Secret Sharing Scheme with Perfect Concealment

Izumi Takeuti
National Institute of Advanced Industrial Science and Technology
takeuti.i@aist.go.jp

Tomoko Adachi
Shizuoka Institute of Science and Technology
adachi.tomoko@sist.ac.jp

February 27, 2023

Abstract

In 1979, Shamir and Blakley introduced secret sharing schemes to provide both security and reliability. In this study, we construct two secret sharing schemes with perfect concealment. The first is an (n, n)-threshold scheme by a group. Although the scheme itself is already known, we prove that its concealment is perfect. We propose the second as a new $(2, n)$-threshold scheme by a quasigroup.
Keywords: Probabilistic Concealment, Threshold Scheme, Latin Square, Perfect Security, Quasigroup, Mutual Orthogonality
MSC2022: 94A62, 60B99

1 Introduction

In this study, we construct two secret sharing schemes with perfect concealment.

As discussed in prior works [1, 7], secret sharing schemes provide both security and reliability. In a (t, n)-threshold scheme, which is one of the most typical secret sharing schemes, the secret is divided into n shadows and delivered to n participants, where t of participants together can recover the secret, but fewer than t cannot. IN terms of security, even if $t - 1$ of the shadows are leaked, the secret remains concealed. As for reliability, even if $n - t$ of the shadows are destroyed, the secret can still be recovered.

In this study, we provide two main results on secret sharing schemes with perfect concealment.

Our first main result is the proof of the perfect concealment provided by an (n, n)-threshold scheme constructed by a group. Although this scheme itself is already known. the proof of its perfect concealment is a contribution of the present work. This result appears as Proposition 2 in Subsection 4.2.

We also present a novel $(2, n)$-threshold scheme constructed by a quasigroup with perfect concealment as our second main result, which appears as Theorem 5 in Subsection 6.2.

A quasigroup is equivalent to a Latin square; that is, there exists a bijection between the set of all quasigroups of order q and the set of all Latin squares with a size of $q \times q$ as described in the Theorem 1.1.1 in the book [5]. Researches on secret sharing schemes by Latin squares has been undertaken for some time, and some methods have been reported in a prior work [2, 11]. The scheme provided in [2] does not provide perfect concealment. In this study, we propose secret sharing schemes with perfect concealment, and prove that an existing scheme has the same property. The precise definition of perfect concealment is given in Subsection 2.2. The authors of [11] propose an (n, n)-threshold scheme with perfect concealment, which is an application of the (n, n)-threshold scheme in Subsection 4.2 of the present work. The precise commentaries of these studies [2, 11] appear in Section 7.

The concept of perfect concealment is sometimes referred to as perfect security [10]. Security refers to a property of a phenomena, and the word 'concealment' describes an action which makes a phenomena. In this work, we refer to "perfect concealment" to focus on an action rather than a property. Note that the concept of perfect concealment has also been discusses as 'information-theoretical concealment' [12, 13].

The remainder of this study article is organised constructed as follows. Section 2 briefly reviews some preliminaries to probability theory and the definition of perfect concealment. In Section 3, we give the definition of secret sharing schemes. Section 4 describes secret sharing schemes by groups. The proof of the perfect concealment provided by the scheme in Subsection 4.2 is the first main result of this study. Section 5 provides definitions and some known results on quasigroups and mutual orthogonality. Section 6 gives secret sharing schemes by quasigroups. Subsection 6.2 provides the other main result of this study, which is a $(2, n)$-threshold scheme by quasigroups with perfect concealment. Section 7 discusses related works.

2 Concealment

The concept of concealment includes concepts from probability theory. Therefore, this section consists of preliminaries on probability theory and gives definitions of concealment.

2.1 Preliminaries to Probability Theory

This subsection gives preliminaries of probability theory including the definitions of uniformity, independency, prior distribution and posterior distribution.

The probability space consists of a triple $(\Omega, \mathcal{B}, \mu)$, where Ω is the set of elementary events, $\mathcal{B}$ is the set of measurable sets over Ω, and μ is the probability measure. In this study, the set Ω is always finite, and $\mathcal{B}$ is always the power set

of Ω. The letters X, Y, Z, and so forth are used for random variables. A random variable X represents a function f_X of Ω into V_X which is the set within which the value of X ranges. The notation $\Pr[X = x]$ denotes $\mu(\{\omega \in \Omega | f_X(\omega) = x\})$. The notation $|S|$ for a finite set S denotes the number of the elements of S, while $|r|$ for a real number r is the absolute value of r.

Definition 1 (Uniformity and Independency) The distribution of X is *uniform* when, for each $x \in V_X$, $\Pr[X = x] = 1/|V_X|$. Random variables X and Y are *independent* or X is *independent* of Y when, for each $x \in V_X$ and each $y \in V_Y$, $\Pr[X = x, Y = y] = \Pr[X = x] \cdot \Pr[Y = y]$.

The joint probability distribution of X and Y is the distribution
$(x, y) \mapsto \Pr[X = x, Y = y] : V_X \times V_Y \to [0, 1]$.

Definition 2 (Prior and Posterior Distributions) Here, we define the joint probability distribution of X and Y.

The *prior distribution* of X is the distribution
$x \mapsto \Pr[X = x] = \sum_y \Pr[X = x, Y = y] : V_X \to [0, 1]$.
The *posterior distribution* of X after observing $Y = y$ is the distribution
$$x \mapsto \frac{\Pr[X = x, Y = y]}{\Pr[Y = y]} : V_X \to [0, 1].$$

If the random variables X and Y are independent, then the posterior distribution of X after observing Y is equal to its prior distribution before observing Y.

2.2 Perfect Concealment

There are several concepts of concealment. Some works have provided lists with up to six different concepts of concealment [12, 13]. In this study, we consider four concepts of concealment are discussed.

The concepts of possibilistic concealment and probabilistic concealment are defined as follows.

Possibilistic concealment There exist plural possibilities for the value of the secret, and the intruder cannot tell which is the value of the secret.

Probabilistic concealment After the intruder observes the observable variables, the posterior distribution of the secret remains equal to or very close to the prior distribution of the secret.

The concept of 'very close' is to be defined formally as in the definition of asymptotic concealment below.

Two concepts of possibilistic and probabilistic concealment have been considers in several works [4, 12, 13, 14]. The concept of possibilistic concealment is called 'concealment under a non-probabilistic argument' in the work [14]. Some authors [4, 14] have considered possibilistic concealment as weaker than probabilistic concealment, and probabilistic concealment is thus preferred in terms of the security of cryptographic protocols.

In this study, we also discuss two other concepts of concealment which are refinements of the concept of probabilistic concealment.

Asymptotic concealment Suppose that the secret X is either x_1 or x_0 with a probability of $1/2$. For an arbitrary polynomial p, there exists a large number N such that for any security parameter $n > N$ as large as the length of the encryption key, the distance $|\Pr[X = X'] - 1/2|$ is smaller than $1/p(n)$ in computation time $p(n)$, for the computation result X'.

Perfect concealment After an intruder observes the observable variables, the posterior distribution of the secret is equal to the prior distribution of the secret.

The concept of asymptotic concealment appears in the context of public-key cryptography [3]. Perfect concealment is sometimes referred to as perfect security [10], or information-theoretic concealment [12, 13].

Based on the discussion in the previous subsection, the following remark holds.

Remark 1 *A protocol provides perfect concealment if the secret X and the observable variable Y are independent.*

3 Secret Sharing Schemes

In this study, we consider only secret sharing schemes as secret sharing schemes. We refer to the explanation of threshold secret sharing schemes given in [9] as follows.

> A (t, w)-threshold scheme is a method of sharing a secret key K among a finite set P of w participants, in such a way that any t participants can compute the value of K, but no group of $t - 1$ participants can do so. The value of K is chosen by a special participant called the dealer. The dealer is denoted by D and we assume $D \notin P$. When D wants to share the key K among the participants in P, he gives each participant some partial information called a share. The shares should be distributed secretly, so no participant knows the share given to another participant.
>
> At a later time, a subset of participants $B \subset P$ will pool their shares in an attempt to compute the secret key K. If $|B| \geq t$, then they should be able to compute the value of K as a function o f the shares they collectively hold; if $|B| < t$, then they should not be able to compute K.

Shamir's scheme [7] is a well-known example of a threshold scheme. He showed only the possibilistic concealment of the scheme. Although he did not mention perfect concealment, the scheme does provide perfect concealment [14].

We consider the following the mathematical definitions of threshold schemes and of their perfect concealment as followings.

Definition 3 (Randomised Algorithm) Let X, Y and Z be random variables. Let V_X be the set in which the value of X ranges. Take the sets V_Y and V_Z similarly. Let f be a function of $V_X \times V_Y$ into V_Z.

Then, a scheme $Z = f(X, Y)$ is called to be a *randomised algorithm* with input X, random oracle Y, and output Z if the following conditions hold.
(1) The distribution of Y is uniform.
(2) The random variables X and Y are independent.
(3) $Z = f(X, Y)$ at each elementary event $\omega \in \Omega$.

We refer to the random oracles explicitly in this article, although they are often omitted in the literature.

Definition 4 (Threshold Scheme) Take a randomised algorithm $(Z_1, Z_2, ..., Z_n) = f(X, Y)$ with input X, random oracle Y, and output $(Z_1, Z_2, ..., Z_n)$.

Suppose that, for each sequence $S = (i_1, i_2, ..., i_t) \in \{1, 2, ..., n\}^t$ where all of i_j's are distinct, there is a function $\tilde{f}_S$ such that, if $(z_1, z_2, ..., z_n) = f(x, y)$, then it holds that $x = \tilde{f}_S(z_{i_1}, z_{i_2}, ..., z_{i_t})$ for each $x \in V_X, y \in V_Y, z_1 \in V_{Z_1}, z_2 \in V_{Z_2}, ..., z_n \in V_{Z_n}$.

Then, this randomised algorithm $(Z_1, Z_2, ..., Z_n) = f(X, Y)$ is regarded as a (t, n)-*threshold scheme* which proceeds as follows.

The function f is public. There is a secret $X \in V_X$. The dealer chooses a random oracle $Y \in V_Y$ such that the distribution of Y is uniform and Y is independent of X. The dealer calculates $Z_1, Z_2, ..., Z_n$ such as $(Z_1, Z_2, ..., Z_n) = f(X, Y)$, and delivers the shadow Z_i to the participant P_i.

The party of t participants $P_{i_1}, P_{i_2}, ..., P_{i_t}$ together can recover the secret X because $X = \tilde{f}_S(Z_{i_1}, Z_{i_2}, ..., Z_{i_t})$ where $S = (i_1, i_2, ..., i_t)$.

Definition 5 (Perfect Concealment) A (t, n)-threshold scheme $(Z_1, Z_2, ..., Z_n) = f(X, Y)$ provides *perfect concealment* if, for any subset $\{i_1, i_2, ..., i_{t-1}\} \subset \{1, 2, ..., n\}$, the random variable X is independent of $(Z_{i_1}, Z_{i_2}, ..., Z_{i_{t-1}})$.

4 Threshold Schemes by Groups

In this section, we constructs two threshold schemes. That in Subsection 4.1 is a simple example of a $(2, 2)$-threshold scheme. Subsection 4.2 gives a (n, n)-threshold scheme. This scheme itself is already known and has been considers in prior works [11]. More precise commentary is given in Subsection 7.2. We proves the perfect concealment of this scheme as the first main result of this study.

4.1 Simple Threshold Scheme by a Group

We constructs a (2,2)-threshold scheme by a finite group G. This is quite a simple example of a threshold scheme. The authors of the prior study [15] construct a (2,2)-threshold scheme by the group $(\{0, 1\}, \oplus)$; we provide a generalisation of their approach.

Definition 6 (Threshold Scheme I) Let G be a finite group. *Threshold Scheme I* is a scheme defined by the randomised algorithm.

$(Z_1, Z_2) = f_{\mathrm{I}}(X, Y) = (Y, XY)$

with input $X \in G$, random oracle $Y \in G$, and output $(Z_1, Z_2) \in G^2$.

This Threshold Scheme I proceeds as follows.

Consider a dealer and two participants P_1 and P_2. All the data of a finite group G are public. There exists a secret $X \in G$. The dealer chooses $Y \in G$ such that the distribution of Y is uniform and Y is independent of X. The dealer gives $Z_1 = Y$ to the participant P_1 and $Z_2 = XY$ to the other participant P_2.

Then, the next theorem holds.

Theorem 1 *Threshold Scheme I is a (2,2)-threshold scheme providing perfect concealment.*

Proof. We prove the following. (1) X is recovered from $Z_1 = Y$ and $Z_2 = XY$. (2) X is independent both of $Z_1 = Y$ and of $Z_2 = XY$.

(1) is simple because $X = Z_2 Z_1^{-1}$. (2) is shown as follows. First, X is independent of $Z_1 = Y$ by the assumption. Next, X is independent of Z_2 by the next proposition. ∎

Proposition 1 *Let G be a finite group, and X and Y be random variables over G. Suppose that the distribution of Y is uniform, X and Y are independent, and $Z = XY$. Then, (1) the distribution of Z is uniform, and (2) X and Z are independent.*

Proof. (1) For any $z \in G$,

$\Pr[Z = z] = \Pr[XY = z] = \sum_{x \in G} \Pr[X = x, xY = z]$

$= \sum_{x \in G} \Pr[X = x, Y = x^{-1}z] = \sum_{x \in G} \Pr[X = x] \cdot \Pr[Y = x^{-1}z]$

$= \sum_{x \in G} (\Pr[X = x]/|G|) = (\sum_{x \in G} \Pr[X = x])/|G| = 1/|G|$.

(2) For any $x, z \in G$,

$\Pr[X = x, Z = z] = \Pr[X = x, XY = z] = \Pr[X = x, Y = x^{-1}z]$

$= \Pr[X = x] \cdot \Pr[Y = x^{-1}z] = \Pr[X = x]/|G|$.

By the discussion of (1), we have $\Pr[Z = z] = 1/|G|$; therefore

$\Pr[X = x, Z = z] = \Pr[X = x] \cdot \Pr[Z = z]$. ∎

4.2 (n, n)-Threshold Scheme by a Group

The (2,2)-threshold scheme in Subsection 4.1 can be generalised into an (n, n)-threshold scheme.

Definition 7 (Threshold Scheme II) Let G be a finite group. *Threshold Scheme II* is a scheme defined by the randomised algorithm:

$(Z_1, Z_2, ..., Z_n) = f_{\mathrm{II}}(X, Y_1, Y_2, ..., Y_{n-1})$

$= (Y_1, Y_2, ..., Y_{n-1}, Y_{n-1}^{-1} Y_{n-2}^{-1} ... Y_1^{-1} X)$

with input $X \in G$, random oracles $Y_1, Y_2, ..., Y_{n-1} \in G$ and output $(Z_1, Z_2, ..., Z_n) \in G^n$.

This Threshold Scheme II proceeds as follows.

Consider a dealer and n participants $P_1, P_2, ..., P_n$. All the data of a finite group G are public. There exists a secret $X \in G$. The dealer chooses $Y_1, Y_2, ..., Y_{n-1} \in G$ such that each distribution of Y_i is uniform, and $X, Y_1, Y_2, ...,$ Y_{n-2} and Y_{n-1} are independent. The dealer gives $Z_i = Y_i$ to the participant P_i for $i = 1, 2, ..., n-1$, and gives $Z_n = Y_{n-1}^{-1} Y_{n-2}^{-1} ... Y_1^{-1} X$ to the participant P_n.

Then, the next theorem holds.

Theorem 2 *Threshold Scheme II is an (n,n)-threshold scheme providing perfect concealment.*

Proof. We will prove the following: (1) X is recovered from $Z_1, Z_2, ..., Z_n$. (2) X is independent of $(Z_1, ..., Z_{i-1}, Z_{i+1}, ..., Z_n)$ for each $i \in \{1, 2, ..., n\}$.

(1) is simple because $X = Z_1 Z_2 ... Z_n$. (2) is shown as follows. First, X is independent of $(Z_1, Z_2, ..., Z_{n-1}) = (Y_1, Y_2, ..., Y_{n-1})$ by the assumption. Next, X is independent of $(Z_1, ..., Z_{i-1}, Z_{i+1}, ..., Z_n)$ for each $i \in \{1, 2, ..., n-1\}$ by the next proposition. ∎

Proposition 2 *Let G be a finite group and $X, Y_1, Y_2, ..., Y_{n-1}$ be random variables over G. Suppose that the distribution of Y_i is uniform for each i, the distributions of $X, Y_1, Y_2, ..., Y_{n-2}$ and Y_{n-1} are independent, and $Z = Y_{n-1}^{-1} Y_{n-2}^{-1} ... Y_1^{-1} X$. Then, (1) the distribution of Z is uniform, and (2) the random variables $X, Y_1, Y_2, ..., Y_{i-1}, Y_{i+1}, ..., Y_{n-1}$ and Z are independent for each i.*

Proof. (1) For any $z \in G$,

$$\begin{aligned}
&\Pr[Z = z] = \Pr[Y_{n-1}^{-1} Y_{n-2}^{-1} ... Y_1^{-1} X = z] = \Pr[X = Y_1 Y_2 ... Y_{n-1} z] \\
&= \Pr[Y_1 = X z^{-1} Y_{n-1}^{-1} Y_{n-2}^{-1} ... Y_2^{-1}] \\
&= \textstyle\sum_{x, y_2, y_3, ..., y_{n-1} \in G} \Pr[X = x, Y_2 = y_2, Y_3 = y_3, ..., Y_{n-1} = y_{n-1}, \\
&\qquad\qquad Y_1 = x z^{-1} y_{n-1}^{-1} y_{n-2}^{-1} ... y_2^{-1}] \\
&= \textstyle\sum_{x, y_2, y_3, ..., y_{n-1} \in G} \Pr[X = x, Y_2 = y_2, Y_3 = y_3, ..., Y_{n-1} = y_{n-1}] \\
&\qquad\qquad \Pr[Y_1 = x z^{-1} y_{n-1}^{-1} y_{n-2}^{-1} ... y_2^{-1}] \\
&= \textstyle\sum_{x, y_2, y_3, ..., y_{n-1} \in G} \Pr[X = x, Y_2 = y_2, Y_3 = y_3, ..., Y_{n-1} = y_{n-1}] / |G| \\
&= (\textstyle\sum_{x, y_2, y_3, ..., y_{n-1} \in G} \Pr[X = x, Y_2 = y_2, Y_3 = y_3, ..., Y_{n-1} = y_{n-1}]) / |G| \\
&= 1/|G|.
\end{aligned}$$

(2) Note that $x = y_1 y_2 ... y_{n-1} z$ iff $y_i = y_{i-1}^{-1} y_{i-2}^{-1} ... y_1^{-1} x z^{-1} y_{n-1}^{-1} y_{n-2}^{-1} ... y_{i+1}^{-1}$.

For any $x, y_1, y_2, ... y_{i-1}, y_{i+1}, ..., y_{n-1}, z \in G$,

$$\begin{aligned}
&\Pr[X = x, Y_1 = y_1, Y_2 = y_2, ..., Y_{i-1} = y_{i-1}, \\
&\qquad\qquad Y_{i+1} = y_{i+1}, ..., Y_{n-1} = y_{n-1}, Z = z] \\
&= \Pr[X = x, Y_1 = y_1, Y_2 = y_2, ..., Y_{i-1} = y_{i-1}, \\
&\qquad Y_i = y_{i-1}^{-1} y_{i-2}^{-1} ... y_1^{-1} x z^{-1} y_{n-1}^{-1} y_{n-2}^{-1} ... y_{i+1}^{-1}, Y_{i+1} = y_{i+1}, ..., Y_{n-1} = y_{n-1}] \\
&= \Pr[X = x] \Pr[Y_1 = y_1] \Pr[Y_2 = y_2] ... \Pr[Y_{i-1} = y_{i-1}] \\
&\quad \Pr[Y_i = y_{i-1}^{-1} y_{i-2}^{-1} ... y_1^{-1} x z^{-1} y_{n-1}^{-1} y_{n-2}^{-1} ... y_{i+1}^{-1}] \\
&\quad \Pr[Y_{i+1} = y_{i+1}] ... \Pr[Y_{n-1} = y_{n-1}] \\
&= \Pr[X = x] / |G|^{n-1}.
\end{aligned}$$

By the discussion of (1), we have $\Pr[Z = z] = 1/|G|$; therefore,

$$\begin{aligned}
&\Pr[X = x, Y_1 = y_1, Y_2 = y_2, ..., Y_{i-1} = y_{i-1},
\end{aligned}$$

$$Y_{i+1} = y_{i+1}, ..., Y_{n-1} = y_{n-1}, Z = z]$$
$$= \Pr[X = x]/|G|^{n-1}$$
$$= \Pr[X = x] \Pr[Y_1 = y_1] \Pr[Y_2 = y_2] ... \Pr[Y_{i-1} = y_{i-1}]$$
$$\Pr[Y_{i+1} = y_{i+1}] ... \Pr[Y_{n-1} = y_{n-1}] \Pr[Z = z].$$ ∎

This proposition is the first main result of this study.

The secret sharing scheme in [11] essentially uses this (n, n)-threshold scheme.

5 Quasigroup

The definition of groupoids appears on Page 8 [8] as follows.

Definition 8 (Binary Groupoid) A *binary groupoid* (G, A) is a non-empty set G together with a binary operation A.

The definition of quasigroup appears in Definition 1.21 in [8] as follows.

Definition 9 (Quasigroup) A binary groupoid $(Q, \circ)$ is called a *quasigroup* if for any ordered pair $(a, b) \in Q^2$ there exist unique solutions $x, y \in Q$ to the equations $x \circ a = b$ and $a \circ y = b$.

Many quasigroups over the same underlying set considered in this study can be constructed. Therefore, we denotes $*$ a quasigroup over Q such that $(Q, *)$ is a quasigroup.

In this work, we consider only quasigroups over finite underlying sets in this study. Hereafter, we denote by the word "quasigroup" denotes a quasigroup over a finite underlying set.

Notation 1 *For a quasigroup $*$ over Q, the solution x to $a * x = b$ is denoted as $(a *)^{-1}b$, and the solution x to $x * a = b$ is denoted as $b(* a)^{-1}$.*

Thus, $x * ((x *)^{-1}y) = y$ and $(y * (* x)^{-1}) * x = y$.

For a quasigroup $*$ over Q and $x \in Q$, the functions $y \mapsto x * y : Q \to Q$ and $y \mapsto y * x : Q \to Q$ are bijections, and the function $(x *)^{-1}$, or $(* x)^{-1}$, is the inverse of $y \mapsto x * y : Q \to Q$, or $y \mapsto y * x : Q \to Q$, respectively. Therefore, the followings hold: $(x *)^{-1}(x * y) = y$ and $(y * x)(* x)^{-1} = y$.

Orthogonality of quasigroups is defined according to the definition of orthogonality of groupoids given in Definition 1.329 in [8] as follows.

Definition 10 (Orthogonality) Binary groupoids (Q, A) and (Q, B) are called *orthogonal* if the system of equations

$$\begin{cases} A(x, y) = a \\ B(x, y) = b \end{cases}$$

has a unique solution (x_0, y_0) for any fixed pair of elements $a, b \in Q$.

Two quasigroups $*$ and $*'$ over Q are orthogonal when $(Q, *)$ and $(Q, *')$ are orthogonal as two binary groupoids.

Definition 11 (Mutual Orthogonality) A set of quasigroups $\{*_1, *_2, ..., *_N\}$ over Q is a *mutually orthogonal quasigroup system* when $*_i$ and $*_j$ are orthogonal for any i, j where $i \neq j$.

A mutually orthogonal quasigroup system as defined above is equivalent to the mutually orthogonal Latin squares (MOLS) described in [6].

Notation 2 *We denote by $N(q)$ the largest number N such that there exists a mutually orthogonal quasigroup system $\{*_1, *_2, ..., *_N\}$ over Q where $q = |Q|$.*

Here, $N(q)$ is defined for mutually orthogonal quasigroup system. $N(q)$ has been defined for mutually orthogonal Latin squares on Page 80 in [8] as follows.

> Denote by $N(q)$ the number of mutually (in pairs) orthogonal Latin squares of order q.

Both the definitions of $N(q)$ in Notation 2 and that in [8] are equivalent to each other.

A theorem on the magnitude of $N(q)$ is given as Theorem 1.335 in [8] as follows.

Theorem 3 – $N(q) \leq (q-1)$*;*
– *If q is prime, then $N(q) = (q-1)$;*
– $N(q_1 q_2) \geq min\{N(q_1), N(q_2)\}$*, in particular, if $q = q_1 \cdots q_t$ is the canonical decomposition of q, then $N(q) \geq min\{q_1 - 1, \cdots, q_t - 1\}$;*
– $N(q) \geq q^{10/143} - 2$*;*
– $N(q) \geq 3$*, if $q \notin \{2, 3, 6, 10\}$;*
– $N(q) \geq 6$ *whenever $q > 90$;*
– $N(q) \geq q^{10/148}$ *for sufficiently large q.*

6 Threshold Schemes by Quasigroups

In this section, we constructs two threshold schemes. That in Subsection 4.1 is a simple example of $(2, 2)$-threshold scheme by a quasigroup. It is a generalisation of Threshold scheme I in Subsection 4.1 by relaxing groups into quasigroups Subsection 4.2 gives a $(2, n)$-threshold scheme, which is the second main result of this study.

6.1 Simple Threshold Scheme by a Quasigroup

The (2,2)-threshold scheme by a group in Subsection 4.1 can be generalised into a (2,2)-threshold scheme by a quasigroup. In this subsection, we constructs a (2,2)-threshold scheme by a quasigroup $*$ as given below.

Definition 12 (Threshold Scheme III) Let $*$ be a quasigroup over Q. *Threshold Scheme III* is a scheme defined by the randomised algorithm:

$(Z_1, Z_2) = f_{\mathrm{III}}(X, Y) = (Y, X * Y)$

with input $X \in Q$, random oracle $Y \in Q$ and output $(Z_1, Z_2) \in Q^2$.

This Threshold Scheme III proceeds as follows.

Consider a dealer and two participants P_1 and P_2. All the data of the quasigroup $*$ over Q are public. There exists a secret $X \in Q$. The dealer chooses $Y \in Q$ such that the distribution of Y is uniform and Y is independent of X. The dealer gives $Z_1 = Y$ to the participant P_1 and $Z_2 = X * Y$ to the other participant P_2.

Then, the next theorem holds.

Theorem 4 *Threshold Scheme III is a (2,2)-threshold scheme providing perfect concealment.*

Proof. We prove the followings. (1) X is recovered from $Z_1 = Y$ and $Z_2 = X * Y$. (2) X is independent both of $Z_1 = Y$ and of $Z_2 = X * Y$.

(1) is simple because $X = Z_2(* Z_1)^{-1}$. (2) is shown as follows. First, X is independent of $Z_1 = Y$ by the assumption. Next, X is independent of Z_2 by the next proposition. ∎

Proposition 3 *Let $*$ be a quasigroup over Q, and X and Y be random variables over Q. Suppose that the distribution of Y is uniform, X and Y are independent, and $Z = X * Y$. Then, (1) the distribution of Z is uniform, and (2) X and Z are independent.*

Proof. The proof is similar to that of Proposition 1. The proof of this proposition is obtained by replacing $x^{-1}z$ in the proof of Proposition 1 with $(x *)^{-1}z$.

(1) For any $z \in Q$,

$\Pr[Z = z] = \Pr[X * Y = z] = \sum_{x \in Q} \Pr[X = x, x * Y = z] = \sum_{x \in Q} \Pr[X = x, Y = (x *)^{-1}z]$

$= \sum_{x \in Q} \Pr[X = x] \cdot \Pr[Y = (x *)^{-1}z] = \sum_{x \in Q} (\Pr[X = x]/|Q|)$

$= (\sum_{x \in Q} \Pr[X = x])/|Q| = 1/|Q|$.

(2) For any $x, z \in Q$,

$\Pr[X = x, Z = z] = \Pr[X = x, X * Y = z] = \Pr[X = x, Y = (x *)^{-1}z]$

$= \Pr[X = x] \cdot \Pr[Y = (x *)^{-1}z] = \Pr[X = x]/|Q|$.

By the discussion of (1), we have $\Pr[Z = z] = 1/|Q|$, therefore

$\Pr[X = x, Z = z] = \Pr[X = x] \cdot \Pr[Z = z]$. ∎

6.2 Threshold Scheme by a Mutually Orthogonal Quasigroup System

As the second main result of this study, this subsection constructs a $(2, n)$-threshold scheme by a quasigroup. By using $(*_1, *_2, ..., *_{n-1})$ a mutually orthogonal quasigroup system, the $(2, n)$-threshold system is constructed as follows.

Definition 13 (Threshold Scheme IV) Let $(*_1, *_2, ..., *_{n-1})$ be a mutually orthogonal quasigroup system over Q. *Threshold Scheme IV* is a scheme defined by the randomised algorithm:

$(Z_1, Z_2, ..., Z_n) = f_{\mathrm{IV}}(X, Y) = (X *_1 Y, X *_2 Y, ..., X *_{n-1} Y, Y)$

with input $X \in Q$, random oracle $Y \in Q$, and output $(Z_1, Z_2, ..., Z_n) \in Q^n$.

This Threshold Scheme IV proceeds as follows.

Consider There are a dealer and n participants $P_1, P_2, ..., P_n$. All the data of the orthogonal quasigroup system $(*_1, *_2, ..., *_{n-1})$ over Q are public. There is a secret $X \in Q$. The dealer chooses $Y \in Q$ such that the distribution of Y is uniform, and $Z_n = Y$ is independent of X. The dealer gives Y to the participant P_n and gives $Z_i = X *_i Y$ to the participant P_i for each $i = 1, 2, ..., n-1$.

Then, the next theorem holds.

Theorem 5 *Threshold Scheme IV is a (2,n)-threshold scheme providing perfect concealment.*

Proof. We prove the followings. (1) X is recovered from any two of $Z_1, Z_2, ..., Z_n$. (2) X is independent of each of $Z_1, Z_2, ..., Z_n$.

(1) is shown as follows. For $i \neq n$, X is recovered from $Z_i = X *_i Y$ and $Z_n = Y$ by calculating $X = Z_h(*_h Y)^{-1}$. For i and j where $h \neq h'$ and $h, h' \in \{1, 2, ..., n-1\}$, X is recovered from Z_i and Z_j by solving the equation system $\{X *_i Y = Z_i, X *_j Y = Z_j\}$.

(2) is shown as follows. First, X is independent of $Z_n = Y$ by the assumption. Next, X is independent of $Z_i = X *_i Y$ for $i \in \{1, 2, ..., n-1\}$ by Proposition 3. ∎

7 Related Works

Section 7.2 gives two related works which construct secret sharing schemes by Latin squares. As a preliminary, Subsection 7.1 explains the identification of Latin squares to subsets.

7.1 Latin Squares as Sets

A Latin square of order q is a $q \times q$ array such that each of its entries is an element of $\{1, 2, ..., q\}$ and the entries in each row and in each column are distinct. Let $\mathbb{Z}_q$ be $\{1, 2, ..., q\}$.

A Latin square L is identified as the set $L = \{(i, j; k_{ij}) | i, j \in \mathbb{Z}_q\} \subset \mathbb{Z}_q^3$ where k_{ij} is the entry of the i-th row and j-th column. Not all subsets $s \subset \mathbb{Z}_q^3$ are Latin squares. Some $s_1 \subset \mathbb{Z}_q^3$ is a Latin square, as the following example:

$$s_1 = \{(1,1;1), (1,2;2), (2,1;2), (2,2;1)\} = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}.$$

Some $s_2 \subset \mathbb{Z}_q^3$ is an array but not a Latin square, as in the following example.

$$s_2 = \{(1,1;1), (1,2;2), (2,1;1), (2,2;2)\} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}.$$

Some $s_3 \subset \mathbb{Z}_q^3$ is a subset of a Latin square, as in the following example.

$$s_3 = \{(1,1;1), (1,2;2)\} = \begin{bmatrix} 1 & 2 \\ . & . \end{bmatrix}.$$

Some $s_4 \subset \mathbb{Z}_q^3$ is a subset of an array but not a subset of a Latin square, as in the following example.

$s_4 = \{(1,1;1),(1,2;1)\} = \begin{bmatrix} 1 & 1 \\ . & . \end{bmatrix}$.

Some $s_5 \subset \mathbb{Z}_q^3$ is not a subset of an array, as in the following example.

$s_5 = \{(1,1;1),(1,1;2)\}$.

Let $\mathcal{L}(q)$ be the sets of all the Latin squares of order q. There exists a bijection $L(\,)$ of the quasigroups over $\mathbb{Z}_q$ into the Latin squares of order q such that, for a quasigroup $*$, the Latin square $L(*)$ is $L(*) = \{(i,j;i*j)|i,j \in \mathbb{Z}_q\}$.

7.2 Secret Sharing Schemes by Latin Squares

Several studies has considered secret sharing schemes using Latin squares [2, 11].

The secret sharing scheme in the literature [2] is constructed as follows.

A critical set s of a Lain square $L \in \mathcal{L}(q)$ is a subset of $L = \{(i,j;k_{ij})|i,j \in \mathbb{Z}_q\}$ such that, for each proper subset $s' \subsetneq s$, there exists another $L' \in \mathcal{L}(q)$ such that $s' \subset L' \neq L$. That is, a critical set determines a Latin square uniquely, but no proper subset of it does so.

In this secret sharing scheme, a secret is a Latin square L which ranges over $\mathcal{L}(q)$. The dealer delivers an element of the set L to each participant. A party C of the participants can recover the secret L if the set of all the elements delivered to the participants in C includes a critical set of L.

If a participant P receives a triple $(i,j;k) \in L$, then P alone knows that the secret data is not L' where $(i,j;k) \notin L'$. The probability that the secret is L' is zero after P received $(i,j;k)$, although the probability was positive before P received it. Because the posterior probability differs from the prior probability, this scheme does not provide perfect concealment.

The secret sharing scheme in the literature [11] is an application of Threshold Scheme II in Subsection 4.2. It is constructed as follows.

Let $\mathbb{S}_q$ be the symmetric group over $\mathbb{Z}_q$. An element $\theta = (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{S}_q^3$ acts on $(i,j;k) \in \mathbb{Z}_q^3$ as $\theta(i,j;k) = (\sigma_1 i, \sigma_2 j; \sigma_3 k)$, and acts on $s \subset \mathbb{Z}_q^3$ as $\theta s = \{(\sigma_1 i, \sigma_2 j; \sigma_3 k)|(i,j;k) \in s\}$. It is known that if $L \in \mathcal{L}(q)$ then $\theta L \in \mathcal{L}(q)$. If $\theta L = L$, then θ is called an autotopism of L.

For $\theta \in \mathbb{S}_q^3$, the notation $order(\theta)$ denotes the order of θ, that is, $order(\theta)$ is the minimum positive integer h such that θ^h is the identity element. The notation $\mathcal{P}(\mathbb{Z}_q^3)$ denotes the power set of $\mathbb{Z}_q^3$. The function g of $\mathcal{P}(\mathbb{Z}_q^3) \times \mathbb{S}_q^3$ into $\mathcal{P}(\mathbb{Z}_q^3)$ is defined as $g(s,\theta) = \bigcup_{h=0}^{order(\theta)-1} \theta^h s$. The subset $D \subset \mathcal{P}(\mathbb{Z}_q^3) \times \mathbb{S}_q^3$ is defined as $D = \{(s,\theta)|g(s,\theta) \in \mathcal{L}(q)\}$. Clearly, if $(s,\theta) \in D$, then θ is an autotopism of $g(s,\theta)$.

The secret sharing scheme in [11] proceeds as follows. The subset $s \subset \mathbb{Z}_q^3$ is public. The secret is $L \in \{g(s,\theta)|(s,\theta) \in D\}$. The dealer chooses $X \in \mathbb{S}_q^3$ such that $L = g(s,X)$. The dealer chooses elements $Y_1, Y_2, ..., Y_{n-1} \in \mathbb{S}_q^3$ such that each distribution of Y_i is uniform, and the variables $X, Y_1, Y_2, ..., Y_{n-2}$ and Y_{n-1} are independent. The dealer gives Y_i to a participant P_i for $i = 1, 2, ..., n-1$ and gives $Z = Y_{n-1}^{-1} Y_{n-2}^{-1} ... Y_1^{-1} X$ to the participant P_n. From the discussion in Proposition 2, the random variables $X, Y_1, Y_2, ..., Y_{i-1}, Y_{i+1}, ..., Y_{n-1}$ and Z are also independent. Because X determines L, the random variables

$L, Y_1, Y_2, ..., Y_{i-1}, Y_{i+1}, ..., Y_{n-1}$ and Z are also independent. None of $n-1$ participants can solve the value of L, because L is independent both of $(Y_1, Y_2, ..., Y_{n-1})$, and of $(Y_1, Y_2, ..., Y_{i-1}, Y_{i+1}, ..., Y_{n-1}, Z)$ for $i = 1, 2, ..., n-1$. In contrast, all of $P_1, P_2, ..., P_n$ in collaboration can recover the value of L as $L = g(s, X) = g(s, Y_1Y_2...Y_{n-1}Z)$. Therefore, this is an (n, n)-threshold secret sharing scheme with perfect concealment, which is not asserted explicitly in [11].

The security of this scheme essentially depends on the security of the scheme in Subsection 4.2. Although the range of X in the scheme in Subsection 4.2 is G, that of X in this scheme is $\{X \in \mathbb{S}_q^3 | (s, X) \in D\}$. This fact enables a type of error detection.

References

[1] Blakley, G.R.: Safeguarding cryptographic keys. In: International Workshop on Managing Requirements Knowledge, pp. 313–318 (1979)

[2] Cooper, J., Donovan, D., Seberry, J.: Secret sharing schemes arising from Latin squares. Bulletin of the Institute of Combinatorics and its Applications **12**, 33–43 (1994)

[3] Goldreich, O.: Foundations of Cryptography, Vol. I. Cambridge University Press (2008)

[4] Halpern, J.Y., O'Neill, K.R.: Secrecy in multiagent systems. ACM Trans. Inf. Syst. Secur. **12**(5), 1–47 (2003)

[5] Keedwell, A.D., Dénes, J.: Latin Squares and their Applications, 2nd edition. North-Holland (2015)

[6] Laywine, C.F., Mullen, G.L.: Dscrete Mathematics Using Latin Squares. John Weiley & Sons, INC. (1998)

[7] Shamir, A.: How to share a secret. Communication of the ACM **22**(11), 612–613 (1979)

[8] Shcherbacov, V.: Elements of Quasigroup Theory and Applications. Chapman and Hall/CRC (2017)

[9] Stinson, D.R.: An explication of secret sharing schemes. Designs, Codes and Cryptography **2**, 357–390 (1992)

[10] Stinson, D.R.: Cryptography: Theory and Practice, Third Edition. Chapman and Hall/CRC (2005)

[11] Stones, R.J., Su, M., Liu, X., Wang, G., Lin, S.: A Latin square autotopism secret sharing scheme. Designes, Codes and Cryptography **80**(3), 635–650 (2016)

[12] Takeuti, I.: Bayesian concealment. In: T. Adachi (ed.) Algebraic System, Logic, Language and Related Areas in Computer Science II, *RIMS Kôkyûroku*, vol. 2188, pp. 159–162. Kyoto University (2021)

[13] Takeuti, I.: Formalisation of bayesian concealment. Japan Journal of Industrial and Applied Mathematics **38**, 677—692 (2021)

[14] Takeuti, I., Adachi, T.: Formalisation of probabilistic concealment. Japan Journal of Industrial and Applied Mathematics **36**(2), 473–495 (2019)

[15] Takeuti, I., Mano, K.: A proof of secrecyby probabilistic modal logic. Bulletin of the Japan Society for Industrial and Applied Mathematics **22**(1), 23–45 (2012). In Japanese