Optimum Secret Sharing Scheme Secure against Cheating

Wakaha Ogata[1] and Kaoru Kurosawa[2]

[1] Himeji Institute of Technology, 2167 Shosha, Himeji-shi, Hyogo 671–22, Japan
wakaha@comp.eng.himeji-tech.ac.jp
[2] Tokyo Institute of Technology, 2–12–1 O-okayama, Meguro-ku, Tokyo 152, Japan
kurosawa@ss.titech.ac.jp

Abstract. Tompa and Woll considered a problem of cheaters in (k, n) threshold secret sharing schemes. We first derive a tight lower bound on the size of shares $|\mathcal{V}_i|$ for this problem: $|\mathcal{V}_i| \geq (|\mathcal{S}| - 1)/\delta + 1$, where $\mathcal{V}_i$ denotes the set of shares of participant P_i, $\mathcal{S}$ denotes the set of secrets, and δ denotes the cheating probability. We next present an optimum scheme which meets the equality of our bound by using "difference sets."

1 Introduction

(k, n) threshold secret sharing schemes [2, 3] have been studied extensively so far because of their wide applications in fields, like key management and secure computation. In such a scheme, a dealer D distributes a secret s to n participants $P_1, \ldots, P_n$ in such a way that any k or more participants can recover the secret s but any $k - 1$ or fewer participants have no information on s. A piece of information given to P_i is called a share and is denoted by v_i. An important issue in secret sharing schemes is the size of shares $|\mathcal{V}_i|$, where $\mathcal{V}_i \stackrel{\triangle}{=} \{v_i \mid \Pr(v_i) > 0\}$, because the security of a system will decrease if $|\mathcal{V}_i|$ increases. Let $\mathcal{S} \stackrel{\triangle}{=} \{s \mid \Pr(s) > 0\}$. Then it is known that

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

in any (k, n) threshold scheme [4].

Tompa and Woll [1] considered the following scenario. Suppose that $k - 1$ participants $P_1, \ldots, P_{k-1}$ want to cheat a k-th participant P_k by opening forged shares $v'_1, \ldots, v'_{k-1}$. They succeed if the secret s' reconstructed from $v'_1, \ldots, v'_{k-1}$ and v_k is different from the original secret s. Tompa and Woll showed that Shamir's scheme [2] is insecure against this attack in that even a single participant can, with high probability, deceive $k - 1$ honest participants. They showed a scheme secure against this problem, but $|\mathcal{V}_i|$ in their scheme is very large:

$$|\mathcal{V}_i| = ((|\mathcal{S}| - 1)(k - 1)/\epsilon + k)^2 \tag{1}$$

where ϵ denotes the cheating probability. Carpentieri, De Santis, and Vaccaro [5] recently showed the following lower bound on $|\mathcal{V}_i|$ for this problem:

$$|\mathcal{V}_i| \geq |\mathcal{S}|/\epsilon. \tag{2}$$

U. Maurer (Ed.): Advances in Cryptology - EUROCRYPT '96, LNCS 1070, pp. 200-211, 1996.

Now, we see that there is a big gap between eq. (1) and (2). Both of them can be improved. Furthermore, in the derivation of eq. (2) it is assumed that $k-1$ cheaters $P_1, \ldots, P_{k-1}$ somehow know the secret s before they cheat P_k. (We call this the CDV assumption.)

In this paper we first derive a tight lower bound on $|V_i|$ for this problem by using a probabilistic method. In deriving our bound, we do not use the CDV assumption. That is, it is assumed that $k-1$ cheaters have no information on s (according to the definition of (k,n) threshold secret sharing schemes). Let δ be the probability that $P_1, \ldots, P_{k-1}$ can cheat P_k. Then our bound is

$$|V_i| \geq (|S|-1)/\delta + 1. \tag{3}$$

We then present an optimum scheme which meets the equality of our bound by using "difference sets." A planar difference set modulo $N = l(l-1)+1$ is a set of l numbers $B = \{d_0, d_1, \ldots, d_{l-1}\}$ with the property that the $l(l-1)$ differences $d_i - d_j$ $(d_i \neq d_j)$, when reduced modulo N, are exactly the numbers $1, 2, \ldots, N-1$ in some order [6]. It is known that there exists a planar difference set if l is a prime power [6]. Our optimum scheme is then characterized as follows. If there exists a planar difference set modulo $N = l(l-1)+1$ such that N is a prime, then there exists a (k,n) threshold secret sharing scheme which meets the equality of our bound eq. (3) such that $|S| = l, \delta = 1/l, n < N$.

Furthermore, this result is generalized as follows. Let $(\Gamma, +)$ be a group of order N and let $B = \{d_0, d_1, \ldots, d_{l-1}\}$ be a subset of Γ. Then B is called a (N, l, λ) difference set [7] if each nonzero element x of Γ appears λ times as a difference $d_i - d_j$ $(d_i \neq d_j)$. Our generalized scheme is then given as follows. There exists a (k,n) threshold secret sharing scheme which meets the equality of our bound eq. (3) such that $|S| = l, \delta = \lambda/l, n < N$ if there exists a (N, l, λ) difference set B in $(GF(N), +)$. It is known that there exists a (N, l, λ) difference set B in $(GF(N), +)$ such that $N = 4t-1, l = 2t-1, \lambda = t-1$ [7].

Finally, for the model with the CDV assumption, we show a lower bound on $|V_i|$ more tight than eq. (2) by using the same technique we use to derive eq. (3). Our bound for the model with the CDV assumption is

$$|V_i| \geq (|S|-1)/\epsilon^2 + 1.$$

A slightly different problem has been studied by other researchers. McElice and Sarwate [8] showed that in Shamir's (k,n) threshold scheme, any group of $k+2e$ participants which includes at most e cheaters can always identify cheaters and correctly calculate the secret. (More than k participants are required though.) The problem of identifying cheaters has also been studied [9, 10, 11, 12]. Those schemes, however, require $|V_i|$ much bigger than the bound given in eq. (3). On the other hand, in this paper, we are interested only in detecting the fact of cheating.

2 Preliminaries

2.1 Definition of cheating

D denotes a probabilistic Turing machine called a dealer, S denotes a random variable distributed over a finite set $\mathcal{S}$, and $s \in \mathcal{S}$ is called a secret. On input $s \in \mathcal{S}$, D outputs $(v_1, \ldots, v_n)$ randomly. For $1 \leq i \leq n$, each participant P_i holds v_i as his share. V_i denotes the random variable induced by v_i. Let $\mathcal{V}_i \triangleq \{v_i \mid \Pr(V_i = v_i) > 0\}$.

Definition 1. We say that (D, S) is a (k, n) threshold secret sharing scheme if the following two requirements hold: For any $\{i_1, \ldots, i_j\} \subseteq \{1, \ldots, n\}$ and $(v_{i_1}, \ldots, v_{i_j})$ such that $\Pr(V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}) > 0$,
(A1) if $j \geq k$, there exists a unique $s \in \mathcal{S}$ such that

$$\Pr(S = s \mid V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}) = 1,$$

(A2) if $j < k$, for each $s \in \mathcal{S}$,

$$\Pr(S = s \mid V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}) = \Pr(S = s).$$

Definition 2. For $w \in \mathcal{V}_{i_1} \times \cdots \times \mathcal{V}_{i_k}$,

$$Sec_{(i_1,\ldots,i_k)}(w) \triangleq \begin{cases} s & \text{if } \exists s \in S \text{ such that } \Pr(S = s \mid V_{i_1} \cdots V_{i_k} = w) = 1, \\ \perp & \text{otherwise.} \end{cases}$$

($(i_1, \ldots, i_k)$ will be omitted.)

Definition 3. Suppose that $k-1$ cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ have $b = (v_{i_1}, \ldots, v_{i_{k-1}})$ as their shares. We say that the cheaters can cheat P_{i_k} by opening $b' = (v'_{i_1}, \ldots, v'_{i_{k-1}})$ if $Sec(b', v_{i_k}) \neq Sec(b, v_{i_k})$ and $Sec(b', v_{i_k}) \in \mathcal{S}$, where v_{i_k} denotes the share of P_{i_k}.

2.2 Known bound on $|\mathcal{V}_i|$ under the CDV assumption

Carpentieri, De Santis, and Vaccaro [5] showed the following lower bound on $|\mathcal{V}_i|$ by using entropy. In deriving that bound they assumed that $k-1$ cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ shomehow know the secret s before they cheat P_k, although, in the definition of (k, n) threshold secret sharing schemes, $k-1$ cheaters have no information on s. (We call this the CDV assumption.) Let $b = (v_{i_1}, \ldots, v_{i_{k-1}})$ denote the shares of the cheaters, and let $b' = (v'_{i_1}, \ldots, v'_{i_{k-1}})$ denote the forged shares that the cheaters open to cheat P_{i_k}. Carpentieri et al. defined the average cheating probability as follows:

$$P'(Cheat \mid V_{i_1}, \ldots, V_{i_{k-1}}, S) \triangleq E[\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b. \text{ They also know } s)], \quad (4)$$

Definition 4. [5] A (k, n) threshold secret sharing scheme is called a (k, n, ϵ) robust secret sharing scheme if $P'(Cheat \mid V_{i_1}, \ldots, V_{i_{k-1}}, S) \leq \epsilon$ for any $\{i_1, \ldots, i_{k-1}\} \subseteq \{1, \ldots, n\}$.

Proposition 5. *[5] In a (k, n, ϵ) robust secret sharing scheme, if the secret is uniformly chosen, then $|\mathcal{V}_i| \geq |\mathcal{S}|/\epsilon$.*

3 New Lower Bound on $|\mathcal{V}_i|$

3.1 Definition of secure secret sharing

In this section we derive a tight lower bound on $|\mathcal{V}_i|$ by using a probabilistic method. In deriving this bound we do not make the CDV assumption (see subsection 2.2). That is, it is assumed that, according to the definition of (k, n) threshold secret sharing schemes, $k-1$ cheaters have no information on s. Suppose that $P_{i_1}, \ldots, P_{i_{k-1}}$ are cheaters. Let $b = (v_{i_1}, \ldots, v_{i_{k-1}})$ denote the shares of the cheaters, and let $b' = (v'_{i_1}, \ldots, v'_{i_{k-1}})$ denote the forged shares that the cheaters open to cheat P_{i_k}. Since the cheaters have no information on s, we define the average cheating probability as follows:

$$\begin{aligned} &P(Cheat \mid V_{i_1}, \ldots, V_{i_{k-1}}) \\ &\triangleq E[\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b)], \end{aligned} \tag{5}$$

(S and s in eq. (4) are absent from eq. (5).)

Definition 6. A (k, n) threshold secret sharing scheme is called a (k, n, δ) secure secret sharing scheme if $P(Cheat \mid V_{i_1}, \ldots, V_{i_{k-1}}) \leq \delta$ for any $\{i_1, \ldots, i_{k-1}\} \subseteq \{1, \ldots, n\}$.

3.2 New lower bound on $|\mathcal{V}_i|$

In the distribution phase, suppose that cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ have $b = (v_{i_1}, \cdots, v_{i_{k-1}})$ as their shares of a secret s and P_{i_k} has x as his share. That is, $Sec(b, x) = s$. In the reconstruction phase, if P_{i_1} opens $v'_{i_1} (\neq v_{i_1})$ such that $Sec(v'_{i_1}, v_{i_2}, \cdots, v_{i_{k-1}}, x) = s'$ and $s' \neq s$, then P_{i_k} is cheated. Now, let

$$Y(x, s) \triangleq \{v'_{i_1} \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s' \in \mathcal{S}, s' \neq s\}$$

For fixed x and s, $Y(x, s)$ denotes the set of forged shares of P_{i_1} which can cheat P_{i_k}. (However, the cheaters do not know x nor s.) Let

$$W(s) \triangleq \{x \in \mathcal{V}_{i_k} \mid Sec(b, x) = s\}.$$

$W(s)$ denotes the set of possible shares of P_{i_k} for a fixed s.

Lemma 7. *For $\forall s \in \mathcal{S}, \forall x \in W(s)$,*

$$|Y(x, s)| \geq |\mathcal{S}| - 1.$$

Proof. Since k participants can recover the secret uniquely, for $\forall s', s''(s' \neq s'')$,

$$\{v'_{i_1} \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s'\}$$
$$\cap \{v'_{i_1} \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s''\} = \emptyset.$$

From (A2) of Def.1, for any $s' \in \mathcal{S}$, there exists at least one v'_{k_1} such that

$$Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s'.$$

Therefore, from the definition of $Y(x,s)$,

$$\begin{aligned}
|Y(x,s)| &= |\bigcup_{s' \in \mathcal{S}, s' \neq s} \{v'_{i_1} \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s'\}| \\
&= \sum_{s' \in \mathcal{S}, s' \neq s} |\{v'_{i_1} \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s'\}| \\
&\geq \sum_{s' \in \mathcal{S}, s' \neq s} 1 \\
&= |\mathcal{S}| - 1.
\end{aligned}$$

□

Now our lower bound on $|\mathcal{V}_i|$ is given as follows. The following bound holds for any distribution on S.

Theorem 8. *In a (k, n, δ) secure secret sharing scheme,*

$$|\mathcal{V}_i| \geq \frac{|\mathcal{S}| - 1}{\delta} + 1. \tag{6}$$

Proof. Consider cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ such that only P_{i_1} opens a forged share $v'_{i_1}(\neq v_{i_1})$. The other $P_{i_2}, \ldots, P_{i_{k-1}}$ open their shares honestly. For these specific cheaters,

$$\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b)$$

$$\geq \max_{v'_{i_1}} \Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b) \tag{7}$$

Now, we randomize v'_{i_1} in order to compute the right-hand side. Consider P_{i_1} who opens $v'_{i_1}(\neq v_{i_1})$ randomly. More precisely,

$$\Pr(P_{i_1} \text{ opens } v'_{i_1}) = \begin{cases} 1/(|\mathcal{V}_{i_1}| - 1) & \text{if } v'_{i_1} \neq v_{i_1} \\ 0 & \text{if } v'_{i_1} = v_{i_1}. \end{cases}$$

For this probabilistic P_{i_1}, let's compute

$$E[\Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b)],$$

where E is taken over v'_{i_1} and Pr() is taken over s and x. Then from lemma 7,

$$\begin{aligned}
&E_{v'_{i_1}}[\Pr_{s,x\in W(s)}(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1}\cdots P_{i_{k-1}} \text{ have } b)]\\
&= E_{s,x\in W(s)}[\Pr_{v'_{i_1}}(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1}\cdots P_{i_{k-1}} \text{ have } b)]\\
&= E_{s,x\in W(s)}[|Y(x,s)|/(|\mathcal{V}_{i_1}|-1)]\\
&\geq (|\mathcal{S}|-1)/(|\mathcal{V}_{i_1}|-1).
\end{aligned}$$

Therefore

$$\begin{aligned}
&\max_{v'_{i_1}}\Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1}\cdots P_{i_{k-1}} \text{ have } b)\\
&\geq E_{v'_{i_1}}[\Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1}\cdots P_{i_{k-1}} \text{ have } b)]\\
&\geq (|\mathcal{S}|-1)/(|\mathcal{V}_{i_1}|-1).
\end{aligned}$$

Hence, from eq. (7),

$$\max_{b'}\Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1}\cdots P_{i_{k-1}} \text{ have } b) \geq (|\mathcal{S}|-1)/(|\mathcal{V}_{i_1}|-1).$$

$$E_b[\max_{b'}\Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1}\cdots P_{i_{k-1}} \text{ have } b)] \geq (|\mathcal{S}|-1)/(|\mathcal{V}_{i_1}|-1).$$

Consequently, in a (k,n,δ) secure secret sharing scheme,

$$\delta \;\geq\; P(Cheat \mid V_{i_1},\ldots,V_{i_{k-1}}) \;\geq\; (|\mathcal{S}|-1)/(|\mathcal{V}_{i_1}|-1).$$

Therefore, $|\mathcal{V}_{i_1}| \geq (|\mathcal{S}|-1)/\delta+1$. □

4 Optimum (k,n,δ) Secure Scheme

In this section, we show an optimum scheme which meets the equality of Theorem 8 by using "difference sets."

4.1 Difference set

Definition 9. [6] A *planar difference set* modulo $N = l(l-1)+1$ is a set of l numbers $B = \{d_0, d_1, \ldots, d_{l-1}\}$ with the property that the $l(l-1)$ differences $d_i - d_j$ $(d_i \neq d_j)$, when reduced modulo N, are exactly the numbers $1, 2, \ldots, N-1$ in some order.

Example 1. [6] $\{d_0 = 0, d_1 = 1, d_2 = 3\}$ is a planar difference set modulo 7 with $l = 3$. Indeed, the differences modulo 7 are

$$1-0=1,\; 3-0=3,\; 3-1=2,\; 0-1=6,\; 0-3=4,\; 1-3=5.$$

Proposition 10. *[6] In a projective plane $PG(2,q)$, a line has $l = q+1$ points $\alpha^{d_0}, \ldots, \alpha^{d_{l-1}}$, where q is a prime power. Then $\{d_0, \ldots, d_{l-1}\}$ is a planar difference set modulo q^2+q+1.*

Definition 9 is generalized as follows.

Definition 11. [7] Let $(\Gamma, +)$ be a group of order N. B is called a (N, l, λ)-difference set if it satisfies

- $B \subset \Gamma$ and $|B| = l$,
- the list of differences $d - d' \neq 0$, where $d, d' \in B$, contains each nonzero element of Γ precisely λ times.

Proposition 12. *[7] There exists a (N, l, λ) difference set B in $(GF(N), +)$ such that $N = 4t - 1, l = 2t - 1, \lambda = t - 1$, where t is a positive integer.*

Example 2. [7] $B = \{1, 3, 4, 5, 9\}$ is a $(11, 5, 2)$-difference set in $(GF(11), +)$.

4.2 Optimum scheme based on planar difference set

In this subsection we show that if there exists a planar difference set modulo $N = l(l-1) + 1$ such that N is a prime, then there exists a (k, n, δ) secure secret sharing scheme which meets the equality of our bound eq. (6) such that $|\mathcal{S}| = l, \delta = 1/l, n < N$.

Let $B = \{d_0, \ldots, d_{l-1}\}$ be a planar difference set modulo $N = l(l-1) + 1$ such that N is a prime. We show a (k, n, δ) secure secret sharing scheme such that $\mathcal{S} = B$. Assume that S is uniformly distributed over $\mathcal{S}$. In what follows, all operations are done over $GF(N)$.

Distribution phase. For a secret $d_s \in \mathcal{S}(= B)$, the dealer D chooses a random polynomial $f(x)$ of degree $k - 1$ over $GF(N)$ such that $f(0) = d_s$. The share of P_i is given as $v_i = f(i)$. Note that

$$\forall i, \quad |\mathcal{V}_i| = N = l(l-1) + 1. \tag{8}$$

Reconstruction phase. Suppose that $P_{i_1}, \ldots, P_{i_k}$ open $\tilde{v}_{i_1}, \ldots, \tilde{v}_{i_k}$. Each participant computes $\tilde{d}_s = \sum_{j=1}^{k} c_j \tilde{v}_{i_j}$, where $c_j = \prod_{l \neq j}(-i_l)/(i_j - i_l)$ for $1 \leq j \leq k$. If $\tilde{d}_s \in B$, they accept $\tilde{d}_s$ as the secret. Otherwise, they output $\perp$. Note that, for any k honest shares $v_{i_1} = f(i_1), \ldots, v_{i_k} = f(i_k)$,

$$d_s = \textstyle\sum_{j=1}^{k} c_j v_{i_j} \tag{9}$$

from Laglange formula [13].

Proposition 13 (Lagrange formula). *[13] Let $h(x)$ be a polynomial over $GF(N)$ such that $\deg h(x) = k - 1$. For any distinct $i_1, \ldots, i_k$,*

$$h(0) = \sum_{j=1}^{k} c_j h(i_j), \ \textit{where } c_j = \prod_{l \neq j} (-i_l)/(i_j - i_l)$$

Lemma 14. *The proposed scheme is a (k, n) threshold secret sharing scheme.*

Proof. (A1) of Defnition 1 is satisfied from eq. (9). Next,

$$\begin{aligned}&\Pr(S = d_s \mid V_{i_1} = v_{i_1}, \dots, V_{i_{k-1}} = v_{i_{k-1}})\\ &= \frac{\Pr(S = d_s)\Pr(V_{i_1} = v_{i_1}, \dots, V_{i_{k-1}} = v_{i_{k-1}} \mid S = d_s)}{\Pr(V_{i_1} = v_{i_1}, \dots, V_{i_{k-1}} = v_{i_{k-1}})}.\end{aligned}$$

For each $d_s \in \mathcal{S}$, $f(x)$ is randomly chosen and $\deg f(x) = k - 1$. Therefore $V_{i_1} \cdots V_{i_{k-1}}$ is random for each $d_s \in \mathcal{S}$. Hence

$$\Pr(V_{i_1} = v_{i_1}, \dots, V_{i_{k-1}} = v_{i_{k-1}} \mid S = d_s) = \Pr(V_{i_1} = v_{i_1}, \dots, V_{i_{k-1}} = v_{i_{k-1}}).$$

Consequently,

$$\Pr(S = d_s \mid V_{i_1} = v_{i_1}, \dots, V_{i_{k-1}} = v_{i_{k-1}}) = \Pr(S = d_s).$$

Thus (A2) of Defnition 1 is also satisfied. □

Lemma 15. *The proposed scheme is a (k, n, δ) secure secret sharing scheme such that $|S| = l, \delta = 1/l$ and $n < N$. Furthermore, the equality of eq. (6) is satisfied.*

Proof. Suppose that cheaters $P_{i_1}, \dots, P_{i_{k-1}}$ have $b = (v_{i_1}, \dots, v_{i_{k-1}})$. Let the share of P_{i_k} be $x \in \{0, 1, \dots, N-1\}$. Then, from eq. (9),

$$Sec(b, x) = \sum_{j=1}^{k-1} c_j v_{i_j} + c_k x = d_s \in B(= \mathcal{S}). \tag{10}$$

Define

$$T \triangleq \{x \mid Sec(b, x) \in B\}.$$

For any fixed b, eq. (10) defines a bijection τ from B to T such that $\tau(d_s) = x \in T$ because $c_k \neq 0$. Since d_s is uniformly distributed over B, x is uniformly distributed over T. (Remember that S is uniformly distributed over $\mathcal{S}$.) Therefore for any fixed b and b',

$$\Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b) = |\tilde{V}_{i_k}(b \to b')|/|T|, \tag{11}$$

where

$$\tilde{V}_{i_k}(b \to b') = \{x \mid Sec(b, x) \in B, Sec(b', x) \in B \text{ and } Sec(b, x) \neq Sec(b', x)\}.$$

Since τ is a bijection,

$$|T| = |B| = l. \tag{12}$$

Now let's compute $|\tilde{V}_{i_k}(b \to b')|$. Fix $b = (v_{i_1}, \dots, v_{i_{k-1}})$ and $b' = (v'_{i_1}, \dots, v'_{i_{k-1}})$ arbitrarily. Define

$$a \triangleq \sum_{j=1}^{k-1} c_j v_{i_j}, \quad a' \triangleq \sum_{j=1}^{k-1} c_j v'_{i_j}.$$

From eq. (10) and since τ is a bijection,

$$\begin{aligned}|\tilde{V}_{i_k}(b \to b')| &= |\{x \mid a + c_k x \in B, a' + c_k x \in B \text{ and } a + c_k x \neq a' + c_k x\}| \\ &= |\{d \mid d \in B, d - (a - a') \in B \text{ and } a - a' \neq 0\}|\end{aligned}$$

Note that $a - a'$ is a constant for fixed b and b'. On the other hand, from Definition 9, for $\forall e \neq 0$,

$$\begin{aligned}|\{(d, d') \mid d \in B, d' \in B, d - d' = e\}| &= 1 \\ |\{d \mid d \in B, d - e \in B\}| &= 1\end{aligned}$$

since $d' = d - e$. So we obtain

$$|\tilde{V}_{i_k}(b \to b')| \;=\; 1 \tag{13}$$

for b and b' such that $a - a' \neq 0$. If $a - a' = 0$, then $|\tilde{V}_{i_k}(b \to b')| = 0$ because no d (or no x) satisfies $a - a' \neq 0$. Therefore, from eq. (11),(12) and (13),

$$\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b) = 1/l.$$

Consequently, from eq. (5),

$$P(Cheat \mid V_{i_1}, \ldots, V_{i_{k-1}}) \;=\; 1/l.$$

Thus this scheme is a (k, n, δ) secure scheme such that $\delta = 1/l$. It is clear that $|\mathcal{S}| = |B| = l$. Finally, from eq. (8), $\forall j, |\mathcal{V}_j| = N = (l-1)l + 1 = (|\mathcal{S}| - 1)/\delta + 1$. Hence, this scheme meets the equality of eq. (6). □

Now the following theorem is obtained from lemma 14 and 15.

Theorem 16. *If there exists a planar difference set modulo $N = l(l-1) + 1$ such that N is a prime, then there exists a (k, n, δ) secure secret sharing scheme which meets the equality of our bound eq. (6) such that $|\mathcal{S}| = l, \delta = 1/l, n < N$.*

From proposition 10, we obtain the following corollary.

Corollary 17. *Let q be a prime power such that $q^2 + q + 1$ is a prime. Then, there exists a (k, n, δ) secure secret sharing scheme which meets the equality of eq. (6) such that $|\mathcal{S}| = q + 1, \delta = 1/(q + 1)$ and $n < q^2 + q + 1$.*

Remark. Instead of publicizing a planar difference set B itself, it is enough to publicize two points α^0 and α^1 of $PG(2, |\mathcal{S}| - 1)$. According to Proposition 10, B can be obtained from (α^0, α^1).

4.3 Optimum scheme based on a (N, l, λ) difference set

Theorem 16 is generalized as follows.

Theorem 18. *If there exists a (N, l, λ) difference set B in $(GF(N), +)$, then there exists a (k, n, δ) secure secret sharing scheme which meets the equality of our bound eq. (6) such that $|\mathcal{S}| = l, \delta = \lambda/l, n < N$.*

The following corollary is obtained from proposition 12.

Corollary 19. *For a positive integer t such that $4t - 1$ is a prime power, there exists a (k, n, δ) secure secret sharing scheme which meets the equality of our bound eq. (6) such that $|\mathcal{S}| = 2t - 1, \delta = (t-1)/(2t-1), n < 4t - 1$.*

5 Tighter Bound on $|\mathcal{V}_i|$ under the CDV Assumption

In this section, we use the same technique used in subseection 3.2 and, under the CDV assumption, show a lower bound on $|\mathcal{V}_i|$ that is more tight than proposition 5. (The CDV assumption is that $k-1$ cheaters $P_1, \ldots, P_{k-1}$ somehow know the secret s.)

In the distribution phase, suppose that cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ have $b = (v_{i_1}, \ldots, v_{i_{k-1}})$ as their shares of a secret s and P_{i_k} has x as his share. That is, $Sec(b, x) = s$. Fix s and b. Let

$$Y'(x) \triangleq \{v'_{i_1} \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s' \in \mathcal{S}, s' \neq s\}$$
$$W' \triangleq \{x \in \mathcal{V}_{i_k} \mid Sec(b, x) = s\}.$$

In the reconstruction phase, if P_{i_1} opens $v'_{i_1} \in Y'(x)$, then P_{i_k} is cheated. W' denotes the set of possible shares of P_{i_k}.

Lemma 20. *For fixed s and b such that* $\Pr(V_{i_1} \cdots V_{i_{k-1}} = b, S = s) > 0$,

$$|W'| \geq 1/\epsilon. \tag{14}$$

Proof. Consider cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ such that only P_{i_1} opens a forged share $v'_{i_1} (\neq v_{i_1})$. The other $P_{i_2}, \ldots, P_{i_{k-1}}$ open their shares honestly. The way that P_{i_1} opens v'_{i_1} is as follows. First, P_{i_1} chooses $\hat{x} \in W'$ such that

$$\Pr(V_{i_k} = \hat{x} \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = s) = \max_{x \in W'} \Pr(V_{i_k} = x \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = s).$$

Then, P_{i_1} opens $v'_{i_1} \in Y'(\hat{x})$ arbitrarily. In this case, P_{i_k} is cheated if his share is $\hat{x}$. For these specific cheaters, in eq. (4),

$$\begin{aligned}
&\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b. \text{ They also know } s)\\
&\geq \Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b. \text{ They also know } s)\\
&\geq \Pr(V_{i_k} = \hat{x} \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = s)
\end{aligned}$$

$$= \max_{x \in W'} \Pr(V_{i_k} = x \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = s)$$
$$\geq |W'|^{-1} \sum_{x \in W'} \Pr(V_{i_k} = x \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = s)$$
$$\geq |W'|^{-1}.$$

Since the scheme is ϵ-robust, $\epsilon \geq E[|W'|^{-1}] = |W'|^{-1}$. Therefore, we obtain eq. (14). □

Lemma 21. *For* $\forall x \in W'$, $|Y'(x)| \geq (|\mathcal{S}| - 1)/\epsilon$.

Proof. From lemma 20, $|\{y \in \mathcal{V}_{i_1} \mid Sec(y, v_2, \ldots, v_{k-1}, x) = s'\}| \geq 1/\epsilon$. Therefore,

$$\begin{aligned}
|Y'(x)| &= |\bigcup_{s' \in \mathcal{S}, s' \neq s} \{y \in \mathcal{V}_{i_1} \mid Sec(v'_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, x) = s'\}| \\
&= \sum_{s' \in \mathcal{S}, s' \neq s} |\{y \in \mathcal{V}_{i_1} \mid Sec(y, v_2, \ldots, v_{k-1}, x) = s'\}| \\
&\geq \sum_{s' \in \mathcal{S}, s' \neq s} 1/\epsilon \\
&= (|\mathcal{S}| - 1)/\epsilon.
\end{aligned}$$

□

Now, our lower bound on $|\mathcal{V}_i|$ is as follows.

Theorem 22. *In a* (k, n, ϵ) *robust secret sharing scheme,*

$$|\mathcal{V}_i| \geq \frac{|\mathcal{S}| - 1}{\epsilon^2} + 1. \tag{15}$$

Proof. Consider a probabilistic P_{i_1} such as shown in the proof of Theorem 8. For such P_{i_1}, let's compute

$$E[\Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b \text{ and they know } s],$$

where E is taken over v'_{i_1} and Pr() is taken over $x \in W'$. Then from lemma 21,

$$E_{v'_{i_1}}[\Pr_{x \in W'}(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b \text{ and they know } s]$$
$$= E_{x \in W'}[\Pr_{v'_{i_1}}(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b \text{ and they know } s]$$
$$= E_{x \in W'}[|Y'(x)|/(|\mathcal{V}_{i_1}| - 1)]$$
$$\geq (|\mathcal{S}| - 1)/\epsilon(|\mathcal{V}_{i_1}| - 1).$$

Therefore

$$\max_{v'_{i_1}} \Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b \text{ and they know } s)$$
$$\geq E_{v'_{i_1}}[\Pr(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b \text{ and they know } s)]$$
$$\geq (|\mathcal{S}| - 1)/\epsilon(|\mathcal{V}_{i_1}| - 1).$$

Hence

$$\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b \text{ and they know } s)$$
$$\geq (|\mathcal{S}| - 1)/\epsilon(|\mathcal{V}_{i_1}| - 1).$$

Consequently, in a (k, n, ϵ) robust secret sharing scheme,

$$\epsilon \geq E[\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1} \cdots P_{i_{k-1}} \text{ have } b. \text{ They also know } s)]$$
$$\geq (|\mathcal{S}| - 1)/\epsilon(|\mathcal{V}_{i_1}| - 1).$$

Then, eq. (15) is obtained. □

References

1. M. Tompa and H. Woll. "How to share a secret with cheaters". In *Journal of Cryptology, vol.1*, pages 133–138, 1988.
2. A. Shamir. "How to Share a Secret". In *Communications of the ACM, vol.22, no.11*, pages 612–613, 1979.
3. G.R. Blakely. "Safeguarding cryptographic keys". In *Proc. of the AFIPS 1979 National Computer Conference, vol.48*, pages 313–317, 1979.
4. E.D. Karnin, J.W.Green, and M.E. Hellman. "On secret sharing systems". In *IEEE Trans. IT-29, No.1*, pages 35–41, 1982.
5. M. Carpentieri, A. De Santis, and U. Vaccaro. "Size of Shares and Probability of Cheating in Threshold Schemes". In *Proc. of Eurocrypto'93, Lecture Notes in Computer Science, LNCS 765, Springer Verlag*, pages 118–125, 1993.
6. F.J. MacWilliams and N.J.A. Sloane. "The theory of error-correcting codes". In *North-Holland*, pages 397–398, 1981.
7. T.Beth,T, D.Jungnickel and H.Lenz. "Design Theory". In *Cambridge University Press*, pages 260–264, 1993.
8. R.J. McEliece and D.V. Sarwate. "On sharing secrets and Reed-Solomon codes". In *Comm.ACM, 24*, pages 583–584, 1981.
9. T. Rabin and M. Ben-Or. "Verifiable secret sharing and multiparty protocols with honest majority". In *Proc. 21st ACM Symposium on Theory of Computing*, pages 73–85, 1989.
10. E.F. Brickell and D.R. Stinson. "The Detection of Cheaters in Threshold Schemes". In *SIAM J. DISC. MATH, Vol.4, No.4*, pages 502–510, 1991.
11. M. Carpentieri. "A perfect threshold secrety sahring scheme to identify cheaters". In *Designs, Codes and Cryptography, vol.5, no.3*, pages 183–187, 1995.
12. K. Kurosawa, S. Obana, and W. Ogata. "t-cheater identifiable (k,n) threshold secret sharing schemes". In *Proc. of Crypt'95, Lecture Notes in Computer Science, LNCS 963, Springer Verlag*, pages 410–423, 1995.
13. D.R. Stinson. "Cryptography: Theory and Practice". In *CRC Press*, pages 330–331, 1995.