Optimal Improvement Ratios of Multi-Secret Sharing Schemes Can Be Achieved

Justie Su-Tzu Juan [1,a], Jennifer Hui-Chan Tsai [1] and Yi-Chun Wang [1]

[1]*Department of Computer Science & Information Engineering, National Chi Nan University, Nantou, Taiwan*

Abstract. Secret sharing schemes (SSS) deal with activities relative to the secure distribution of a secret among a group of participants who then securely reconstruct the secret by collecting the shares which are held by individuals in qualified sets. A multi-secret sharing scheme (MSSS) is an extension of this where multiple secrets are shared simultaneously and where the performance is estimated using both the maximum improvement and average improvement ratios. In 2003, Crescenzo calculated a lower bound of maximum and average improvement ratios for a MSSS and proposed some special MSSS which achieve the lower bound of the maximum improvement ratio. Wang and Juan deployed a more flexible MSSS to achieve the optimal maxi-mum improvement ratio 2006. This paper provides evidence such that the optimal maximum improvement ratio and the optimal average improvement ratio may both be achieved through even simpler and more flexible MSSS through even simpler and more flexible multi-secret sharing schemes for any arbitrary n and m.

1 Introduction

Secret sharing was invented by Shamir [7] and Blakely [1] independently. A secret sharing scheme (SSS, for short) includes two algorithms (D, R); D refers to the *distribution algorithm* and R refers to the *reconstruction algorithm*. Formally, given a group of participants $P = \{P_1, P_2, \ldots, P_n\}$, the distribution algorithm is executed by a *dealer* who has been given a secret. The dealer then calculates the *shares* S_i and distributes them to each participant P_i. The reconstruction algorithm is executed by authorized subsets of participants who combine their shares to reconstruct the secret. A subset A of P is called a *qualified subset* and a secret can be reconstructed if every participant in A uses their shares and executes the reconstruction algorithm R. $\Gamma \subseteq 2^P$ is an *access structure* which is the set of all qualified subsets.

Let a secret K be chosen from K with the uniform distribution. p_K denotes a probability distribution on K and $p_{S(A)}$ denotes a probability distribution on the shares $S(A)$ given to a subset $A \subseteq P$. A SSS is *perfect* if

$$H(K|A) = \begin{cases} 0 & \text{if } A \in \Gamma \\ H(K) & \text{if } A \notin \Gamma \end{cases}$$

where $H(K)$ and $H(K|A)$ denote the entropy of p_K and the conditional entropy of the joint probability distribution $p_{\mathrm{K}\times S(A)}$, respectively. In other words, when a dealer distributes a shared S_i to every participant P_i, only qualified participants can reconstruct the secret K by using their shares. If we collect all the shares owned by nonqualified subsets, K cannot be reconstructed. Then we call this scheme is *perfect* which means that the nonqualified participants receive no information about the original secret.

Let $S(P_i)$ denote the set of possible shares that P_i might receive. $\rho_i = \log|K| / \log|S(P_i)|$ denotes the *information rate* for P_i. In general, the efficiency of a SSS (D, R) is measured by the information rate ρ defined as $\rho = \min\{\rho_i : 1 \le i \le n\}$ [9]. A SSS (D, R) is *ideal* if $\rho((D, R)) = 1$.

A multi-secret sharing scheme (MSSS, for short) deals with m secrets $s_0, s_1, \ldots, s_{m-1}$ at the same time. The most efficient algorithm of each single SSS can be used for distributing shares and reconstructing the secret. In this case, it is called a *basic MSSS* (b-D, b-R) in which the size of given shares will increase according to the secrets. Notably, the issue of reducing the size of shares given to every participant becomes an important one. Generally, an *Improvement Ratio* (*IR*) is used to estimate the performance of a MSSS. Crescenzo [3] announced a MSSS and studied this issue in 2003. After that, Wang and Juan [10] gave the instances of MSSS to show that the optimal maximum improvement ratio can be achieved for any $n > m$ in 2006.

This paper focuses on the optimal maximum improvement ratios and optimal average improvement ratios of MSSSs such that they can both be achieved in more flexible cases, most notably, for any arbitrary n and m. The next section will lay out Crescenzo's definitions and Wang and Juan's results. Section 3 proposed a MSSS, which extends the results of Crescenzo and Wang and Juan. The proposed scheme is proved to be secure and perfect in Section 4, conclusions are given.

[a] Corresponding author: jsjuan@ncnu.edu.tw

2 Preliminaries

Maximum improvement ratio and *average improvement ratio* are two criteria which are used to estimate the performance of a MSSS. In a MSSS (D, R), the dealer distributes m secrets $s_0, s_1, \ldots, s_{m-1}$ with associated access structures $A_0, A_1, \ldots, A_{m-1}$. The maximum improvement ratio (denoted by MaxIR) and the average improvement ratio (denoted by AvIR) are defined as follows Crescenzo [3]:

$$\text{MaxIR}(A_0, A_1, \ldots, A_{m-1}, (D, R)))$$

$$= \frac{\text{MaxShSize}(A_0, A_1, \ldots, A_{m-1}, (D, R))}{\text{MaxShSize }(A_0, A_1, \ldots, A_{m-1}, (\text{b-}D, \text{b-}R))};$$

$$\text{AvIR}(A_0, A_1, \ldots, A_{m-1}, (D, R)))$$

$$= \frac{\text{AvShSize}(A_0, A_1, \ldots, A_{m-1}, (D, R))}{\text{AvShSize }(A_0, A_1, \ldots, A_{m-1}, (\text{b-}D, \text{b-}R))}.$$

where MaxShSize(A_0, A_1, …, A_{m-1}, (D, R)) and AvShSize(A_0, A_1, …, A_{m-1}, (D, R)) denote, respectively, the maximum size of shares and the total size of shares obtained by the qualified participants when executing the (D, R) algorithm.

Next, the *optimal maximum improvement ratio* (denoted by OpMaxIR) and the *optimal average improvement ratio* (denoted by OpAvIR) are defined for the access structures $A_0, A_1, \ldots, A_{m-1}$ as follows:

$$\text{OpMaxIR}(A_0, A_1, \ldots, A_{m-1})$$

$$= \min_{(D, R)} \text{MaxIR}(A_0, A_1, \ldots, A_{m-1})$$

$$\text{OpAvIR}(A_0, A_1, \ldots, A_{m-1})$$

$$=\min_{(D, R)} \text{AvIR}(A_0, A_1, \ldots, A_{m-1})$$

The following theorems show the lower bounds and upper bounds of OpMaxIR and OpAvIR which are given by Crescenzo [3].

Theorem 1 [3] Let m, n be positive integers and let A_0, A_1, …, A_{m-1} be access structures over a set of size n. It holds that

$$\text{OpMaxIR}(A_0, A_1, \ldots, A_{m-1}) \geq 1 / m,$$
$$\text{OpAvIR}(A_0, A_1, \ldots, A_{m-1}) \geq 1 / m.$$

Theorem 2 [3] Let m be an integer. For any $\varepsilon > 0$, there exist access structures A_0, A_1, …, A_{m-1} such that OpAvIR($A_0, A_1, \ldots, A_{m-1}$) $\geq 1 / m + \varepsilon$.

Theorem 3 [3] Let m be an integer. There exists an integer n and access structures $A_0, A_1, \ldots, A_{m-1}$ over a set of size n such that

$$\text{OpMaxIR}(A_0, A_1, \ldots, A_{m-1}) = 1 / m.$$

In order to prove Theorem 3, Crescenzo provides an instance of MSSS in which the max improvement ratio is equal to $1/m$. He uses one particular access structure and an associative algorithm which are overly complicated and is forced to use some previous results in the literature. In this instance, for any positive integer m, the number of participant $n = m + 6^{d-1}$, where $d = 2(1 + \lceil \log m \rceil) - 1$. For example, if $m = 5$, n will be 46661. Also, to understand this scheme, one must be familiar with the results of Blundo et al. [2], Dijk [4], and Stinson [8]. Furthermore, the other access structures in [2, 5, 6, 8] are not intuitive enough either. Wang and Juan [10] solved this problem and proposed two simple schemes which can directly achieve the lower bound of the OpMaxIR. Additionally, their result shows that the OpMaxIR can be achieved for all cases such that m only needs to be greater than n.

Theorem 4 [10] For any two positive integers $n > m$, there exist access structures $A_0, A_1, \ldots, A_{m-1}$ over a set of size n such that

$$\text{OpAvIR}(A_0, A_1, \ldots, A_{m-1}) = 1 / m.$$

The OpMaxIR is shown to be achievable in Theorem 3 and Theorem **4**. Additionally, the OpAvIR is shown to be nearly achievable in Theorem 2. However, those existing schemes only obtained in some special cases. That is, for any two arbitrary positive integers n (the number of secrets) and m(the number of participants), it is still unknown whether the OpMaxIR and OpAvIR are achievable. Specifically, this paper solves this dilemma such that for any two arbitrary positive integers n and m, and builds a set of access structures with a pair of associative algorithms which obtains both the lower bounds of OpMaxIR and OpAvgIR at the same time.

3 The Proposed Scheme

Let m denote the number of secrets and n denote the number of participants. For convenience, the operations at the footnote are calculated in Z_{n-1} space (in modulo n – 1) for the whole of this work. The m secrets $s_0, s_1, \ldots, s_{m-1}$ are selected from K. Note that ⊕ is the "exclusive-or" operation and this paper defines the "general exclusive-or" operation ⊕ as follows:

Definition 1 *Let I be a nonempty set and U be a universe. For each $i \in I$ let $A_i \subseteq U$. Then I is called an index set (or set of indices), and each $i \in I$ is called an index.*
Under these conditions, say $I = \{i_1, i_2, \ldots, i_k\}$

$$\oplus_{i \in I} A_i = A_{i_1} \oplus A_{i_2} \oplus \ldots \oplus A_{i_k}.$$

A particular access structure is defined as follows. Let the participants $P = \{X_0, X_1, \ldots, X_{n-2}, Y\}$. For $i = 0, 1, \ldots, m - 1$, there are two cases:

1) when $n > m$, access structure A_i of secret s_i is defined as: $A_i = \{A_{i1}, A_{i2}\}$, where $A_{i1} = \{X_i, Y\}$, $A_{i2} = P - A_{i1}$;

2) when $m \geq n$, access structure A_i of secret s_i is defined as: $A_i = \{A_{i1}, A_{i2}\}$, where $A_{i1} = \{X_i, Y\}$, $A_{i2} = P - A_{i1}$ for $0 \leq i \leq n$ - 2; $A_i = \{A_{i1}, A_{i2}\}$, and $A_{i1} = \{Y\}$, $A_{i2} = P - A_{i1}$, for $n - 1 \leq i \leq m - 1$.

When sharing secret s_i for any $0 \leq i \leq m - 1$, two ideal schemes are proposed.At first, a basic MSSS is given.

An ideal SSS (b-*D*, b-*R*) for $A_0, A_1, \ldots, A_{m-1}$:
Distribution algorithm (b-*D*):
When $n > m$:

(1)Select random numbers $a_{i,1}, a_{i,2}, \ldots, a_{i,n-3}$ from K. Let $S_{i,i+j} = a_{i,j}$ for $1 \leq j \leq n - 3$ and $0 \leq i \leq m - 1$.

(2)Select random number $a_{i,n-2}$ and let $S_{i,i} = a_{i,n-2}$ for $0 \leq i \leq m - 1$.

(3)Let $S_{i,i-1} = (\oplus_{j=1}^{n-3} a_{i,j}) \oplus s_i$ for $0 \le i \le m - 1$.

(4)Let $S_{i,y} = s_i \oplus a_{i,n-2}$ for $0 \le i \le m - 1$.

(5)For $0 \le j \le n - 2$, send $S_j = \{S_{0,j}, S_{1,j}, \ldots, S_{m-1,j}\}$ to X_j and send $S_y = \{S_{0,y}, S_{1,y}, \ldots, S_{m-1,y}\}$ to Y.

When $n \le m$:

For $0 \le i \le n - 2$, the share S_i of A_i is given as same as the case of $n > m$; and for $n - 1 \le i \le m - 1$, the share S_i is given as follows:

(1)Select random numbers $a_{i,1}, a_{i,2}, \ldots, a_{i,n-1}$ from K. Let $S_{i,i+j} = a_{i,j}$ for $1 \le j \le n - 1$.

(2)Let $S_{i,0} = (\oplus_{j=1}^{n-1} a_{i,j}) \oplus s_i$ and $S_{i,y} = s_i$.

(3)For $n - 1 \le i \le m - 1$, $0 \le j \le n - 2$, send $S_j = \{S_{0,j}, S_{1,j}, \ldots, S_{m-1,j}\}$ to X_j and send $S_y = \{S_{0,y}, S_{1,y}, \ldots, S_{m-1,y}\}$ to Y.

Reconstruction algorithm (b-*R*):

(1)If the shares in A_{i1} are collected, for $0 \le i \le m - 1$, s_i can be reconstructed by using $S_{i,i} \oplus S_y$.

(2)If the shares in A_{i2} are collected, for $0 \le i \le m - 1$, s_i can be reconstructed by using $\oplus$ operations to $S_{i,k}$ for all X_k in A_{i2}.

According to the above algorithms, the results are as follows:

$$\text{AvShSize}(A_0, \ldots, A_{m-1}, (\text{b-}D, \text{b-}R)) = mn,$$
$$\text{MaxShSize}(A_0, \ldots, A_{m-1}, (\text{b-}D, \text{b-}R)) = m;$$

Actually, for the same access structures $A_0, \ldots, A_{m-1}$ of multi-secret $s_0, \ldots, s_{m-1}$, there exists an efficient MSSS (G-*D*, G-*R*) which is given:

An efficient MSSS (G-*D*, G-*R*) for $A_0, A_1, \ldots, A_{m-1}$:
Distribution algorithm (b-*D*):

When $n > m$:

(1)Select random numbers $Q_1, Q_2, \ldots, Q_k$ from K, where $k = n - m$ if n is even, otherwise $k = n - m - 1$. Let $s_{m+l-1} = Q_1$ for $1 \le l \le k$ and $m' = m + k$.

(2)For $0 \le j \le n - 2$, calculate $S_j = \oplus_{0 \le i \le m'-1, i \ne j} s_i$ and send S_j to X_j.

(3) Calculate $S_y = \oplus_{i=0}^{m'-1} s_i$ and send S_y to Y.

(4) If n is even, add one unreal person U_1 and publish the value of $\oplus_{i=0}^{n-2} s_i$ to U_1 as the share.

When $n \le m$:

(1)Add unreal persons $U_1, U_2, \ldots, U_k$ into P where $\text{k} = m + 1 - n$ if m is even, otherwise $k = m + 2 - n$. Let $n' = n + k$ and $X_{n-2+1} = U_1$ for $1 \le l \le k$.

(2)If m is odd, select a random number Q_1 and let $s_m = s_{n'-2} = Q_1$.

(3)For $0 \le j \le n' - 2$, calculate $S_j = \oplus_{0 \le i \le n'-2, i \ne j} s_i$ and send S_j to X_j.

(4)Calculate $S_y = \oplus_{i=0}^{n'-2} s_i$ and send S_y to Y.

Note that the shares sent to unreal persons are actually published.

Reconstruction algorithm (G-*R*):

(1)If the shares in A_{i1} are collected, for $0 \le i \le m - 1$, s_i can be reconstructed by $S_i \oplus S_y \oplus$ published shares if necessary.

(2)If the shares in A_{i2} are collected, for $0 \le i \le m - 1$, s_i can be reconstructed by $\oplus_{0 \le i \le n-2, j \ne i} s_i \oplus$ published shares if necessary.

In algorithm G-*R* (2), note that in the equation when reconstructing s_i, if $n > m$, then let n' equal to n if n is odd; n' will be equal to $n + 1$ otherwise. The secret s_i appears exactly $n' - 2$ times and for any $j \ne i$, s_j appears exactly $n' - 3$ times. Since n' is always an odd number, after exclusive-or calculations, it results in s_i.

According to the above algorithms, the results are as follows:

$$\text{AvShSize}(A_0, \ldots, A_{m-1}, (\text{G-}D, \text{G-}R)) = n,$$
$$\text{MaxShSize}(A_0, \ldots, A_{m-1}, (\text{G-}D, \text{G-}R)) = 1.$$

The published shares are over K^{α}, where α shows as Table 1. Table 2 shows two examples. In (a), $m = 4$ and $n = 5$; in (b), $m = 3$ and $n = 4$.

Table 1. The The number of published shares α

	$n > m$	$n \le m$
$\max\{n,m\}$ is even	1	$m - n + 1$
$\max\{n,m\}$ is odd	0	$m - n + 2$

Table 2. Shares in two examples.

(a) for $m = 4$ and $n = 5$.

	(b-*D*, b-*R*)	(G-*D*, G-*R*)
X_0	$a_{0,3}, s_1 \oplus a_{1,1} \oplus a_{1,2}, a_{2,2}, a_{3,1}$	$s_1 \oplus s_2 \oplus s_3$
X_1	$a_{0,1}, a_{1,3}, s_2 \oplus a_{2,1} \oplus a_{1,2}, a_{3,2}$	$s_0 \oplus s_2 \oplus s_3$
X_2	$a_{0,2}, a_{1,1}, a_{2,3}, s_3 \oplus a_{3,1} \oplus a_{3,2}$	$s_0 \oplus s_1 \oplus s_3$
X_3	$s_0 \oplus a_{0,1} \oplus a_{0,2}, a_{1,2}, a_{2,1}, a_{3,3}$	$s_0 \oplus s_1 \oplus s_2$
Y	$s_0 \oplus a_{0,3}, s_1 \oplus a_{1,3}, s_2 \oplus a_{2,3}, s_3 \oplus a_{3,3}$	$s_0 \oplus s_1 \oplus s_2 \oplus s_3$

(b) for $m = 3$ and $n = 4$.

	(b-*D*, b-*R*)	(G-*D*, G-*R*)
X_0	$a_{0,2}, s_1 \oplus a_{1,1}, a_{2,1}$	$s_1 \oplus s_2 \oplus Q_1$
X_1	$a_{0,1}, a_{1,2}, s_2 \oplus a_{2,1}$	$s_0 \oplus s_2 \oplus Q_1$
X_2	$s_0 \oplus a_{0,1}, a_{1,1}, a_{2,2}$	$s_0 \oplus s_1 \oplus Q_1$
U_1	No unreal participant	$s_0 \oplus s_1 \oplus s_2$
Y	$s_0 \oplus a_{0,2}, s_1 \oplus a_{1,2}, s_2 \oplus a_{2,2}$	$s_0 \oplus s_1 \oplus s_2 \oplus Q_1$

4 Security Analysis

Whether the efficient MSSS can be secure and perfect must be proven. This study proves that, in addition to the fact that the subset belongs to the specific access structure, when collecting any other shares there is no way to reconstruct the original secret or even glean any information about the secret.

Theorem 5 *After executing the algorithm G-D, collect all the shares belong to the participants in any subset A of P that does not include A_{i1} and A_{i2}, there is no way to reconstruct the secret s_i*, and $H(s_i|A) = H(s_i)$.

Proof. According to the properties of $\oplus$, it is not satisfied with a combination rule. Consequently, there is no way in which four fundamental operations of arithmetic can cancel the information excluding s_i but also the calculation is made more complicated. Notably, the inverse operation of $\oplus$ is itself. Therefore, by using $\oplus$, whether one can obtain any information about s_i when one collects all the shares in any subset A of P that does not include any qualified subset of A_i. In this proof, we take into account the added unreal persons $U_1, U_2, \ldots, U_k$ and random numbers $Q_1, Q_2, \ldots, Q_k$ as real persons $X_{n-2+1} = P_l$ and real secrets $s_{m+l} = Q_l$ for $1 \le l \le k$. Note that $P = \{X_0, X_1, \ldots, X_{n-1}, Y\}$, and let n' and m' be the new number of participants and secrets, respectively. Now, $n' = m' + 1$ if m' is even and $n' = m' + 2$ otherwise. For any subset $A \subseteq P$, A does not include all sets in A_{i1} or A_{i2}. According to the associative and commutative properties of ⊕, a series of exclusive-or operations can be taken when executing multiple exclusive-or operations. Therefore, we only have to prove that there is no way to reconstruct s_i when executing exclusive-or operations for any subset of A. In other words, for any subset A of P, let

$$T = \begin{cases} \oplus_{\forall X_j \in A} S_j \oplus S_y & \text{if } Y \in S \\ \oplus_{\forall X_j \in A} S_j & \text{if } Y \notin S \end{cases}$$

If A_{i1} and $A_{i2} \not\subset A$, we must show that $T \neq s_i$. If $|A| \ge n' - 1$, A is definitely includes A_{i1} or A_{i2}. On the other hand, if $|A| = 1$, besides $m \ge n$ and $n - 1 \le i \le m - 1$, $Y \in A_{i1}$, implies Y can reconstruct the secret alone, in another subset A which does not include A_{i1} or A_{i2}; because there is only one participant in A, it is easy to verify that $T \neq s_i$. Therefore, only $2 \le |A| \le n' - 2$ needs to be considered. Note that $A_{i1} = \{X_i, Y\} \not\subset A$, so we have the following three cases.

Case 1. When $|A|$ is even and $X_i \notin A$ or when $|A|$ is odd and $X_i \in A$: Since each share of A contains s_i except S_i, there are even numbers of s_i in A in this situation. Therefore, the s_i will be cancelled after executing exclusive-or operations. Hence, it results $T \neq s_i$.

Case 2. When $|A|$ is even and $X_i \in A$ (hence $Y \notin A$): For any $X_j \in A$, each S_k contains s_j for any $X_k \in A$ except S_j. Thus, there is an odd number of s_j. Since $|A| \ge 2$, then $T = \oplus_{\forall X_j \in A} S_j = s_i \oplus s_{j1} \oplus s_{j2} \oplus \ldots \oplus s_{|A|-1} \neq s_i$, for $X_i, X_{j1}, X_{j1}, \ldots, X_{|A|-1} = A$

Case 3. When $|A|$ is odd, $X_i \notin A$: Since $A_{i2} = P - A_{i2} \not\subset A$, there exists a number $k \in \{0, 1, \ldots, n' - 1\}$ such that $k \neq i$ and $X_k \neq A$. For any $X_j \in A$, each S_j contains s_k and there is an odd number of s_k when calculating T. Therefore, it results $T \neq s_i$.

According to these cases, if we take unreal persons and secrets to be real ones, we still have proven that under ⊕, excluding the specific access structures A_{i1} and A_{i2}, there is no possibility of reconstructing s_i and no information has been revealed regarding the secret s_i.
Hence, it results $H(s_i|A) = H(s_i)$ for any secret s_i.

Therefore, we have proven that the proposed MSSS is perfect and secure.

The values of MaxIR and AvIR of (G-D, G-R) for the specific access structures $A_0, A_1, \ldots, A_{m-1}$ are given, and according to Theorem 1, Theorem 6 is concluded.

Theorem 6 For any two positive integers m and n, there exist access structures $A_0, A_1, \ldots, A_{m-1}$ over a set of size n such that

$$\text{OpMaxIR}(A_0, A_1, \ldots, A_{m-1}) = 1/m,$$
$$\text{OpAvIR}(A_0, A_1, \ldots, A_{m-1}) = 1/m.$$

5 Conclusions

This paper has successfully proven that there exists a set of access structures and an associated MSSS which can achieve:

$$\text{OpAvIR}(A_0, \ldots, A_{m-1}) = 1/m,$$
$$\text{OpMaxIR}(A_0, \ldots, A_{m-1}) = 1/m.$$

Although this result may be largely of theoretical interest and the access structure will likely seldom be used in practical, it encourages further inquiry for any one that may attempt to design a MSSS. Specifically, when designing an efficient MSSS, the maximum and average improvement ratios should approach $1/m$. Since the results in [3]. are a special case (m is decided according to n), this work has extended (for both cases) and improved (for the case of OpAvIR) the results of [3] and [10]. Therefore, this scheme is considered flexible, and thereby generally applicable, because the number of participants and secrets are independent. In conclusion, given a set of access structures for any number of participants and secrets, finding an associated MSSS which can achieve two optimal improvement ratios at the same time is possible.

References

1. G.R. Blakley, Safeguarding cryptographic keys. *Proceedings of the National Computer Conference*, 48 of American Federation of Information Processing Societies, pp. 313-317 (1979)
2. C. Blundo, A.D. Santis, R.D. Simone, U. Vaccaro, Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography* **11**, 2, pp. 107-122 (1997)
3. G.D. Crescenzo, Sharing one secret vs. sharing many secrets. *Theoretical Computer Science*, **295**, pp. 123-140 (2003)
4. M.V. Dijk, On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography* **6**, pp. 143-169 (1995)
5. W.A. Jackson, K.M. Martin, C.M. O'Keefe, A construction for multi-secret threshold schemes. *Designs, Codes and Cryptography* **9**, pp. 287-303(1996)
6. W.A. Jackson, K.M. Martin, C.M. O'Keefe, Ideal secret sharing schemes with multiple secrets. *Journal of Cryptology* **9**, pp. 233-250 (1996)
7. A. Shamir, How to share a secret. *Communications of the ACM* **22**, 11, pp. 612-613 (1979)
8. D.R. Stinson, An explication of secret sharing schemes. *Designs, Codes and Cryptography* **2**, pp. 357-390 (1992)
9. D.R. Stinson, *Cryptography: Theory and practice.* CRC Press (1995)
10. Y.-C. Wang, J.S.-T. Juan, Simple multi-secret sharing schemes to achieve the optimal maximum improvement ratio. *Proc. of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 58-63 (2006)