 x^2\). These polynomials satisfy \(f_a(x) + f_b(x) + f_c(x)\). Suppose \(P_1, P_2\) are \(v=2\) heaters, and now they collude and try to recover the shared \(k=3\) secrets with the other \(3\) honest participants, say \(P_3, P_4, P_5\). In step 1 of the reconstruction phase, \(P_3, P_4, P_5\) provide their true first shadows \((x_0, f(x_0))\). While \(P_1, P_2\) supply fake first shadows. Note using the true first shadows provided by \(P_3, P_4, P_5\) together with their own true first shadows, \(P_1, P_2\) can reconstruct \(f_a(x)\) while \(P_3, P_4, P_5\) cannot. The honest participants \(P_1, P_3, P_5\) will detect the cheating behavior of \(P_1, P_2\) and reject to continue the next steps of the reconstruction phase. But, they have no means to stop the cheaters \(P_1, P_2\) from reconstructing \(f_a(x)\) since the true second shadows owned by \(P_1\) and \(P_2\) are enough to completely determine \(f_a(x) = c_1 + c_2 x^2\).

Having recovered both \(f_a(x)\) and \(f_b(x)\), all the shared secret are known to the cheaters \(P_1, P_2, P_3, P_5\). However, the honest participants \(P_1, P_3, P_5\) know nothing about the shared secrets. Also note that \(4\) honest participants are enough to recover the shared secrets. Hence the scheme is neither a \((t, n)\) threshold secret sharing scheme, nor a v-fairness secret sharing scheme.

### 4. Our New Schemes

In this section we propose two new schemes that are v-fairness \((t, n)\) multi-secret sharing schemes. In our schemes, the masked shadow denotes that the value will be used to reconstruct these secrets in the recovery phases. It is determined by both the (real) shadow selected by a participant himself and a random integer selected by the dealer. We use the Diffie-Hellman key agreement protocol[23] to generate the masked shadows in the first scheme, whereas in the second scheme, we employ the technique in the secret sharing scheme (HC scheme) of [18].

---

New Efficient and Practical v-Fairness \((t, n)\) Multi-Secret Sharing Schemes
Wenjie Yang, Futai Zhang
4.1. Scheme 1

Let $D$ be the dealer, $P=\{P_1, P_2, \ldots, P_n\}$ be a set of $n$ participants, $t<n$ be the threshold. Let $GF(p)$ be a field of prime order $p$, and $g$ a generator of $GF(p)^t$. The size of the field is determined by the security parameter. In our scheme, each secret is a bit string of length $n_s$, where $2^{n_s} \leq p$.

Let $(S_1, S_2, \ldots, S_k)$ denotes $k$ secrets selected by dealer. $ID_r \in GF(p)$ denotes the unique identity of the participant $P_r$. We also allow every participant to choose his (real) shadow by himself and to transmit it to the dealer $D$ by a public channel. Our scheme is preformed as follows:

- **Initialization Phase**
  IS1: $D$ first picks at random an integer $s_0 \in GF(p)$. He computes and publishes $R_0 = g^{s_0} \mod p$.
  IS2: Next, $D$ randomly chooses $k$ bit-strings $a_1, a_2, \ldots, a_k$ of length $n_s$ and computes $b_i = a_i \oplus S_i$, where $\oplus$ denotes the bitwise exclusive OR operation.
  IS3: Each participant $P_i$ selects at random an integer $s_i \in GF(p)$ as his own secret (real) shadow and computes $R_i = g^{s_i} \mod p$. $P_i$ transmits $(ID_i, R_i)$ to the dealer $D$ through public channels. $D$ records these information. It requires that $R_i \neq R_j$ for all $P_i \neq P_j$. Once $R_i = R_j$, $D$ should demand that these participants select their secret shadows again until all the $R_s$ are different. $D$ then publishes $\{(ID_1, R_1), (ID_2, R_2), \ldots, (ID_n, R_n)\}$.

- **Construction Phase**(by the dealer)
  CS1: Let $d_i = R_i^{s_0}$, $1 \leq i \leq n$. $D$ picks at random $k$ integers $w_j \in GF(p)$ where $w_j \not\in \{ID_i | i = 1, 2, \ldots, n\}$, $j = 1, 2, \ldots, k$. Taking $a_1, a_2, \ldots, a_k$ as integers, $D$ generates a polynomial $f_j(x)$ mod $p$ of degree $n+1$ by the Lagrange interpolation method using points $\{(w_1, a_1), (w_2, a_2), \ldots, (w_k, a_k)\}$ and points $\{(ID_1, d_1), (ID_2, d_2), \ldots, (ID_n, d_n)\}$. $D$ then randomly selects $n+k-t-v$ different integers $r_j \in GF(p)$, where $r_j \not\in \{ID_1, ID_2, \ldots, ID_n, w_1, w_2, \ldots, w_k\}$. He computes $f_j(x)$ and publishes $(r_j, f_j(r_j)), 1 \leq j \leq n+k-(t-v)$.
  CS2: Next, let $d_{j,i} = h(d_{i,j}), 1 \leq j \leq n$, where $h(x)$ denotes a secure hash function. $D$ determines a polynomial $f(x)$ with degree $n+k-1$ by the Lagrange interpolation method using $n+k$ different points $(ID_i, d_{i,j}), 1 \leq i \leq n$, and $(w_j, b_j), 1 \leq j \leq k$. Using the same way as in step CS1, $D$ computes and releases public information $(r_j, f_j(r_j))$, where $r_j \in GF(p)$ and $r_j \not\in \{ID_1, ID_2, \ldots, ID_n, w_1, w_2, \ldots, w_k\}, l = 1, 2, \ldots, n+k-t$.
  CS3: At last, $D$ computes and releases $n$ public verification values $v_l = h(d_{i,j}), 1 \leq i \leq n$.

- **Recovery and Verification Phase**(by $t$ out of $n$ participants):
  RS1: The participant $P_i$ first computes second masked shadow $d'_{2,j} = h(R_i^{s_0})$ and then checks validity of the corresponding verification value by the dealer $D$ by the following equation: $h(d_{2,j}) = v_j$. If the equation holds, release $d'_{2,j}$ and go to step RS2; Otherwise, the recovery steps stop and the participant $P_i$ makes a complaint.
  RS2: $P_i$ checks the validity of the second masked shadow supplied by $P_j$ using the following equation: $h(d'_{2,j}) = v_j, j \neq i$. If there exists at least $t$ valid masked shadows, go to step RS3. Otherwise, the recovery steps stop.
  RS3: Using at least $t$ valid second masked shadows from step RS2 and the additional $n+k-t$ public points $(r_j, f_j(r_j)), l = 1, 2, \ldots, n+k-t$, the participants can reconstruct the polynomial $f(x)$ by Lagrange interpolation method.
  RS4: The participant $P_i$ releases his first masked shadow $d'_{1,j} = R_i^{s_0}$.
  RS5: Each participant $P_i$ verifies the correctness of the first masked shadow $d'_{1,j}$ provided by $P_j$ by checking whether $h(d'_{1,j})$ is equal to the second masked shadow $d'_{2,j}$ released by $P_j$ in step RS1. As there are at most $v$ cheaters among the $t$ participants in the recovery phases, at least $(t-v)$ participants are honest. These honest participants release their true first masked shadows. Using these $(t-v)$ shadows with their corresponding $ID_s$ and the additional $n+k-(t-v)$ public points $(r_j, f_j(r_j)), 1 \leq i \leq n+k-(t-v)$, any user can reconstruct the polynomial $f(x)$ by the Lagrange interpolation...
method.

RS6: Finally, the shared secrets can be obtained using $S_j = f_i(w_j) \oplus f_i(w_j)$, $1 \leq j \leq k$.

4.2. Scheme 2

Let $D$ be the dealer, $P = \{P_1, P_2, \ldots, P_n\}$ be a set of $n$ participants, $t < n$ be the threshold. Let $GF(p)$ be a field of prime order $p$, and $g$ a generator of $GF(p)$. The size of the field is determined by the security parameter. In our scheme, each secret is a bit string of length $n$, where $2^n \leq p$. Moreover, we define notation $f(r, s)$ denotes any publicly known two-variable one-way function according to the definition in the section 2.

Here, $(S_1, S_2, \ldots, S_k)$ still denotes $k$ secrets picked by dealer. Similar to the former, each participant $P_i$ with a unique identity $ID_i \in GF(p)$ chooses his (real) shadow by himself and then transmits it to the dealer $D$ by a public channel. Then, start performing our scheme as follows:

- **Initialization Phase**
  - **IS0**: $D$ first chooses two large primes $p_1, p_2$ and computes $N = p_1 p_2$, where $N$ must be large enough so that factoring it will be computationally infeasible. Then, $D$ selects a small integer $e$ which is coprime to $\phi(N)$ and computes the integer $d$ satisfying $ed \equiv 1 \mod \phi(N)$ hold. Finally, the dealer $D$ publishes the parameters $(e, N)$.
  - **IS1**: In accordance with the parameters publicly declared by $D$, each participant $P_i$ randomly chooses a large integer $S_i \in GF(p)$ as his secret (real) shadow. The participant $P_i$ then computes and sends $c_i = s_i \mod N$ to the dealer $D$.
  - **IS2**: On receiving the ciphertext $c_i$, the dealer $D$ obtains the corresponding (real) shadows for every participant by the formula $s = c_i \mod N$ for $i = 1, 2, \ldots, n$. $D$ then records these information and meanwhile, requires that $s_i \neq s_j$ for all $i \neq j$. Once $s_i = s_j$ $(i \neq j)$, $D$ should demand those participants to repick their real shadows until $s_i$ are unique in our scheme.
  - **IS3**: Finally, $D$ randomly chooses $k$ bit-strings $a_1, a_2, \ldots, a_k$ of length $n$, and computes $b_i = a_i \oplus S_i$, where $\oplus$ denotes the bitwise exclusive OR operation.

- **Construction Phase (by the dealer)**
  - **CS1**: $D$ first picks and publishes at random an integer $e \in GF(p)$ and let $d_i = f(r, s_i)$, $1 \leq i \leq n$. Then, $D$ picks at random $k$ integers $w_j \in GF(p)$ where $w_j \notin \{ID_j\}_{j=1,2,\ldots,n}$, $j = 1, 2, \ldots, k$. Taking $a_1, a_2, \ldots, a_k$ as integers, $D$ generates a polynomial $f(x)$ mod of degree $n + k - 1$ by the Lagrange interpolation method using points $\{(w_1, a_1), (w_2, a_2), \ldots, (w_k, a_k)\}$ and points $\{(ID_1, d_1), (ID_2, d_2), \ldots, (ID_n, d_n)\}$. Finally, $D$ randomly selects $(n + k + t - v)$ different integers $r_i \in GF(p)$, where $r_i \notin \{ID_1, ID_2, \ldots, ID_n, w_1, w_2, \ldots, w_k\}$, and computes $f(x)$ and publishes $(r_i, f(r_i))$, $1 \leq i \leq n + k + t - v$.
  - **CS2**: Let $d_i = h(d_i)$, $1 \leq i \leq n$, where $h(x)$ denotes a secure hash function. $D$ determines a polynomial $f(x)$ with degree $n + k - 1$ by the Lagrange interpolation method using $n + k$ different points $(ID_i, d_i)$, $1 \leq i \leq n$, and $(w_j, b_j)$, $1 \leq j \leq k$. Using the same way as in step CS1, $D$ computes and releases public information $(r_i, f(r_i))$, where $r_i \in GF(p)$ and $r_i \notin \{ID_1, ID_2, \ldots, ID_n, w_1, w_2, \ldots, w_k\}$, $1 \leq i \leq n + k - t$.
  - **CS3**: At last, $D$ computes and releases $p$ public verification values $v_i = h(d_i)$, $1 \leq i \leq n$.

- **Recovery and Verification Phase (by $t$ out of $n$ participants):**
  - **RS1**: The participant $P_i$ first computes second masked shadow $d'_i = h(f(r, s_i))$ and then checks validity of the corresponding verification value by the dealer $D$ by the following equation: $h(d'_i) = v_i$. If the equation holds, release $d'_i$, and go to step RS2; Otherwise, the recovery steps stop and the participant $P_i$ makes a complaint.
  - **RS2**: $P_i$ checks the validity of the second masked shadow supplied by $P_j$ using the following equation: $h(d'_j) = v_j$, $j \neq i$. If there exists at least $t$ valid masked shadows, go to step RS3. Otherwise, the recovery steps stop.
  - **RS3**: Using at least $t$ valid second masked shadows from step RS2 and the additional $n + k - t$ public points $(r_j, f(r_j))$, $l = 1, 2, \ldots, n + k - t$, the participants can reconstruct the polynomial $f(x)$ by Lagrange interpolation method.
  - **RS4**: The participant $P_i$ releases his first masked shadow $d'_i = h(f(r, s_i))$.
  - **RS5**: Each participant $P_i$ verifies the correctness of the first masked shadow $d'_i$ provided by $P_j$ by
checking whether \( h(d_{1,j}) \) is equal to the second masked shadow \( d_{2,j} \) released by \( P_j \) in step RS1. As there are at most \( v \) cheaters among the \( t \) participants in the recovery phases, at least \( (t-v) \) participants are honest. These honest participants release their true first masked shadows. Using these \( (t-v) \) shadows with their corresponding IDs and the additional \( n+k-(t-v) \) public points \( (r_i, f_i(r_i)) \), \( 1 \leq i \leq n+k-(t-v) \), anyone can reconstruct the polynomial \( f_i(x) \) by the Lagrange interpolation method.

**RS6:** Finally, the shared secrets can be obtained using \( S_j = f_i(w_j) \oplus f_j(w_j), 1 \leq j \leq k. \)

5. The Security Analysis and Discussions

In this section, we show that our schemes satisfy the security requirements of a \((v, t, n)-fairness\) secret sharing scheme. That is in the recovery phase, either both the honest participants and the cheaters get the shared secrets, or both of them cannot obtain the shared secrets. In other words, even if there are \( v < t/2 \) cheaters providing incorrect masked shadows, the honest participants and the cheaters have the same probability to obtain the shared secrets. The cheaters get no advantage over the honest participants. We consider four different cases in the following.

**Analysis of security scheme 1**

**CASE1:** Assuming that all participants always release their correct masked shadows:

If all participants truly release their masked shadows \( d_{2,j} \) (i.e. \( h(R_i) \)) and \( d_{1,j} \) (i.e. \( R_i \)) in the recovery phases, the polynomial \( f_2(x) \) and \( f_1(x) \) can be recovered sequentially. Thereby these shared secrets can be obtained by any participants who want to recovery those secrets using \( S_j = f_i(w_j) \oplus f_j(w_j), 1 \leq j \leq k. \)

**CASE2:** Assuming that \( v \) or less cheaters provide incorrect second masked shadows, but the other \((t-v)\) honest participants provide correct second masked shadows:

In this case, the cheaters can obtain the polynomial \( f_2(x) \), and the honest participants cannot. However, the honest participants can know whom the cheaters are by cheater detection method in the recovery phases. Then, they stop the recovery process. Since \( v < t/2 \), the cheaters get \( n+k-(t-v)+v=n+k-t+2v < n+k \) points on \( y=f_1(x) \). So the cheaters cannot recover \((n+k-1)\)-degree polynomial \( f_1(x) \). Thus, both the cheaters and the honest participants cannot obtain the secrets.

**CASE3:** Assuming that \( v \) or less cheaters among \( t \) participants provide correct second masked shadows and incorrect first masked shadows:

In this case, the \( v \) cheaters can obtain the polynomials \( f_1(x) \) and \( f_2(x) \). Thus they have the ability to obtain the secrets \( (S_1, S_2, ..., S_k) \) by computing \( S_j = f_i(w_j) \oplus f_j(w_j), 1 \leq j \leq k. \) However, the other \((t-v)\) honest participants can also obtain the secrets. Using cheater detection method in the recovery phases, they can find out the correct \((t-v)\) first masked shadows published by the honest participants. Then, they can recover the \((n+k-1)\)-degree polynomial \( f_1(x) \) with those true shadows and the corresponding public information using Lagrange interpolation method. So, the honest participants can also reconstruct the polynomials \( f_1(x) \) and \( f_2(x) \). Hence, the \((t-v)\) honest participants can also obtain the secrets \( (S_1, S_2, ..., S_k) \).

**CASE4:** Assuming that the dealer publishes some of the inconsistent public information, e.g. some invalid \( (r_i, f_i(r_i)) \), or some invalid \( (r_j, f_j(r_j)) \):

In this case, both the honest participants and the cheaters cannot obtain the correct polynomials \( f_1(x) \) or \( f_2(x) \). In other word, all of the participants are cheated by the dealer. We think this kind of cheating is pointless as no participants can ever recover the right secrets.

**Analysis of security scheme 2**

The security of scheme 2 can be analyzed in the same way.

Note that in both of our new schemes, no information about the real shadow of a participant is leaked in the recovery phase. A participant \( P_j \) just need to release the masked shadows \( d_{1,j} \) (and \( d_{2,j} = h(d_{1,j}) \)) in order to recover the secrets in the verification and recovery phases. Meanwhile, in scheme 1, the secret masked shadow \( d_{1,j} \) is computed by formula \( d_{1,j} = R_i \mod N \). Hence, the security of the real shadow \( s_i \) in this scheme is based on the difficulty of discrete logarithm problem. In scheme 2, the masked shadow \( d_{1,j} \) is computed by formula \( d_{1,j} = f(r, s_i) \). Thus, the security of the real shadow \( s_i \) in this
scheme is based on the properties of the two-variable one-way function \( f(r, s_i) \) [11]. So even those shared secrets have been reconstructed, the confidentiality of the real shadows does not compromised.

5. Performance Analysis and Discussions

- Comparing with some traditional multi-secret sharing schemes, our schemes enjoy the following extra properties:
  1. In our schemes, because every participant \( P_i \) chooses the secret shadows \( s_i \) and computes \( d_{1,i} \) and \( d_{2,i} \) by her/himself, it is impossible for the dealer to cheat any participant.
  2. As shown in Table 1, our new schemes are more efficient in computation. In the comparison, we only consider the cost of modular exponentiation, since other operation's computational cost can be ignored compared with modular exponentiation.
  3. Each participant \( P_i \) can easily and quickly verify the validity of his masked shadows \( d_2',i \) and \( d_1',i \) by checking whether \( v_i = h(d_2',i) \) and \( d_2',i = h(d_1',i) \).
  4. In our proposed schemes, if there are \( v < t/2 \) dishonest participants (cheaters), all participants still have equal probability to recover the shared secrets. The dishonest participants cannot get any advantage over the honest ones.

- Comparing with the other two fair secret sharing schemes very recently proposed:

<table>
<thead>
<tr>
<th>Scheme vs. Performance</th>
<th>Lee et al.'s Scheme[16]</th>
<th>Jen-Ho Yang al.'s Scheme[17]</th>
<th>Our new schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of shadows held by each participant</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Public channel</td>
<td>( N )</td>
<td>( N )</td>
<td>( Y )</td>
</tr>
<tr>
<td>Reusability of the shadow</td>
<td>( N )</td>
<td>( N )</td>
<td>( Y )</td>
</tr>
<tr>
<td>Multi-secret sharing</td>
<td>( N )</td>
<td>( Y )</td>
<td>( Y )</td>
</tr>
<tr>
<td>Computational complexity</td>
<td>Lower</td>
<td>Lower</td>
<td>Higher</td>
</tr>
</tbody>
</table>

Table 2 is a brief performance comparison of our schemes with the other two fair secret sharing schemes that were proposed very recently. Although the computational cost of our schemes are relatively high, they enjoy some preferable features such as good security, fairness, no need for private channels, a small number of secret shadows, reusable of secret shadows, and multi-secret sharing. None of the other two fair secret sharing schemes enjoys all these good features.

6. Conclusion

In this paper, we analyze and point out some security weaknesses in an existing \( v \)-fairness \((t, n)\) multi-secret sharing scheme. After that, we propose two new efficient and practical \( v \)-fairness \((t, n)\) multi-secret sharing schemes. Compared with the traditional multi-secret sharing schemes without fairness property, our schemes are not only efficient and practical in real environment, but also ensure that cheaters can get no advantage over the honest participants in the recovery phase assuming there are...
v< t/2 cheaters. While compared with some existing fair secret sharing schemes, although our schemes have a higher computational cost, they enjoy some preferable features such as good security, fairness, no need for private channels, a small number of secret shadows, reusable of secret shadows, and multi-secret sharing. The security analysis and performance comparisons indicate that our new schemes may have practical applications for sharing multiple secrets simultaneously where the fairness is a great concern and the private channels between participants and the dealer are hard to establish.

Acknowledgement

This work is supported by National Natural Science Foundation of China (No.61170298), Natural Science Foundation of Jiangsu Province (No.BK2011101).

References