1998 International Computer Symposium
Workshop on Cryptology and Information Security
December 17-19, 1998, N.C.K.U., Tainan, Taiwan, R.O.C.

EFFICIENT CHEATER IDENTIFICATION IN SEQUENTIAL SECRET SHARING SCHEMES

Chin-Laung Lei and Cheng-Tsung Cho

Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
E-mail: lei@cc.ee.ntu.edu.tw

ABSTRACT

In this paper we propose two efficient secret sharing schemes with cheater identification based on the sequential model. Our schemes greatly reduce the amount of data kept by the participants as well as the data transmitted by the dealer. In our schemes, the dealer only has to send $O(n)$ data instead of $O(n^2m)$ for the existing schemes in the literature, where n is the number of participants and m is the number of rounds of the sequential model. Moreover, only one shadow is kept by each participant in our schemes without the need of any checking parameters while $O(m)$ shadows and $O(nm)$ checking parameters are needed for each participant in the previous schemes.

1. INTRODUCTION

A secret sharing scheme is a method of hiding a secret by a dealer among several shadows such that the secret can be reconstructed by some subsets, called access structure, of these shadows. Secret sharing schemes are mainly used to protect a secret from being lost, destroyed or abused. In 1979, Shamir [11] first proposed a (t,n)-threshold scheme which is an algorithm to divide secret into n shadows, such that the secret can be recovered by any group of t or more participants.

Shamir's (t,n)-threshold scheme uses a polynomial, whose degree is $t-1$, to share the secret. The dealer sets the constant term of the polynomial to be the true secret and then he computes n distinct points which are all on the polynomial. Each participant receives only one point of the polynomial from the dealer. Surely the participants hold different points. If any t participants want to derive the secret, they can use their shadows to derive the polynomial, for its degree is $t-1$.

Since a cheater may derive the true secret and preclude others from reconstructing the secret, cheater detection and identification are of crucial importance in secret sharing schemes. In 1989, Rabin and Ben-Or* [9] proposed a method of checking vector for secret sharing. Their method requires that all participants keep a lot of data to achieve cheater identification. Although a cheater can be identified with high probability, the cheater has already obtained the secret while the honest participants did not. This is unfair, so Tompa and Woll [14] proposed a sequential model in 1986. Lin and Harn [8] improved this sequential scheme in 1995. In [8], the dealer hides the secret S in a sequence, D_1, $D_2,\ldots, D_j, D_{j+1}, \ldots, D_k$, where $D_j=S$ for some j chosen randomly and privately. $D_{j+1}=P$, P is public information, and D_i is a dummy secret for all $i \neq j$ and $i \neq j+1$. Each D_i is a secret in the ith round, and they will be recovered in order. They use Rabin's checking vector to verify the validity of each shadow in each round. If all shadows are correct in the ith round, then the derived D_i is valid and all the cooperative participants continue to derive the next secret D_{i+1}. If any shadow is invalid, the reconstruction stops. When the derived secret D_i equals the public information P, the true secret is the one derived in the previous round, i.e., $S= D_{i-1}$.

In a k-round sequential model, cheaters only have probability about $1/k$ to be

successful, because they do not know in which round the true secret is hidden.

In 1997, Laih and Lee proposed a new sequential model that can compensate all honest participants when the number of cheaters is less than $t/2$ [6].

In 1991, Lin and Harn proposed a secret sharing scheme for general access structures [7]. In a general access structure scheme, the secret can only be recovered by some groups of specified participants (access structure). Unlike the threshold scheme, the access structure scheme is not depend on the number of participants.

In this paper, we present two efficient cheater identification schemes based on the sequential model. In our schemes, the data kept by the participants and delivered by the dealer are greatly reduced, and the checking vectors are eliminated.

The remainder of this paper is organized as follows. In section 2, we review the Rabin's checking vector scheme and the sequential model scheme proposed by Laih and Lee. In section 3, we present our efficient cheater identification schemes. The analysis of our proposed schemes is given in section 4. Finally, a concluding remark is given in section 5.

2. PRELIMINARY

2.1 Rabin's Checking Vector Scheme

Cheater identification is an important issue in a secret sharing scheme. If there is no cheater identification feature in a secret sharing scheme, then the cheater can cheat the other participants without being nabbed. We will discuss the checking vector scheme proposed by Rabin and Ben-Or* [9].

There are n participants $P_1, P_2, \ldots, P_n$ in this scheme, and a dealer uses a secret sharing scheme to construct the shadows $f(P_1), f(P_2), \ldots, f(P_n)$ for the participants.

The initialization phase

1. For each shadow $f(P_i)$ the dealer chooses $2(n-1)$ random numbers b_{ji}, $c_{ji}, 1 \le j \le n; j \ne i$, secretly.
2. For each i the dealer computes $n-1$ numbers $y_{ji}, 1 \le j \le n; j \ne i$, such that $f(P_i)+b_{ji}y_{ji} = c_{ji}$.
3. The dealer delivers $f(P_i)$ and $y_{ji}, 1 \le j \le n; j \ne i$, to P_i through a secure channel.
4. The dealer delivers b_{ji}, $c_{ji}, 1 \le j \le n; j \ne i$, to P_j through a secure channel.

The recovering phase

1. All cooperative participants pool their shadows to recover the secret. Participant P_i reveals his shadow $f(P_i)$ and publishes his own checking vector y_{ji}.
2. Participant P_j uses his checking vectors b_{ji} and c_{ji} to verify P_i's shadow $f(P_i)$. They must satisfy equation $f(P_i)+b_{ji}y_{ji}=c_{ji}$. Otherwise, P_i is cheating.
3. If all shadows are valid, the secret can be derived. □

In this protocol, all participants need to keep a large amount of checking vectors, and the dealer has to send them through a secure channel. It is intractable for a cheater to make a fake shadow which can successfully pass through all the checking-vector validation processes without being caught.

2.2 Laih and Lee's Sequential Model

A secret sharing scheme is said to be V-fair provided that the honest participants can also reconstruct the secret when the cheaters can derive the secret.

In 1997, Laih and Lee proposed a V-fairness (t, n) secret sharing scheme [6], where the number of cheaters V is less than that of the honest participants. In this scheme, participants are not required to release their shadows simultaneously while reconstructing a secret.

The initialization phase

1. The dealer uses Shamir's (2,3)-threshold scheme to encode the true secret K into three subsecrets k_1, k_2, and k_3.
2. The dealer randomly chooses and publishes a number P.
3. The dealer determines a number m

such that there are m rounds in the scheme.

4. The dealer randomly selects a number r secretly, $1 \le r \le m-2$. Let $S_{r-1}=k_1$、$S_r=k_2$、$S_{r+1}=P$ and $S_{r+2}=k_3$.
5. S_1, S_2, S_j, ...,S_{r-2} and S_{r+3}, S_{r+4}, ...,S_m are random numbers selected by the dealer secretly and are used as dummy secrets for their corresponding rounds.
6. The dealer uses Shamir's (t,n)-threshold scheme to divide S_j, $1 \le j \le m; j \ne r+2$, into n shadows and delivers them to all participants through a secure channel.
7. The dealer uses Shamir's $(t\text{-}V,n)$-threshold scheme to divide S_{r+2} into n shadows and delivers them to all participants through a secure channel.

The recovering phase

1. All cooperative participants pool their shadows to recover the secret of the jth round, S_j, sequentially. If there is no cheater, S_j can be derived.
2. If $S_j=P$, then $S_{j-1}=k_2$ and $S_{j-2}=k_1$. The true secret K can be recovered by the subsecrets k_1 and k_2 using Shamir's (2,3)-threshold scheme.
3. If there is any cheater, stop the whole recovering phase right now. □

This protocol is fair when the number of cheaters is less than the number of honest participants. If the cheaters release their fake shadows in the rth round, then the cheaters are able to derive the subsecret k_2 while the honest ones can not. In other words, the cheaters can derive the true secret using k_1 and k_2 while the honest participants can not derive it at this time. However the honest participants can go on to derive the subsecret k_3 hidden in the $(r+2)$th round, and then recover the true secret K using k_1 and k_3. Recall that the $(r+2)$th round is a $(t\text{-}V, n)$-threshold scheme.

3. THE EFFICIENT CHEATER IDENTIFICATION SCHEMES

In this section, we present two efficient cheater identification schemes. The cheater identification in our schemes is based on a one-way hash function. In our schemes, each participant keeps only one shadow without the need of any checking vectors. One of our schemes is a pure threshold scheme and the other allows the combination of both threshold and general access structures.

3.1 The Threshold Scheme

In this section we present a scheme based on Shamir's (t,n)-threshold scheme. There are n participants sharing a secret K and if any group of t or more participants cooperate together, they can derive the secret. In this scheme, we assume that there are at most V cheaters, where V can be any nonnegative integer less than $t/2$.

Our scheme consists of two phases: (1) initialization, (2) recovering. In the initialization phase, the dealer hides the secret and generates the shadows. The dealer also computes the corrective parameters and publishes the necessary information. In the recovering phase, all the cooperative participants derive the secret and identify cheaters if necessary.

The initialization phase

1. The dealer uses Shamir's (2,3)-threshold scheme to encode the true secret K into three subsecrets k_1, k_2, and k_3.
2. The dealer randomly selects numbers d_i, $c_{1,j}$, $c_{2,j}$, and $c_{3,k}$, where $0 \le i < t, 1 \le j < t, 1 \le k < t-V$, secretly. Then the dealer constructs the following polynomials
$$f_1(x)= c_{1,t-1}x^{t-1}+\ldots+c_{1,1}x+k_1$$
$$f_2(x)= c_{2,t-1}x^{t-1}+\ldots+c_{2,1}x+k_2$$
$$f_3(x)=c_{3,t-V-1}x^{t-V-1}+\ldots+c_{3,1}x+k_3$$
$$g(x)= d_{t-1}x^{t-1}+\ldots+d_1x+d_0$$
3. The dealer chooses a number m where m is the number of rounds in this scheme. The dealer also selects and publishes a one-way hash function $h(x)$. We define $h^{(k)}(x)=h(h^{(k-1)}(x))$ for $k \ge 1$ and $h^{(0)}(x)=x$.
4. The dealer randomly chooses n different numbers R_i, $1 \le i \le n$, and computes $K_{i,j} = h^{(m-j)}(R_i)$, $0 \le j < m$, such that all the $K_{i,j}$'s are distinct. The dealer delivers the shadow R_i to P_i through a secure channel. P_i knows

$K_{i,j}$, $0 \le j < m$, which can be computed from R_i using the hash function.

5. The dealer randomly selects a number r from $\{1, 2, ..., m-2\}$ secretly, and for each i, $1 \le i \le n$, computes and publishes.
   $D_i^{(s1)} = f_1(P_i) - K_{i,r-1}$,
   $D_i^{(s2)} = f_2(P_i) - K_{i,r}$,
   $D_i^{(s3)} = f_3(P_i) - K_{i,r+2}$, and
   $D_i^{(p)} = g(P_i) - K_{i,r+1}$

Also, the dealer publishes $h(g(0))$ and $K_{i,0} = h^{(m)}(R_i)$, $1 \le i \le n$.

The recovering phase

Suppose there is a group of t participants who are going to recover the secret. Without loss of generality, we can assume that these t cooperative participants are P_1 through P_t. In the recovering phase, P_i's, $1 \le i \le t$, pool their corresponding shadows in each round sequentially. P_i reveals his shadow $K_{i,j}$ in the jth round.

1. In the jth round, if $h(K_{i,j}) \neq K_{i,j-1}$, then P_i is a cheater and the cooperative participants stop the whole recovering phase immediately. If $h(K_{i,j}) = K_{i,j-1}$, P_i is regarded as honest.
2. If there is no cheater in the jth round, a $t-1$ degree polynomial $g_j(x)$ is derived by the t points $(P_i, K_{i,j} + D_i^{(p)})$, $1 \le i \le t$.
3. If $h(g_j(0)) = h(g(0))$, then we believe $j = r+1$ and compute the polynomial $f_1(x)$ using the t points $(P_i, K_{i,j-2} + D_i^{(s1)})$ and polynomial $f_2(x)$ using the t points $(P_i, K_{i,j-1} + D_i^{(s2)})$, $1 \le i \le t$.
4. The true secret K can be derived by subsecrets $k_1 = f_1(0)$ and $k_2 = f_2(0)$ using Shamir's (2,3)-threshold scheme. □

We use a one-way hash function $h(x)$ in our scheme. It can reduce the amount of secret data kept by each participant. The dealer also delivers fewer data, only a random number R_i, than the existing schemes in the literature.

Although we use $h(x)$ to generate all shadows, the corrective parameters $D_i^{(*)}$ can help us to go back to Shamir's scheme. So this is also a threshold scheme.

We use the function $g(x)$ to determine the position of the three subsecrets k_1, k_2, and k_3. In the jth round, all the cooperative participants only need to compute one polynomial $g_j(x)$ whose constant term is used to check if the round that hides the subsecret has reached.

Our cheater identification scheme is quite efficient, because the one-way hash function $h(x)$ can be used to identify cheaters quickly without the need for the participants to hold any checking vectors.

If there are V cheaters release their fake shadows in the rth round, then the cheaters are able to derive the subsecret k_2 while the honest ones can not. However the honest participants can compute the polynomial $f_3(x)$ using the $t-V$ points $(P_i, K_{i,j+2} + D_i^{(s3)})$. The subsecret $k_3 = f_3(0)$ will be derived and the true secret K can be recovered by using k_1 and k_3. Since the $(r+2)$th round is a $(t-V, n)$-threshold scheme.

3.2 The General Secret Sharing Scheme

In this section, we present a secret sharing scheme to deal with general access structures. We assume that the secret value is K and there are n participants.

Our scheme consists of two phases: (1) initialization, (2) recovering. In the initialization phase, the dealer hides the secret, generates the shadows, computes and publishes the corrective parameters. In the recovering phase, all the cooperative participants identify cheaters and derive the secret.

The initialization phase

1. The dealer chooses a number m where m is the number of rounds in this scheme. The dealer also selects and publishes a one-way hash function $h(x)$. Let Γ be the set of all access structures. The set of minimal access structures, denoted by Γ_{min}, is defined as $\Gamma_{min} \equiv \{A \mid A \in \Gamma \text{ and } \forall B \in \Gamma, B \not\subset A\}$
2. The dealer randomly chooses n different numbers R_i, $1 \le i \le n$, and

computes $K_{i,j}=h^{(m-j)}(R_i)$, $0 \le j < m$, such that all the $K_{i,j}$ are distinct. The dealer delivers R_i to P_i through a secure channel. P_i knows the shadows $K_{i,j}$, $0 \le j < m$, which can be computed from R_i using the hash function $h(x)$.

3. The dealer randomly selects a number r from $\{1, 2, \ldots, m-1\}$ secretly.
4. For each access structure $A_i \in \Gamma_{min}$ the dealer computes and publishes two corrective parameters
   $C_i^{(s)} = K - h(\sum_{\forall P_j \notin A_i} K_{j,r})$, and
   $C_i^{(s+1)} = h(\sum_{\forall P_j \notin A_i} K_{j,r+1})$.
5. The dealer publishes $K_{i,0}=h^{(m)}(R_i)$, $1 \le i \le n$.

The recovering phase

Suppose the members of a minimal access structure $A \in \Gamma_{min}$ are going to recover the secret. The members $P_i \in A$ pool their corresponding shadows in each round sequentially. P_i reveals his shadow $K_{i,j}$ in the jth round.

1. In the jth round, if $h(K_{i,j}) \neq K_{i,j-1}$, then P_i is a cheater and the cooperative participants stop the whole recovering phase right away. If $h(K_{i,j})=K_{i,j-1}$, we believe P_i is honest.
2. If there is no cheater in the jth round, they can compute $h(\sum_{\forall P_i \in A} K_{i,j})$. And if $h(\sum_{\forall P_i \in A} K_{i,j}) = C_1^{(s+1)}$, the true secret can be recovered by the formula $K = h(\sum_{\forall P_i \in A} K_{i,j-1}) + C_1^{(s)}$. □

In this scheme, we use a one-way hash function $h(x)$ to generate all shadows. Each participant only has to keep a random number R_i. The corrective parameters $C_1^{(s)}$ are used to rectify the shadows so that the true secret can be derived. Employing the same compensable method as the previous section, honest participants can also compute the secret when the cheaters deceive them and derive the secret.

Most of the existing schemes in the literatures have the property that if there are N access structures and m rounds, each participant needs to store $O(Nm)$ shadows. Although there are some schemes needing only $O(m)$ shadows for each participant, they demand much more computation time instead. In our scheme, each participant only has to keep one shadow and requires less computation time due to the relative efficiency of hashing functions.

3.3 The Partial Threshold Scheme

In the real world, secret sharing schemes are not always pure threshold. For example, consider a company with 5 departments and 1000 employees (including the president and the 5 department managers). The company would like to use a secret sharing scheme such that the president and managers have higher authority than other staffs. Their blueprint is that all staffs, including the president and managers, employ a (500,1000)-threshold scheme, but the president and the managers can also derive the secret without other employees.

Our scheme in section 3.1 can not deal with this situation since it is not a pure threshold scheme. Direct application of the scheme of section 3.2 is possible, but it will result in too many access structures. In the above case, it will result in about $\binom{1000}{500}$ access structures, which is impractical. Fortunately, we can combine the schemes in section 3.1 and 3.2 to solve this problem efficiently. We call the combined scheme a *Partial Threshold Secret Sharing Scheme.*

First, the initialization phase is the same as that of section 3.1 to treat the threshold part. For the particular access structures, the combination of president and/or managers, can be dealt with the initialization phase described in section 3.2. We must emphasize that only one hash function is required and all participants only hold a random number because the shadow generation can be merged. The single shadow held by the president and managers has two functionalities.

Our *Partial Threshold Secret Sharing Scheme* still possesses the efficiency advantages of both schemes in 3.1 and 3.2. The dealer only has to send a random number to each participant and no checking vectors are required for the participant. We illustrate this scheme by the following example

	$K_{i,0}$	$K_{1,1}$	$K_{i,2}$	$K_{1,3}$	$K_{i,4}$	$K_{i,5}$	$K_{i,6}$	$K_{i,7}$
P_1	52	18	36	8	72	58	51	2
P_2	13	74	73	4	22	42	62	48
P_3	31	76	32	16	44	14	69	45
P_4	26	46	24	65	30	77	11	70
P_5	66	35	53	7	19	10	6	43

Table 1. Shadows for each participant.

	$D_1^{(s1)}=f_1(P_i)-K_{i,3}$	$D_1^{(s2)}=f_2(P_1)-K_{1,4}$	$D_1^{(s3)}=f_3(P_i)-K_{i,6}$	$D_1^{(p)}=g(P_i)-K_{i,5}$
P_1	52	67	13	28
P_2	68	46	10	48
P_3	72	34	11	3
P_4	43	60	77	27
P_5	46	6	11	25

Table 2. Corrective parameters.

Example: Suppose a dealer intend to share a secret K=50 among five participants, P_1, P_2, P_3, P_4, and P_5, such that P_1 and P_2 or any group of 3 or more participants can derive the secret K.

For simplicity, we assume that the hash function $h(x)= 29^x \ (mod\ 79)$ is a secure hash function. Our scheme proceeds as follows:

The initialization phase

1. The dealer uses Shamir's (2,3)-threshold scheme to encode the true secret 50 into three subsecrets, they are 52, 54, and 56.
2. The dealer selects four polynomials, they are
   $f_1(x)=2x^2+6x+52$
   $f_2(x)=x^2+5x+54$
   $f_3(x)=8x+56$
   $g(x)=x^2+x+5$.
3. The dealer chooses m=7, there are 7 round, and publishes the hash function $h(x)= 29^x \ (mod\ 79)$ and $h(g(0))=h(5)=63$.
4. The dealer chooses $R_1=2$, $R_2=48$, $R_3=45$, $R_4=70$, and $R_5=43$ and sends R_i to P_i through a secure channel. The dealer publishes $K_{i,0}$. We list the shadows in Table 1
5. The dealer computes and publishes
   $D_i^{(s1)}=f_1(P_i)-K_{i,3}$
   $D_i^{(s2)}=f_2(P_i)-K_{i,4}$
   $D_i^{(s3)}=f_3(P_i)-K_{i,6}$
   $D_i^{(p)}=g(P_i)-K_{i,5}$
   Where the value $P_i=i$. We list these parameters in Table 2.
6. The dealer computes the corrective parameters of P_1 and P_2, that is $C_i^{(s)}=50 - h(72+22) = 50-12 = 38$ and publishes $C_i^{(s)}=38$.
7. The dealer computes and publishes $C_i^{(s+1)}=h(58+42)=h(21)=41$. □

The recovering phase

We will show how to recover the secret on the (3,5)-threshold condition first, and then show how P_1 and P_2 recover the secret together.

(Threshold Part)

Without loss of generality, we assume P_3, P_4, and P_5 cooperate to recover the secret.

1. They pool their shadows $K_{i,1}$ (i=3,4,5) and check if $h(K_{i,1})= K_{i,0}$. If there is no cheater, pool their shadows $K_{i,2}$ and identify cheaters again.
2. They use three points $(3,K_{3,2}+D_3^{(p)}) = (3,35)$, $(4, K_{4,2}+D_4^{(p)}) = (4,51)$, and $(5,K_{5,2}+D_5^{(p)})=(5,78)$ to derive the polynomial $g_2(x) = 45x^2+17x+53$. $h(53) = 35 \neq 63$, so they must pool their $K_{i,3}$ (i=3,4,5).
3. In the 3rd round, if there is no cheater, they use three points $(3,K_{3,3}+D_3^{(p)}) =$

(3,19), $(4,K_{4,3}+D_4^{(p)})$ = (4,13), and $(5,K_{5,3}+D_5^{(p)})$ = (5,32) to derive the polynomial $g_3(x) = 52x^2+25x+29$. $h(29) = 54 \neq 63$, so they must pool their $K_{i,4}$ $(i=3,4,5)$.

4. In the 4th round, if there is no cheater, they use three points $(3,K_{3,4}+D_3^{(p)})$ = (3,47), $(4,K_{4,4}+D_4^{(p)})$ = (4,57), and $(5,K_{5,4}+D_5^{(p)})$ = (5,44) to derive the polynomial $g_4(x) = 28x^2+51x+37$. $h(37) = 48 \neq 63$, so they must pool their $K_{i,5}$ $(i=3,4,5)$.
5. In the 5th round, if there is no cheater, they use three points $(3,K_{3,5}+D_3^{(p)})$ = (3,17), $(4,K_{4,5}+D_4^{(p)})$ = (4,25), and $(5,K_{5,5}+D_5^{(p)})$ = (5,35) to derive the polynomial $g_4(x)= x^2+x+5$. $h(5)=63$, so the secret can be derived.
6. They use three points $(3,D_3^{(s1)}+K_{3,3})$, $(4,D_4^{(s1)}+K_{4,3})$, and $(5,D_5^{(s1)}+K_{5,3})$ to derive $f_1(x)=2x^2+6x+52$ and use three points $(3,D_3^{(s2)}+K_{3,4})$, $(4,D_4^{(s2)}+K_{4,4})$, and $(5,D_5^{(s2)}+K_{5,4})$ to derive $f_2(x) = x^2+5x+54$. Then they can use two points (1,52) and (2,54) to recover the true secret 50.

(Access Structure Part)

1. P_1 and P_2 cooperate to recover the secret. In the first two rounds, they pool their shadows and identify cheat. Then they compute $h(K_{1,2}+ K_{2,2}) = h(30) = 65 \neq 41$, so they must pool their shadows $K_{1,3}$ and $K_{2,3}$.
2. In the 3rd round, if there is no cheater, they compute $h(K_{1,3}+ K_{2,3}) = h(12) = 21 \neq 41$, so they must pool their shadows $K_{1,4}$ and $K_{2,4}$.
3. In the 4th round, if there is no cheater, they compute $h(K_{1,4} + K_{2,4}) = h(15) = 12 \neq 41$, so they must pool their shadows $K_{1,5}$ and $K_{2,5}$.
4. In the 5th round, if there is no cheater, they compute $h(K_{1,5}+ K_{2,5}) = h(58+42) = h(21)=41= C_i^{(s+1)}$, so the secret can be derived.
5. The true secret is $C_i^{(s)}+ h(K_{1,4}+ K_{2,4}) = 38+12 = 50$.

4. ANALYSIS

Our proposed scheme employs a one-way hash function to identify cheaters. All participants no longer need to hold any checking vector or parameters. The risk of data loss is reduced because the dealer only has to send a random number to each participant.

If a cheater intends to cheat in our scheme, the only chance he can succeed is to guess the right position where the true secret is hidden. Thus, the probability of cheating successfully in our scheme is $1/m$ which is the same as the schemes in [6, 8, 14].

Table 3 summarizes the comparisons of some complexity measures between our schemes and the schemes in [6, 14]. Where n is the number of participants, m is the number of rounds for the sequential model and N is the number of minimal access structures.

The first column of Table 3 shows the number of shadows kept by each participant. In [6, 14], each participant has to keep a different shadow for each round, therefore $O(m)$ shadows are needed. While in our schemes, only a single shadow is required and other checking parameters can be derived from the shadow by a hash function.

The second column of Table 3 shows the number of checking vectors kept by each participant. In [6, 14], each participant has to keep n different checking vectors for each round, therefore $O(nm)$ checking vectors are needed. While in our schemes, no checking vectors are required.

The third column of Table 3 shows the amount of the data sent by the dealer to participants. In [6, 14], the dealer has to send $O(n^2)$ different checking vectors for each round, and $O(n^2m)$ checking vectors are needed. While in our schemes, the dealer only has to send a random number to each participant through a secure channel. Because there are n participants, the dealer only sends $O(n)$ shadows.

The fourth column of Table 3 shows the amount of data published by the dealer. In [6, 14], the dealer has to publish $O(1)$ information that is used to find the position of the subsecrets. While in our schemes, the dealer need to publish $O(n)$ corrective parameters.

	The shadows held by one participant	The checking vectors held by one participant	The data sent by the dealer to participants	The data published by the dealer
Previous scheme (Threshold)	$O(m)$	$O(nm)$	$O(n^2m)$	$O(1)$
Our scheme (Threshold)	1	0	$O(n)$	$O(n)$
Our scheme (Partial Threshold)	1	0	$O(n)$	$O(n)+O(N)$

n is the number of participants.

m is the number of rounds.

N is the number of minimal access structures.

Table 3 Comparisons of storage and communication complexities

5. CONCLUSIONS

Cheater identification is an important issue in secret sharing schemes. In this paper, we have proposed two efficient cheater identification schemes. One is a threshold scheme, and the other is a general secret sharing scheme, which can handle the combination of general access structures and threshold schemes efficiently.

Our schemes are based on the sequential model and greatly reduce the amount of data kept by the participants. Moreover, only $O(1)$ shadows are kept by each participant in our schemes without the need of any checking parameters while $O(m)$ shadows and $O(nm)$ checking parameters are needed for each participant in the previous schemes.

6. REFERENCES

1. E. F. Brickell and D. R. Stinson, "*The Detection of Cheaters in Threshold Schemes,*" CRYPTO'88, pp. 564-577, 1988.
2. M. Carpentieri, "*A Perfect Threshold Secret Sharing Scheme to Identify Cheaters,*" Designs, Codes and Cryptography, Vol. 5, pp. 183–187, 1995.
3. C. C. Chang and R. J. Hwang, "*Efficient Cheater Identification Method for Threshold Schemes,*" IEE Proc.-Comput. Digit. Tech. **144**(1), pp. 23-27, 1997.
4. S. J. Hwang and C. C. Chang, "*A Dynamic Secret Sharing Scheme with Cheater Detection,*" Information Security and Privacy, pp. 48-55, 1996.
5. C. S. Laih and L. Harn, "*Generalized Threshold Cryptosystems,*" Asiacrypt'91, pp. 159-166, 1991.
6. C. S. Laih and Y. C. Lee, "*V-Fairness (t,n) Secret Sharing Scheme,*" IEE Proc-Comput. Digit. Tech. **144**(4), pp. 245-248, 1997.
7. H. Y. Lin and L. Harn, "*A Generalized Secret Sharing Scheme with Cheater Detection,*" ASIACRYPTO'91, pp. 149-158, 1991.
8. H. Y. Lin and L. Harn, "*Fair Reconstruction of A Secret,*" Information Processing Letters 55(1), pp. 45-47, 1995.
9. T. Rabin and M. Ben-Or*, "*Verifiable Secret Sharing and Multiparty Protocols with Honest Majority,*" Proceedings of the 21st Annual ACM Symposium on theory of computing, pp. 73-85, 1989.
10. J. Rifa-Coma, "*How to Avoid the Cheaters Succeeding in the Key Sharing Scheme,*" Designs, Codes and Cryptography, Vol.3, pp. 221-228, 1993.
11. A. Shamir, "*How to Share a Secret*" Comm. ACM, Vol. 22, pp. 612-613, 1979.
12. G. J. Simmons, "*Contemporary Cryptology — The Science of Information Integrity,*" The Institute of Electrical and Electronics Engineers, Inc., 1992.
13. H. M. Sun and S. P. Shieh, "*Construction of Dynamic Threshold Schemes,*" Electronics Letters, 24th, Vol.30, No.24, pp. 2023-2025, 1994.
14. M. Tompa and H. Woll, "*How to Share a Secret with Cheaters,*" CRYPTO'86, pp. 261-265.
15. T. C. Wu and T. S. Wu, "*Cheating Detection and Cheater Identification in Secret Sharing Schemes,*" IEE Proc.-Comput. Digit. Tech. 142(5), pp. 367-369, 1995.