PAPER

On the Practical Secret Sharing Scheme

Wakaha OGATA[†a)], *Member*

SUMMARY In this paper, we attempt to construct practical secret sharing schemes, which scheme has smaller share size and can detect cheating with high probability. We define two secure ramp schemes, secure ramp scheme and strongly secure ramp scheme. Then, we propose two constructions of secure ramp scheme. These schemes both have small share size and the cheating can be detected with high probability. So, they are practical secret sharing schemes.

key words: *secret sharing scheme, ramp scheme, cheating of participant, share size*

1. Introduction

Secret sharing schemes permit a secret to be shared by participants in such a way that only qualified subsets of participants (access subset) can recover the secret. Secret sharing schemes are useful in the management of cryptographic keys, in multiparty protocols, and etc.

Perfect secret sharing schemes (PSS) have been studied extensively so far. In a perfect secret sharing scheme, any subset of participants is an access subset or a non-access subset that has absolutely no information on the secret. No subsets are allowed in between.

Blakley [1] and Shamir [2] introduced (k, n)-threshold secret sharing schemes independently. In such a scheme, the access subsets are all the subsets whose cardinality is more than $k-1$. The most important issue of secret sharing schemes is the size of shares owned by the participants. For any PSS, it is known that [3], [4]

$$|\mathcal{V}_i| \geq |\mathcal{S}|,$$

where $|\mathcal{S}|$ denotes the size of the secret and $|\mathcal{V}_i|$ denotes the size of the share of participant P_i. Therefore, schemes which can achieve

$$|\mathcal{V}_i| < |\mathcal{S}|$$

must be "nonperfect", where semi-access subsets should be allowed. A semi-access subset is a set of participants who can have some information on the secret but cannot recover the secret completely. (d, k, n)-ramp schemes [5], which is an extension of (k, n)-threshold schemes, are such an example. In this scheme, subsets whose cardinality is more than $k-1$ are access subsets and subsets of at most $k-d$ participants are non-access subset.

On the other hands, Tompa and Woll [6] considered the cheating of participants when the secret is reconstructed. For example, Shamir's scheme allows any participant to open forge share. For this problem, some researchers showed threshold secret sharing schemes secure against cheating. However, such scheme needs larger shares than the secret. When $1-\delta$ is a probability of detection of cheating, it is shown that [7]

$$|\mathcal{V}_i| \geq (|\mathcal{S}|-1)/\delta + 1.$$

So secure threshold schemes are not practical.

In this paper, we attempt to construct practical secret sharing schemes, which has smaller share and can detect cheating with high probability. First, we claim there are two situations where ramp schemes are used. Suppose that the dealer knows an adversary can corrupt at most c participants. In this case, the dealer, who wants not to leak any information about the secret to the adversary, can use $(c+d, d, n)$-ramp scheme for some d. However, the dealer often can not guess c correctly in practical case. In such a case, the dealer chooses k large enough, distributes the secret using (k, d, n)-ramp scheme for some d, and hopes an adversary will not corrupt $k-d+1$ or more participants.

Next, we consider an scenario in which an adversary corrupts some participants and opens forged shares to cheat honest one and define two secure ramp schemes. The first scheme is suitable to apply in former situation mentioned above, since it is considered that semi-access subsets do not collude and not open forged shares. On the other hands, the second scheme treats semi-access subsets as dishonest and detects cheating by semi-access subsets with high probability. Therefore, we call it *strongly secure* ramp scheme.

Finally, we propose two constructions of secure ramp scheme. The former one is the scheme for large d. The other is for $d = 2$. These schemes both have small share and the cheating can be detected with high probability. So, they are practical secret sharing schemes.

2. Preliminary

2.1 Notations and definitions

We use the following notations and definitions.

- $P = \{P_1, \ldots, P_n\}$ denotes a set of participants.

[†]The author is with Tokyo Institute of Technology, 2-12-1, O-okayama, Meguro-ku, 152-8552 Japan

a) E-mail: wakaha@craft.titech.ac.jp

- s is a secret distributed over a finite set $\mathcal{S}$. S is a random variable induced by s.
- v_i is a share of P_i distributed over a finite set $\mathcal{V}_i$. V_i is a random variable induced by v_i.
- For a finite set A, $|A|$ denotes the number of elements of A. We call $|\mathcal{V}_i|$ the share size.

The secret sharing scheme is a function $\Pi : \mathcal{V}_1 \times \cdots \times \mathcal{V}_n \to \mathcal{S}$.

2.2 Threshold scheme and secure threshold scheme

Threshold scheme is a most popular secret sharing scheme. We give Shamir's (k, n)-threshold scheme.

Scheme 1 ((k, n)-threshold scheme)
Let $\mathcal{S} = Z_q$. When the dealer has a secret $S = s$, then he chooses a random polynomial f with degree $k-1$ over $GF(q)$ such as

$$f(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$$

where $a_1, \ldots, a_{k-1}$ are random elements of $GF(q)$. A share for participant P_i is $v_i = f(i)$. On reconstruction phase, k or more participants can compute the secret function f from their shares v_i and obtain s.

In Shamir's scheme, the share size equals to the size of secret. This scheme can not detect dishonest participants. Only one cheater can cheat other $k-1$ participants by opening forge share.

Secure threshold scheme is a threshold scheme in which the cheating of less than threshold participants can be detected with high probability. The optimum scheme is presented in [8], which uses a planar difference set.

Definition 1: A planar difference set modulo $N = q(q-1)+1$ is a set of q numbers $B_q = \{b_0, b_1, \ldots, b_{q-1}\}$ with the property that the $q(q-1)$ differences $b_i - b_j (i \neq j)$, when reduced modulo N, are exactly the numbers $1, 2, \ldots, N-1$ in some order.

In a projective plane $PG(2, q-1)$ where $q-1$ is a prime power, a line has q points $\alpha^{b_0}, \ldots, \alpha^{b_{q-1}}$. Then, it is known that $\{b_0, \ldots, b_{q-1}\}$ is a planar difference set modulo N [9]. Therefore, B_q can be determined efficiently from two points of $PG(2, q-1)$.

Scheme 2 ((k, n, δ)-secure threshold scheme)
Let $\mathcal{S} = Z_q$ where $q(q-1)+1$ is a prime power and a planar difference set $B_q = \{b_0, b_1, \ldots, b_{q-1}\}$ modulo $N = q(q-1)+1$ be public. When the dealer has a secret $S = s$, at first he finds $\hat{s} = b_s$ from s. Then he uses Scheme 1 to distribute $\hat{s}$, that is, choose a polynomial f over $GF(N)$ with degree $k-1$ and set $v_i = f(i)$. On reconstruction phase, k or more participants can compute $\hat{s}$. If $\hat{s} = b_t \in B_q$, then t is a secret. Otherwise, some participant must cheat.

From the property of a planar difference set, it can be shown that the probability cheating successes is $\delta = 1/q = 1/|\mathcal{S}|$. The share size is

$$|\mathcal{V}_i| = (|\mathcal{S}| - 1)|\mathcal{S}| + 1 \sim |\mathcal{S}|^2,$$

which is optimum.

In Scheme 2, Scheme 1 is used to distribute $\hat{s}$. Let $\hat{S}$ be a random variable induced by $\hat{s}$. Then, $\hat{S}$ varies on $Z_N, N = q(q-1)+1$ and

$$\Pr[\hat{S} = \hat{s}] = \begin{cases} \Pr[S = s] & \text{if } \hat{s} \in B_q, \\ 0 & \text{if } \hat{s} \notin B_q. \end{cases}$$

Scheme 1 is a (k, n)-threshold scheme for any random variable S, so Scheme 2 is also a (k, n)-threshold scheme.

2.3 Ramp scheme

First, we show two definitions of ramp scheme. One is a weak definition which restricts the amount of leakage of secret to only access subsets and non-access subsets.

Definition 2: If $\Pi : \mathcal{V}_1 \times \cdots \times \mathcal{V}_n \to \mathcal{S}$ satisfies

$$\begin{array}{lll} \text{if} & k \leq l & H(S|V_{i_1} \cdots V_{i_l}) = 0, \\ \text{if} & l \leq k-d & H(S|V_{i_1} \cdots V_{i_l}) = H(S), \end{array}$$

then, we say that Π is a (k, d, n)-ramp scheme for S.

The next definition has an additional condition for semi-access subsets.

Definition 3: If Π is a (k, d, n)-ramp scheme for S and it satisfies

$$\text{if} \quad k-d < l < k \quad H(S|V_{i_1} \cdots V_{i_l}) = \frac{k-l}{d} H(S),$$

then, we say Π is a (k, d, n)-linear ramp scheme for S.

Linear ramp scheme defined as above is called simply *ramp scheme* in general. However, we distinguish (weakly conditioned) ramp scheme and linear ramp scheme.

We show an example of ramp scheme [5].

Scheme 3 ((k, d, n)-ramp scheme)
Let $\mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_{d-1}$ and $\mathcal{S}_j = Z_q$ for all j. Then any secret $s \in \mathcal{S}$ can be represented by $(s_0, \ldots, s_{d-1})$, $s_j \in Z_q$. The dealer chooses a random polynomial f with degree $k-1$ over $GF(q)$ such as

$$f(x) = s_0 + s_1 x + \cdots + s_{d-1} x^{d-1} + a_d x^d + \cdots + a_{k-1} x^{k-1}$$

where $a_d, \ldots, a_{k-1}$ are random numbers over $GF(q)$. The share is $v_i = f(i)$. On reconstruction phase, k or more participants can compute the secret function f from their shares v_i and obtain $s_0, \ldots, s_{d-1}$.

In this scheme, the share size is $|\mathcal{V}_i| = |\mathcal{S}|^{1/d}$.

If every s_i takes every value in $\mathcal{S}_i$ with equal probability, then this scheme is a linear ramp scheme, that is,

$$H(S|V_{i_1}\cdots V_{i_l}) = \frac{k-l}{d}H(S)$$

for any l $(k-d<l<k)$.

Now we consider the case the random variable S has a uniform distribution on $Z_{42} = Z_6 \times Z_7$. If $d=2$, we consider $\mathcal{S}_0, \mathcal{S}_1$ as Z_7, and S_0, S_1 as

$$\Pr[S_0 = s_0] = \begin{cases} 1/6 & \text{if } s_0 \in \{1,2,3,4,5,6\}, \\ 0 & \text{if } s_0 = 0, \end{cases}$$
$$\Pr[S_1 = s_1] = 1/7 \quad \text{always.}$$

S_1 is a uniform distribution and S_0 is not. For the simplicity, let $k=3$. Then, after some calculations we obtain the entropy as follows.

$$\begin{aligned} H(S) &= H(S_0) + H(S_1) = \log 6 + \log 7 \\ H(S|V_{i_1}) &= H(S) \\ H(S|V_{i_1}V_{i_2}V_{i_3}) &= 0 \end{aligned}$$

This means that Scheme 3 is a $(3,2,n)$-ramp scheme. Next, let estimate the conditional entropy $H(S|V_{i_1}V_{i_2})$. Since $v_i = f(i)$,

$$s_1 = \frac{i_2}{i_1(i_2-i_1)}v_{i_1} + \frac{i_1}{i_2(i_1-i_2)}v_{i_2} - \frac{i_2+i_1}{i_1 i_2}s_0.$$

Then,

$$\begin{aligned} &H(S|V_{i_1}=v_{i_1}, V_{i_2}=v_{i_2}) \\ &= H(S_0|V_{i_1}=v_{i_1}, V_{i_2}=v_{i_2}) \\ &\qquad + H(S_1|S_0, V_{i_1}=v_{i_1}, V_{i_2}=v_{i_2}) \\ &= H(S_0) + 0 \\ &= \log 6 < H(S)/2. \end{aligned}$$

Consequently, we obtain

$$H(S|V_{i_1}V_{i_2}) < H(S)/2,$$

and this means that Scheme 3 is not a $(3,2,n)$-*linear* ramp scheme.

3. Two Definitions of Secure Ramp Scheme

3.1 Two situations of ramp scheme

In this section, we claim there are two situations where ramp schemes are used.

Case 1 : If an adversary can corrupt at most c participants and the dealer wants not to leak any information about the secret, then he may use $(c+1,n)$-threshold scheme or $(c+d,d,n)$-ramp scheme for some d. The large d enables to shorten the share size, however, more participants are required to reconstruct the secret.

Case 2 : In practical case, the dealer can not guess correctly how many participants will be corrupted by an adversary. Then the dealer chooses k large enough, distributes the secret using (k,d,n)-ramp scheme for some d, and hopes an adversary will not corrupt $k-d+1$ or more participants. In this case, the dealer is not sure that no adversary can corrupt more than $k-d$.

In case 2, it is desirable that the amount of leakage to semi-access subsets is as small as possible and a *linear* ramp scheme is adequate to use. On the other hand, in case 1 it needs not to minimize the amount of leakage to semi-access subsets, since we assume the semi-access subsets to be honest. So, we can use a weakly conditioned ramp scheme.

3.2 Two definitions

Assume that there are cheaters who open forged shares as their shares. How many cheaters we should consider?

In case 1, we assumed that $k-d$ or less participants can be corrupted. Then, we wish to detect cheating by at most $k-d$ participants.

Definition 4: A (k,d,n)-ramp scheme for S is called *δ-secure* if cheating by at most $k-d$ participants can be detected with probability $1-\delta$.

In case 2, a stronger condition is required.

Definition 5: A (k,d,n)-ramp scheme for S is called *δ-strongly secure* if cheating by at most $k-1$ participants can be detected with probability $1-\delta$.

Similarly, we can define a δ-secure linear ramp scheme and a δ-strongly secure linear ramp scheme.

4. Constructions of Secure Ramp Scheme

In this section, we show two constructions of secure ramp scheme.

4.1 Construction for relatively large d

We can construct a secure ramp scheme combining Scheme 2 and Scheme 3.

Scheme 4 Let $\mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_{d-1}$ and $\mathcal{S}_j = Z_q$ for all j where $q(q-1)+1$ is a prime power. Let a planar difference set $B_q = \{b_0, b_1, \ldots, b_{q-1}\}$ modulo $N = q(q-1)+1$ be public. Suppose the dealer has a secret $s = (s_0, \ldots, s_{d-1})$ where $s_j \in Z_q$. First, he obtains $\hat{s}_j = b_{s_j}$ $(0 \le j < d)$ from s_j $(0 \le j < d)$. We call $\hat{s}_j$ a scattering share, since each $s_j \in Z_q$ is scattered into $\hat{s}_j \in Z_N$. Then, he distributes $\hat{s}_j$ $(0 \le j < d)$ using a random polynomial f with degree $k-1$ over $GF(N)$ similarly as Scheme 3. On reconstruction phase, scattering secrets $(\hat{s}_0, \ldots, \hat{s}_{d-1})$ are obtained at first from k or

more shares. If $\hat{s}_j = b_{t_j} (\in B_q)$ for all j $(0 \le j < d)$, then get $s_j = t_j$ $(0 \le j < d)$. Otherwise, someone must be cheating.

In this scheme, the share size is

$$|\mathcal{V}_i| = N = q(q-1) + 1 \sim |\mathcal{S}|^{2/d}.$$

As mentioned in previous section, B_q can be constructed efficiently using a line in $PG(2, q-1)$.

Lemma 1: Scheme 4 is a (k, d, n)-ramp scheme for any S.

(Proof) k or more shares determine $\hat{s}_j$ $(0 \le j < d)$ and s_j $(0 \le j < d)$. $k-d$ or less shares can not determine either of $\hat{s}_j$ $(0 \le j < d)$ and s_j $(0 \le j < d)$. Q.E.D.

However, this scheme is not a linear ramp scheme, since Scheme 4 uses Scheme 3 with random variable $\hat{S}_j$ such as

$$\Pr[\hat{S}_j = \hat{s}_j] = \begin{cases} \Pr[S_j = t] & \text{if } \hat{s}_j = b_t \in B_q \\ 0 & \text{if } \hat{s}_j \notin B_q, \end{cases}$$

which is not a uniform distribution over Z_q.

The next theorem shows that Scheme 4 is a secure ramp scheme when d is relatively large.

Theorem 1: If S is a uniform distribution on Z_{q^d} and $2d \ge k$, then Scheme 4 is a δ-secure (k, d, n)-ramp scheme for S where $\delta = 1/q^{2d-k+1}$.

(Proof) We will estimate the probability with which $k-d$ cheaters can cheat other d honest participants. Let cheaters be $P_{i_1}, \ldots, P_{i_{k-d}}$. Their true shares are $(v_{i_1}, \ldots, v_{i_{k-d}})$. The honests $P_{i_{k-d+1}}, \ldots, P_{i_k}$ have $(v_{i_{k-d+1}}, \ldots, v_{i_k})$ as their share. On reconstruction phase, assume that the cheater P_{i_l} opens $v'_{i_l} = v_{i_l} + e_l$ as his forged share. $\boldsymbol{e} \stackrel{\triangle}{=} (e_1, \ldots, e_{k-d})^t$ is a cheaters' strategy and we can restrict $\boldsymbol{e} \ne \boldsymbol{0}$. We denote the scattering secrets reconstructed from true shares $(v_{i_1}, \ldots, v_{i_{k-d}}, v_{i_{k-d+1}}, \ldots, v_{i_k})$ as $\hat{s}_j$ $(0 \le j < d)$, and from forged shares and honests' shares $(v'_{i_1}, \ldots, v'_{i_{k-d}}, v_{i_{k-d+1}}, \ldots, v_{i_k})$ as $\hat{s}'_j$ $(0 \le j < d)$. Then, from Lagrange's formula, $\hat{s}'_j$ $(0 \le j < d)$ can be written as

$$\begin{aligned} \hat{s}'_j &= L_1^{(j)} v'_{i_1} + \cdots + L_{k-d}^{(j)} v'_{i_{k-d}} \\ &\qquad + L_{k-d+1}^{(j)} v_{i_{k-d+1}} + \cdots + L_k^{(j)} v_{i_k} \\ &= \hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e}, \end{aligned}$$

where $L_l^{(j)}$ are constant factors determined by indices $i_1, \ldots, i_k$, and $\boldsymbol{L}^{(j)} = (L_1^{(j)}, \ldots, L_{k-d}^{(j)})$. (Especially, $L_l^{(0)}$ is Lagrange's factor $\Pi_{l' \ne l}(-i_{l'})(i_l - i_{l'})^{-1}$.) The cheat will success only if $\hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e}$ belongs to B_q for all j. Since $\hat{s}_j \in B_q$ for all j, the cheating probability $P_{cheat}(\boldsymbol{e})$ for given $\boldsymbol{e}$ is

$$\begin{aligned} &P_{cheat}(\boldsymbol{e}) \\ &= \Pr[\forall j : \hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e} \in B_q \\ &\qquad \mid \text{cheaters have } (v_{i_1}, \ldots, v_{i_{k-d}}), \forall j : \hat{s}_j \in B_q]. \end{aligned}$$

Since $k-d$ shares give no information about the secret,

$$\begin{aligned} &P_{cheat}(\boldsymbol{e}) \\ &= \Pr[\forall j : \hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e} \in B_q \mid \forall j : \hat{s}_j \in B_q] \\ &= \prod_{j=0}^{d-1} \Pr[\hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e} \in B_q \mid \hat{s}_j \in B_q] \end{aligned}$$

Using the property of a planar difference set B_q and the fact that $\hat{s}_j$ is distributed on B_q uniformly,

$$\begin{aligned} &\Pr[\hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e} \in B_q \mid \hat{s}_j \in B_q] \\ &= \begin{cases} 1 & \text{if } \boldsymbol{L}^{(j)} \boldsymbol{e} = 0, \\ 1/|B_q| & \text{otherwise.} \end{cases} \end{aligned} \tag{1}$$

Now we will show that if $k \le 2d$ then there are $2d-k+1$ or more j $(0 \le j \le d-1)$ such that $\boldsymbol{L}^{(j)} \boldsymbol{e} \ne 0$ for any $\boldsymbol{e} \ne \boldsymbol{0}$. We assume that there exists a special $\tilde{\boldsymbol{e}} (\ne \boldsymbol{0})$ such that

$$\boldsymbol{L}^{(j)} \tilde{\boldsymbol{e}} = 0 \tag{2}$$

for $k-d$ js, that is, $j_1, \ldots, j_{k-d}$. Let define a $(k-d) \times (k-d)$ matrix $\mathbf{L}$ as

$$\mathbf{L} = \begin{pmatrix} \boldsymbol{L}^{(j_1)} \\ \vdots \\ \boldsymbol{L}^{(j_{k-d})} \end{pmatrix}.$$

Then, from eq.(2), we obtain

$$\mathbf{L} \tilde{\boldsymbol{e}} = \boldsymbol{0}.$$

On the other hand, using the property of $L_l^{(j)}$, we get

$$\det \mathbf{L} \ne 0.$$

So, $\mathbf{L}$ has an inverse $\mathbf{L}^{-1}$,

$$\begin{aligned} \tilde{\boldsymbol{e}} &= \mathbf{L}^{-1} \mathbf{L} \tilde{\boldsymbol{e}} \\ &= \mathbf{L}^{-1} \boldsymbol{0} = \boldsymbol{0}. \end{aligned}$$

It is contradiction. Consequently, the number of j such that

$$\boldsymbol{L}^{(j)} \boldsymbol{e} = 0$$

is at most $k-d-1$ for any $\boldsymbol{e} \ne \boldsymbol{0}$. Now we have proven that the number of j such that $\boldsymbol{L}^{(j)} \boldsymbol{e} \ne 0$ is $d - (k-d-1) = 2d-k+1$ or more for any $\boldsymbol{e} \ne \boldsymbol{0}$.

Finally, we obtain the cheating probability with the best strategy as

$$\begin{aligned} P_{cheat} &= \max_{\boldsymbol{e} \ne \boldsymbol{0}} (P_{cheat}(\boldsymbol{e})) \\ &= \max_{\boldsymbol{e} \ne \boldsymbol{0}} \left(\prod_{j=0}^{d-1} \Pr[\hat{s}_j + \boldsymbol{L}^{(j)} \boldsymbol{e} \in B_q \mid \hat{s}_j \in B_q] \right) \\ &\le (1/|B_q|)^{2d-k+1} = 1/q^{2d-k+1} \end{aligned}$$

from eq.(1). Q.E.D.

4.2 Construction for $d = 2$

When $d = 2$, we can construct a secure ramp scheme in which cheating of $k-2$ cheaters can be detected with high probability $(1 - 1/|\mathcal{S}|)$ and the share is the same size with the secret size.

Before showing second construction, we define some notations.

Let $B'_q = \{b_0, b_1, \ldots, b_{q-1}\}$ be a subset of $(Z_q)^2$. For two elements $w = (w_0, w_1)$ and $y = (y_0, y_1)$ of $(Z_q)^2$, define addition and subtraction as

$$w \pm y = (w_0 \pm y_0 \bmod q, w_1 \pm y_1 \bmod q) \in (Z_q)^2.$$

Scheme 5 Let $\mathcal{S} = Z_q$ and a set $B'_q = \{b_0, \ldots, b_{q-1}\}$ be public. Suppose the dealer has a secret $s \in Z_q$. First, he obtains $(\hat{s}_0, \hat{s}_1) = b_s \in B'_q$. Then, he distribute $\hat{s}_0$ and $\hat{s}_1$ using Scheme 3, that is, he chooses f over $GF(q)$ such as

$$f(x) = \hat{s}_0 + \hat{s}_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}.$$

The share is $v_i = f(i)$ as usual. On reconstruction phase, $\hat{s}_0$ and $\hat{s}_1$ are obtained from k or more shares. If $(\hat{s}_0, \hat{s}_1) = b_t \in B'_q$, then get $S = t$. Otherwise, someone must be cheating.

In this scheme, the share size is

$$|\mathcal{V}_i| = q = |\mathcal{S}|.$$

We can easily prove the next lemma.

Lemma 2: Scheme 5 is a (k, d, n)-ramp scheme for any S.

Theorem 2: For given set $B'_q = \{b_0, b_1, \ldots, b_{q-1}\}$ and for uniformly distributed S over Z_q, Scheme 5 is $h/|\mathcal{S}|$-secure $(k, 2, n)$-ramp scheme for S, where

$$h = \max_{w \in (Z_q)^2, w \neq (0,0)} |\{(l, l') \mid b_{l'} - b_l = w\}|.$$

(Proof) Let $P_{i_1}, \ldots, P_{i_{k-2}}$ be cheaters. We estimate the probability that the cheaters can cheat honest participants, $P_{i_{k-1}}, P_{i_k}$. Fix the shares of cheaters to be $(v_{i_1}, \ldots, v_{i_{k-2}})$ and let the shares of $P_{i_{k-1}}, P_{i_k}$ be $v_{i_{k-1}}, v_{i_k}$ respectively. Similarly as the proof of theorem 1, let P_{i_l}'s forged share be $v'_{i_l} = v_{i_l} + e_l$, where $\boldsymbol{e} \stackrel{\triangle}{=} (e_1, \ldots, e_{k-2})^t \neq \mathbf{0}$. Then, $(\hat{s}'_0, \hat{s}'_1)$ which is obtained by forged shares are

$$(\hat{s}'_0, \hat{s}'_1) = (\hat{s}_0 + \boldsymbol{L}^{(0)}\boldsymbol{e}, \hat{s}_1 + \boldsymbol{L}^{(1)}\boldsymbol{e})$$

where $(\hat{s}_0, \hat{s}_1)$ is obtained by $(v_{i_1}, \ldots, v_{i_k})$ and $\boldsymbol{L}^{(j)}$ is the same factor of the proof of theorem 1. The cheating successes only if $(\hat{s}_0 + \boldsymbol{L}^{(0)}\boldsymbol{e}, \hat{s}_1 + \boldsymbol{L}^{(1)}\boldsymbol{e})$ belongs to B'_q. From $(\hat{s}_0, \hat{s}_1) \in B'_q$, the cheating probability $P_{cheat}(\boldsymbol{e})$ for given $\boldsymbol{e}$ is

$$\begin{aligned} & P_{cheat}(\boldsymbol{e}) \\ &= \Pr[(\hat{s}_0 + \boldsymbol{L}^{(0)}\boldsymbol{e}, \hat{s}_1 + \boldsymbol{L}^{(1)}\boldsymbol{e}) \in B'_q \\ &\quad \mid \text{cheaters have } (v_{i_1}, \ldots, v_{i_{k-2}}), (\hat{s}_0, \hat{s}_1) \in B'_q]. \end{aligned}$$

The fact that $k-2$ shares has no information about the secret leads

$$\begin{aligned} P_{cheat}(\boldsymbol{e}) = \Pr[&(\hat{s}_0 + \boldsymbol{L}^{(0)}\boldsymbol{e}, \hat{s}_1 + \boldsymbol{L}^{(1)}\boldsymbol{e}) \in B'_q \\ &\mid (\hat{s}_0, \hat{s}_1) \in B'_q]. \end{aligned}$$

Since S is a uniform distribution,

$$\begin{aligned} &\Pr[(\hat{s}_0 + w_0, \hat{s}_1 + w_1) \in B'_q \mid (\hat{s}_0, \hat{s}_1) \in B'_q] \\ &= |\{(l, l') \mid b_{l'} - b_l = w\}|/|B'_q| \end{aligned}$$

for any $w = (w_0, w_1) \in (Z_q)^2$ $(w \neq (0, 0))$. If $\boldsymbol{e} \neq \mathbf{0}$, $(\boldsymbol{L}^{(0)}\boldsymbol{e}, \boldsymbol{L}^{(1)}\boldsymbol{e}) \neq (0, 0)$. Consequently, cheating probability of the best strategy is

$$\begin{aligned} P_{cheat} &= \max_{\boldsymbol{e} \neq \mathbf{0}} \Pr[(\hat{s}_0 + \boldsymbol{L}^{(0)}\boldsymbol{e}, \hat{s}_1 + \boldsymbol{L}^{(1)}\boldsymbol{e}) \in B'_q \\ &\qquad \mid (\hat{s}_0, \hat{s}_1) \in B'_q] \\ &= |\{(l, l') \mid b_{l'} - b_l = (\boldsymbol{L}^{(0)}\boldsymbol{e}, \boldsymbol{L}^{(1)}\boldsymbol{e})\}|/|B'_q| \\ &\leq h/|\mathcal{S}|. \end{aligned}$$

Q.E.D.

If q is an odd prime, we can give B'_q such that

$$|\{(l, l') \mid b_{l'} - b_l = w\}| = 0 \text{ or } 1$$

for all $w \neq (0, 0)$.

Theorem 3: Let q be an odd prime and $b_i = (i, i^2 \bmod q)$ for $0 \leq i < q$. Then $B'_q = \{b_0, \ldots b_{q-1}\}$ satisfies

$$|\{(l, l') \mid b_{l'} - b_l = w\}| = 0 \text{ or } 1$$

for all $w \in (Z_q)^2 \setminus \{(0, 0)\}$.

(Proof) Since $b_i = (i, i^2 \bmod q)$

$$b_{l'} - b_l = (l' - l, (l')^2 - l^2).$$

It is easily shown that

$$|\{(l, l') \mid b_{l'} - b_l = (0, w_1)\}| = 0$$

for all $w_1 \neq 0$. Next, we fix $w = (w_0, w_1)$ $(w_0 \neq 0)$ arbitrarily. If $b_{l'} - b_l = (w_0, w_1)$ for some l and l',

$$\begin{aligned} w_0 &= l' - l \\ w_1 &= (l')^2 - l^2 \;=\; 2w_0 l' - w_0. \end{aligned}$$

Then l and l' are uniquely determined from w_0 and w_1, and

$$|\{(l, l') \mid b_{l'} - b_l = (w_0, w_1)\}| \leq 1.$$

Q.E.D.

Corollary 1: Let q be an odd prime. For uniformly distributed S on Z_q Scheme 5 is $1/|\mathcal{S}|$-weak secure $(k, 2, n)$-ramp scheme for S.

(Proof) We can use B'_q defined in theorem 3. Q.E.D.

5. Conclusion

In this paper, we attempted to construct practical secret sharing schemes. First, we claimed there are two situations where ramp schemes are used. Next we defined two practical secret sharing schemes, secure ramp scheme and strongly secure ramp scheme. And then, we proposed two constructions of secure ramp scheme. The first scheme has shares with the size of

$$|\mathcal{V}_i| \sim |\mathcal{S}|^{2/d}$$

for all i, and the cheating probability is

$$\delta = 1/|\mathcal{S}|^{(2d-k+1)/d}$$

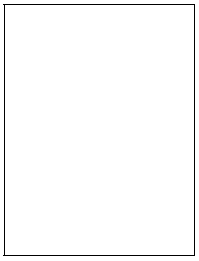
when $2d \geq k$. If $d = 2$ the second scheme can be used, in which the share size and the cheating probability are

$$\begin{aligned} |\mathcal{V}_i| &= |\mathcal{S}|, \\ \delta &= 1/|\mathcal{S}|. \end{aligned}$$

For further works, construction of a strongly secure ramp scheme and showing the lower bound of the share size are remained.

References

[1] G.R. Blakley. "Safeguarding cryptographic keys,"Proc. of the AFIPS 1979 National Computer Conference, Vol. 48, pp. 313-317 (1979)
[2] A. Shamir,"How to share a secret," In communications of the ACM, Vol. 22, No. 11, pp. 612-613 (1979)
[3] E.D. Karnin, J.W. Green, M.E. Hellman, "On secret sharing systems," IEEE Trans. on Inform. Theory, IT-29, pp. 35-41 (1982)
[4] R.M. Capocelli, A.De Santis, L. Gargano and U. Vaccaro, "On the size of shares for secret sharing schemes", Journal of Cryptology, Vol. 6, No. 3, pp. 157-167 (1993)
[5] G.R.Blakley and C. Meadows, "Security of Ramp Scheme," Proc. of Crypto'84, Lecture Note in Computer Science, Vol. 196, pp. 242-268 (1984)
[6] M. Tompa and H. Woll, "How to Share a Secret with Cheaters", Journal of Cryptology, Vol. 1, pp. 133-139 (1988)
[7] K.Kurosawa and K.Okada, "Combinatorial Lower Bounds for Secret Sharing Schemes," Information Processing Letters, Vol. 60, No. 6, pp. 301-304 (1996)
[8] W. Ogata and K.Kurosawa, "Optimum Secret Sharing Scheme Secure against Cheating," Proc. of Eurocrypt'96, Lecture Note in Computer Science, Vol. 1070, pp. 200-211 (1996)
[9] F. J. MacWilliams and N.J.A. Sloane, "The theory of Error-correcting codes," North-Holland, pp. 397–398 (1981)



Wakaha Ogata Received B.S., M.E. and D.E. degrees in electrical and electronic engineering in 1989, 1991 and 1994, respectively, from Tokyo Institute of Technology. From 1995 to 2000, she was an Assistant Professor in the Department of Computer Engineering at Himeji Institute of Technology. Since 2000, she has been an Associate Professor in Center for Research in Advanced Financial Technology at Tokyo Institute of Technology. Her current interests are information security and cryptographic protocols.