Computer Security Symposium 2017
23 - 25 October 2017

Practical Encoding Matrices for Secret Sharing Schemes over $\mathbb{Z}/2^m\mathbb{Z}$

Hidenori Kuwakado[1,a)]

Abstract: Cloud services using secret sharing schemes have been launched recently. Since secret sharing schemes have been usually achieved over a finite field, the throughput for sharing and reconstructing a secret depends on the implementation of operations over the finite field. However, almost all CPUs do not support operations over the finite field as primary instructions. We study k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$. The advantage of the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ is that all CPUs support modulo-2^m arithmetic operations as primary instructions. We show conditions for general encoding matrices and simplified conditions for the special type of encoding matrices. Conditions suggests that any k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ are non-ideal. A Vandermonde-based encoding matrix satisfies simplified conditions and the maximum size of a secret is explicitly given.

Keywords: secret sharing scheme, operations over $\mathbb{Z}/2^m\mathbb{Z}$, modular arithmetic operations, Vandermonde matrix

1. Introduction

Secret sharing schemes are a promising approach to achieve both of confidentiality and availability of data. Accordingly cloud services using secret sharing schemes have been launched recently [2], [5].

Since secret sharing schemes have been achieved over a finite field, the throughput of secret sharing schemes mainly depends on that of operations on the finite field. Hence, many papers have proposed efficient implementations of operations on the finite field such as use of only the XOR operation and use of a binary extension field (e.g., [1], [2], [3], [4]).

In contrast, we focus on the implementation over $\mathbb{Z}/2^m\mathbb{Z}$. The advantage of implementation over $\mathbb{Z}/2^m\mathbb{Z}$ is that all CPUs support modulo-2^m ($m = 8, 16, 32, 64$) arithmetic operations as primary instructions. Furthermore, the throughput of modulo-2^m arithmetic operations of typical CPUs is equal to that of bitwise operations such as XOR. Hence, there is no reason to use only the XOR operation.

The reason why secret sharing schemes over $\mathbb{Z}/2^m\mathbb{Z}$ get less attention is probably not to work well. That is, the reconstruction of a secret may fail, or some information about a secret may leak. However, this article shows that k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ can be achieved securely if the size of a share is allowed to be larger than that of a secret.

In terms of the size of a share, secret sharing schemes are also classified into two classes: *ideal* secret sharing schemes and *non-ideal* secret sharing schemes. If the size of a share is equal to that of the secret, then it is called to be ideal. Otherwise (larger than the size of a secret), it is called to be non-ideal. Shamir's secret sharing scheme is ideal. Non-ideal secret sharing schemes are often discussed for complicated access structures. In other words that described above, this article shows that any k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ are non-ideal.

This article is organized as follows: Section 2 describes four examples of secret sharing schemes over $\mathbb{Z}/2^m\mathbb{Z}$. Section 3 first describes notations, and then shows conditions of encoding matrices for achieving k-out-of-n secret sharing schemes. From conditions, we will see that any k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ are non-ideal. Conditions in Sect. 3 is general, but it seems difficult to check if a given encoding matrix satisfies them or not. Section 4 shows the set of encoding matrices such that conditions can be checked easily. The set of encoding matrices includes the Vandermonde matrix in which all the elements are a power of 2. Section 5 concludes this article.

2. Examples

2.1 2-out-3 Scheme over $\mathbb{Z}/2^8\mathbb{Z}$

This section describes two 2-out-of-3 schemes over $\mathbb{Z}/2^8\mathbb{Z}$. Let s be a secret that is encoded in $z_2 \in \mathbb{Z}/2^8\mathbb{Z}$ in some manner. After z_1 is chosen according to the uniform distribution on $\mathbb{Z}/2^8\mathbb{Z}$, three shares w_1, w_2, w_3 are produced by

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = E \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad \text{over} \quad \mathbb{Z}/2^8\mathbb{Z} \tag{1}$$

[1] Faculty of Informatics, Kansai University
[a)] kuwakado@kansai-u.ac.jp

where E is a public 3×2 matrix.

Equation (1) can be considered as the generalization of Shamir's 2-out-of-3 scheme. In the case of Shamir's 2-out-of-3 scheme, z_2 is s itself and E is given by

$$E = \begin{pmatrix} x_1 & 1 \\ x_2 & 1 \\ x_3 & 1 \end{pmatrix} \tag{2}$$

where each x_i, which is sometimes called a user ID, is a public non-zero element in a finite field. Equation (1) is computed over the finite field.

Unlike Shamir's scheme, our scheme does not restrict E to the form of Eq. (2) and computes Eq. (1) over $\mathbb{Z}/2^8\mathbb{Z}$. Two 2-out-of-3 schemes over $\mathbb{Z}/2^8\mathbb{Z}$ are demonstrated below.

Scheme 1 Suppose that a 7-bit secret s is encoded as

$$z_2 = s \parallel \mathtt{0} \tag{3}$$

where $\mathtt{0}$ denotes the zero bit and E is

$$E = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Three shares w_1, w_2, w_3 are produced by Eq. (1). Although w_3 gives the least significant bit of z_2, no information about the secret is known because of Eq. (3). This is the reason for requiring the zero bit.

Suppose that two shares w_{r_1}, w_{r_2} are given where $1 \leq r_1 < r_2 \leq 3$. Let $E^{(r_1,r_2)}$ be a matrix that consists of the r_1th row and the r_2th row of E. It is easy to conform that there exists D_{r_1,r_2} such that

$$D_{r_1,r_2} \cdot E^{(r_1,r_2)} = I \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z} \tag{4}$$

where I is the 2×2 identity matrix. For example, when $(r_1, r_2) = (1, 3)$, $E^{(1,3)}$ and $D_{1,3}$ are

$$E^{(1,3)} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \quad D_{1,3} = \begin{pmatrix} 1 & 255 \\ 254 & 1 \end{pmatrix}.$$

From two shares w_{r_1}, w_{r_2} and D_{r_1,r_2}, z_2 can be obtained by

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = D_{r_1,r_2} \begin{pmatrix} w_{r_1} \\ w_{r_2} \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z}. \tag{5}$$

Removing the least significant bit of z_2 gives the secret s.

Scheme 2 Suppose that a 7-bit secret s is encoded as

$$z_2 = \mathtt{0} \parallel s \tag{6}$$

and E is

$$E = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 4 \end{pmatrix}.$$

Three shares w_1, w_2, w_3 are produced by Eq. (1). Unlike Scheme 1, no information about z_2 is obtained from each share because of the addition of z_1, which is chosen according to the uniform distribution on $\mathbb{Z}/2^8\mathbb{Z}$.

Suppose that two shares w_{r_1}, w_{r_2} are given where $1 \leq r_1 < r_2 \leq 3$. For any $1 \leq r_1 < r_2 \leq 3$, there exists D_{r_1,r_2} such that

$$D_{r_1,r_2} \cdot E^{(r_1,r_2)} = 2^{f_{r_1,r_2}} I \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z}.$$

Specifically, D_{r_1,r_2} and f_{r_1,r_2} are given as follows:

$$\begin{aligned} D_{1,2} &= \begin{pmatrix} 2 & 255 \\ 255 & 1 \end{pmatrix}, \ f_{1,2} = 0, \\ D_{1,3} &= \begin{pmatrix} 172 & 85 \\ 85 & 172 \end{pmatrix}, \ f_{1,3} = 0, \\ D_{2,3} &= \begin{pmatrix} 4 & 254 \\ 255 & 1 \end{pmatrix}, \ f_{2,3} = 1. \end{aligned} \tag{7}$$

When $(r_1, r_2) = (1, 2)$ and $(1, 3)$, z_2 can be completely recovered by the multiplication of D_{r_1,r_2} like Eq. (5). However, when $(r_1, r_2) = (2, 3)$, z_2 is not completely recovered because

$$\begin{aligned} D_{2,3} \begin{pmatrix} w_2 \\ w_3 \end{pmatrix} &= D_{2,3} E^{(2,3)} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z} \\ &= 2 \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z} \ (\because \text{Eq. (7)}). \end{aligned} \tag{8}$$

Equation (8) means that the most significant bit of z_2 disappears due to the multiplication of 2. However, the secret s can be completely obtained because of Eq. (6). This is the reason for requiring the zero bit.

We observe that two schemes above are comparable in the size of the secret and the number of modular operations for sharing and reconstructing the secret.

2.2 2-out-4 Scheme over $\mathbb{Z}/2^8\mathbb{Z}$

This section describes two 2-out-of-4 schemes over $\mathbb{Z}/2^8\mathbb{Z}$. Let s be a secret that is encoded in $z_2 \in \mathbb{Z}/2^8\mathbb{Z}$ in some manner. After z_1 is chosen according to the uniform distribution on $\mathbb{Z}/2^8\mathbb{Z}$, four shares w_1, w_2, w_3, w_4 are produced by

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = E \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z} \tag{9}$$

where E is a public 4×2 matrix.

Scheme 3 Suppose that a 7-bit secret s is encoded as

$$z_2 = \mathtt{0} \parallel s \tag{10}$$

and E is

$$E = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 3 \\ 1 & 2 \end{pmatrix}.$$

Four shares are produced by Eq. (9). No information about z_2 is obtained from each share because of the addition of z_1.

Suppose that two shares w_{r_1}, w_{r_2} are given where $1 \leq r_1 < r_2 \leq 4$. For any $1 \leq r_1 < r_2 \leq 4$, there exists D_{r_1,r_2} such that

$$D_{r_1,r_2} \cdot E^{(r_1,r_2)} = 2^{f_{r_1,r_2}} I \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z}. \tag{11}$$

For example,

$$D_{1,4} = \begin{pmatrix} 2 & 0 \\ 255 & 1 \end{pmatrix}, \ f_{1,4} = 1, \tag{12}$$
$$D_{3,4} = \begin{pmatrix} 254 & 3 \\ 1 & 255 \end{pmatrix}, \ f_{3,4} = 0.$$

Thus, f_{r_1,r_2} is not always equal to zero. In fact, the maximum value of f_{r_1,r_2} is

$$\max_{1 \leq r_1 < r_2 \leq 4} (f_{r_1,r_2}) = 1. \tag{13}$$

When $(r_1, r_2) = (1, 4)$, z_2 is not completely recovered because

$$D_{1,4} \begin{pmatrix} w_1 \\ w_4 \end{pmatrix} = D_{1,4} E^{(1,4)} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z}$$
$$= 2 \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z} \ (\because \text{Eq. (11), Eq. (12)}). \tag{14}$$

Equation (14) means that the most significant bit of z_2 disappears because of the multiplication of 2. However, the secret s can be completely obtained because of Eq. (10). Equation (13) suggests that the zero bit is required to reconstruct the secret completely.

Scheme 4 Suppose that a 6-bit secret s is encoded as

$$z_2 = \mathsf{0}^2 \parallel s \tag{15}$$

where $\mathsf{0}^2$ denotes two zero bits and E is

$$E = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 4 \\ 1 & 8 \end{pmatrix}.$$

Four shares are produced by Eq. (9). No information about z_2 is obtained from each share because of the addition of z_1.

Suppose that two shares w_{r_1}, w_{r_2} are given where $1 \leq r_1 < r_2 \leq 4$. For any $1 \leq r_1 < r_2 \leq 4$, there exists D_{r_1,r_2} such that

$$D_{r_1,r_2} \cdot E^{(r_1,r_2)} = 2^{f_{r_1,r_2}} I \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z}. \tag{16}$$

For example,

$$D_{2,4} = \begin{pmatrix} 88 & 170 \\ 85 & 171 \end{pmatrix}, \ f_{2,4} = 1,$$
$$D_{3,4} = \begin{pmatrix} 8 & 252 \\ 255 & 1 \end{pmatrix}, \ f_{3,4} = 2. \tag{17}$$

Thus, f_{r_1,r_2} is not always equal to zero. In fact, the maximum value of f_{r_1,r_2} is

$$\max_{1 \leq r_1 < r_2 \leq 4} (f_{r_1,r_2}) = 2. \tag{18}$$

When $(r_1, r_2) = (3, 4)$, z_2 is not completely recovered because

$$D_{3,4} \begin{pmatrix} w_3 \\ w_4 \end{pmatrix} = D_{3,4} E^{(3,4)} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z}$$
$$= 2^2 \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \ \text{ over } \ \mathbb{Z}/2^8\mathbb{Z} \ (\because \text{Eq. (16), Eq. (17)}). \tag{19}$$

Equation (19) means that the two most significant bits of z_2 disappear owing to the multiplication of 2^2. However, the secret s can be completely obtained because of Eq. (15). Equation (18) suggests that the two zero bits are required to reconstruct the secret completely.

Comparing Scheme 3 with Scheme 4, we observe that Scheme 3 is better in the sense that the secret size is larger and the number of modular operations for sharing and reconstructing the secret is less.

3. k-out-of-n Scheme over $\mathbb{Z}/2^m\mathbb{Z}$

3.1 Notations

Since almost all computations that appear in the following sections are performed over $\mathbb{Z}/2^m\mathbb{Z}$, we often omit "over $\mathbb{Z}/2^m\mathbb{Z}$". Let $\mathrm{lgd}\,(x)$ be the logarithm of divisor 2 of x. For example, $\mathrm{lgd}\,(40) = \mathrm{lgd}\left(2^3 \times 5\right) = 3$ and $\mathrm{lgd}\,(-28) = \mathrm{lgd}\left(-2^2 \times 7\right) = 2$. When 0 is regarded as an element in $\mathbb{Z}/2^m\mathbb{Z}$, $\mathrm{lgd}\,(0)$ is defined to be m (i.e., $\mathrm{lgd}\,(0) = m$). If $\mathrm{lgd}\,(x) = 0$, then x is odd. A series of variables such as $r_1, r_2, \ldots, r_\iota$ is sometimes abbreviated to $r_{[\iota]}$. For example, $E^{(r_1,r_2,\ldots,r_k)}$ is abbreviated to $E^{(r_{[k]})}$ and $f_{r_1,r_2,\ldots,r_{k-1}}$ is abbreviated to $f_{r_{[k-1]}}$.

Let E be an $n \times k$ matrix in which all the elements are in $\mathbb{Z}/2^m\mathbb{Z}$.

$$E = \begin{pmatrix} e_{1,1} & e_{1,2} & \ldots & e_{1,k} \\ e_{2,1} & e_{2,2} & \ldots & e_{2,k} \\ \vdots & & & \\ e_{n,1} & e_{n,2} & \ldots & e_{n,k} \end{pmatrix} \tag{20}$$

Consider the case that $n = k$, that is, E is a $k \times k$ square matrix. A determinant of E, denoted by $\det(E)$, is defined in a usual way that

$$\det(E) = \sum_{\sigma \in \Phi_k} \left(\mathrm{sgn}\,(\sigma) \prod_{r=1}^{k} e_{r,\sigma(r)} \right)$$

where Φ_k is the set of all the permutations on $\{1, 2, \ldots, k\}$ and $\mathrm{sgn}\,(\sigma)$ denotes the signature of the permutation σ, which is 1 or -1. Let f be

$$f = \mathrm{lgd}\,(\det(E)). \tag{21}$$

We say that E is *invertible* over $\mathbb{Z}/2^m\mathbb{Z}$ if there exists a $k \times k$ matrix D such that

$$D \cdot E = E \cdot D = 2^f I \tag{22}$$

where $0 \leq f \leq m-1$ and I denotes the $k \times k$ identity matrix. In other articles, if E is invertible, then f is equal to 0 (i.e., $2^f = 1$). In this article, even if E is invertible, f may not be equal to 0.

Let $E^{(r_1,r_2,\ldots,r_\kappa)}$ (abbrev. $E^{(r_{[\kappa]})}$) be a $\kappa \times k$ submatrix that consists of the r_1th row, the r_2th row, ..., and the r_κth row of E.

$$E^{(r_1,r_2,\ldots,r_\kappa)} = E^{(r_{[\kappa]})} = \begin{pmatrix} e_{r_1,1} & e_{r_1,2} & \ldots & e_{r_1,k} \\ e_{r_2,1} & e_{r_2,2} & \ldots & e_{r_2,k} \\ \vdots & & & \\ e_{r_\kappa,1} & e_{r_\kappa,2} & \ldots & e_{r_\kappa,k} \end{pmatrix}$$

This submatrix is called a *κ-row submatrix of E*.

3.2 Scheme

Let S be a random variable corresponding to a secret s and W_{r_ι} be a random variable corresponding to a share w_{r_ι}. Let H be Shannon's entropy. If a scheme satisfies the following two conditions, then it is called a *k-out-of-n secret sharing scheme*.

(1) *Reconstructability* For any k random variables W_{r_ι} $(\iota = 1, 2, \ldots, k)$,

$$H(S|W_{r_1}, W_{r_2}, \ldots, W_{r_k}) = 0. \tag{23}$$

Equation (23) means that the secret can be uniquely determined from any k shares. Furthermore, there exists an efficient algorithm for finding the secret from any k shares.

(2) *Confidentiality* For any $k-1$ random variables W_{r_ι} $(\iota = 1, 2, \ldots, k-1)$,

$$H(S|W_{r_1}, W_{r_2}, \ldots, W_{r_{k-1}}) = H(S). \tag{24}$$

Equation (24) means that no information about the secret can be obtained even if unlimited computational power is available.

This article investigates k-out-of-n secret sharing schemes over $\mathbb{Z}/2^m\mathbb{Z}$ where $2 \leq k < n$[*1]. Let s be a secret and z_k be an element in $\mathbb{Z}/2^m\mathbb{Z}$ such that

$$z_k = \mathtt{0}^{c_h} \parallel s \parallel \mathtt{0}^{c_t} \tag{25}$$

where $0 \leq c_h < m$ and $0 \leq c_t < m$. After $k-1$ elements z_ι $(\iota = 1, 2, \ldots, k-1)$ are independently chosen according to the uniform distribution on $\mathbb{Z}/2^m\mathbb{Z}$, n shares w_r $(r = 1, 2, \ldots, n)$ are produced as follows:

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = E \cdot \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} \tag{26}$$

where an $n \times k$ matrix E is called an *encoding matrix*. Although E is public, each z_r $(r = 1, 2, \ldots, k)$ is kept secret.

[*1] When $n = k$, XOR-based secret sharing schemes are the best in terms of the size of a share and the number of operations for sharing and reconstructing the secret. Hence, the case of $n = k$ is excluded.

The complexity of Eq. (26) with respect to additions and multiplications over $\mathbb{Z}/2^m\mathbb{Z}$ is $\mathrm{O}(nk)$.

Suppose that any k shares $w_{r_1}, w_{r_2}, \ldots, w_{r_k}$ are given. The secret s that is contained in z_k must be reconstructed from the following system of equations on $\mathbb{Z}/2^m\mathbb{Z}$.

$$\begin{pmatrix} w_{r_1} \\ w_{r_2} \\ \vdots \\ w_{r_k} \end{pmatrix} = E^{(r_{[k]})} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix}. \tag{27}$$

It is unnecessary to find $z_1, z_2, \ldots, z_{k-1}$ and to find a total extent of z_k because the secret is a part of z_k as shown in Eq. (25).

3.3 Conditions for Encoding Matrices

This section describes conditions of the encoding matrix E for the reconstructability and the confidentiality. We will see that $\mathtt{0}^{c_h}$ and $\mathtt{0}^{c_t}$ in Eq. (25) are required for the reconstructability and the confidentiality, respectively and at least one of c_h and c_t is larger than zero.

3.3.1 Reconstructability of the Secret

We here show the necessary and sufficient condition for the reconstructability of the secret. Consider the linear summation of k shares w_{r_i} $(i = 1, 2, \ldots, k)$ as $\sum_{i=1}^{k} v_i w_{r_i}$ where v_i is an element in $\mathbb{Z}/2^m\mathbb{Z}$. From Eq. (27), the linear summation is written as

$$\sum_{i=1}^{k} v_i w_{r_i} = \left(\sum_{i=1}^{k} v_i e_{r_i,1}, \ldots, \sum_{i=1}^{k} v_i e_{r_i,k} \right) \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix} \tag{28}$$

$$= \left(2^{f_1} g_1, \ldots, 2^{f_k} g_k \right) \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix} \tag{29}$$

where f_j and g_j are defined as

$$f_j = \mathrm{lgd}\left(\sum_{i=1}^{k} v_i e_{r_i,j} \right), \quad \sum_{i=1}^{k} v_i e_{r_i,j} = 2^{f_j} g_j. \tag{30}$$

The function lgd () was defined in Sect. 3.1. As described below, the value of f_j plays an important role in reconstructing the secret. Let f_τ be

$$f_\tau = \min(f_1, f_2, \ldots, f_{k-1}).$$

Then, Eq. (29) is written as

$$\sum_{i=1}^{k} v_i w_{r_i} = 2^{f_k} g_k z_k + 2^{f_\tau} g_\tau z_\tau + \sum_{j=1, j\neq\tau}^{k-1} 2^{f_j} g_j z_j. \tag{31}$$

We focus on the right-hand side of Eq. (31), which is illustrated in Fig. 1[*2]. For $i = 1, 2, \ldots, k-1$, each $g_i z_i$ is uniformly and independently distributed on $\mathbb{Z}/2^m\mathbb{Z}$ because each z_i is independently chosen according to the uniform distribution on $\mathbb{Z}/2^m\mathbb{Z}$. Furthermore, we make the following

[*2] In Fig. 1, each g_i is ignored.

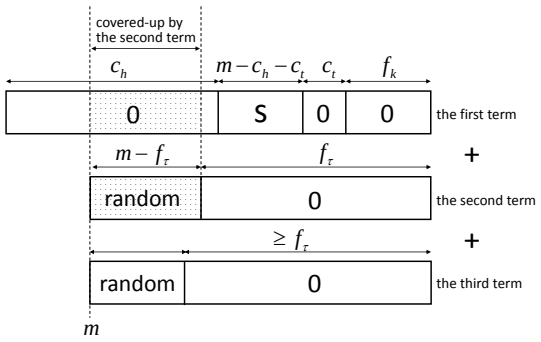

Fig. 1 The right-hand side of Eq. (31).

observations on the right-hand side of Eq. (31).

- Owing to the multiplication of 2^{f_k}, the number of zero bits in the least significant bits of the first term is at least f_k.
  Since the $(m - c_h - c_t)$-bit secret is located in z_k as shown in Eq. (25), the bits related to the secret appear from the $(f_k + c_t)$th bit of the first term. Since g_k is odd, the secret can be reconstructed from the related bits. Hence, the inequality below is required to reconstruct the secret completely.
  $$(m - c_h - c_t) + (f_k + c_t) \leq m,$$
  which is simplified into
  $$f_k \leq c_h. \tag{32}$$
- Owing to the multiplication of 2^{f_τ}, the number of zero bits in the least significant bits of the second term is at least f_τ. Since the other $m - f_\tau$ bits may be uniformly distributed on $\{0,1\}^{m-f_\tau}$, they may cover up the secret. Hence, the inequality below is required to reconstruct the secret completely.
  $$(m - c_h - c_t) + (f_k + c_t) \leq f_\tau,$$
  which is simplified into
  $$m + f_k - f_\tau \leq c_h. \tag{33}$$
- The number of zero bits in the least significant bits of the third term is not smaller than that of the second term. Hence, the third term has no effect on the reconstruction of the secret.

In fact, Eq. (32) is unnecessary because if Eq. (33) holds, then Eq. (32) holds. This is shown by the contrapositive. Suppose that Eq. (32) does not hold, that is, $f_k > c_h$. Since $m > f_\tau$, adding them yields $m + f_k > f_\tau + c_h$, which means that Eq. (33) does not hold. Hence, only Eq. (33) is required for reconstructing the secret completely.

The analysis above assumes that both of both of $w_{r_1}, \ldots, w_{r_k}$ (abbrev. $w_{r_{[k]}}$) and $v_1, \ldots, v_k$ (abbrev. $v_{[k]}$) are fixed. For $j = 1, 2, \ldots, k-1$, each f_j in Eq. (30) depends on them. In order to make the size of the secret large, it is desirable that c_h is small. Since the secret must be reconstructed from any k shares, Eq. (33) is modified into

$$m + \max_{w_{r_{[k]}}, v_{[k]}} (f_k - f_\tau) \leq c_h.$$

Since c_h is implicitly required to be less than m because of Eq. (25), f_k is required to be less than f_τ. When m is fixed, the maximization in the inequality above is possible in principle because the number of allowable $w_{r_{[k]}}$ and that of allowable $v_{[k]}$ are finite.

Lemma 1 Let E be the $n \times k$ encoding matrix and w_{r_i} ($r_i \in \{1, 2, \ldots, n\}$) be the share as shown in Eq. (26). Consider the reconstruction of the secret using the linear summation of k shares such as $\sum_{i=1}^{k} v_i w_{r_i}$ where each $v_i \in \mathbb{Z}/2^m\mathbb{Z}$. The secret can be completely reconstructed from any k shares by the linear summation if and only if the inequality below holds.

$$m + \max_{w_{r_{[k]}}, v_{[k]}} (f_k - f_\tau) \leq c_h. \tag{34}$$

where

$$f_j = \mathrm{lgd}\left(\sum_{i=1}^{k-1} v_i e_{r_i,j}\right) \quad \text{for } j = 1, 2, \ldots, k,$$
$$f_\tau = \min(f_1, f_2, \ldots, f_{k-1}).$$

3.3.2 Confidentiality of the Secret

We here show the necessary and sufficient condition for the confidentiality of the secret. Consider an attack using the linear summation of $k-1$ shares w_{r_i} as $\sum_{i=1}^{k-1} u_i w_{r_i}$ where each u_i is an element in $\mathbb{Z}/2^m\mathbb{Z}$. The attack is characterized by $w_{r_1,\ldots,r_{k-1}}$ (abbrev. $w_{r_{[k-1]}}$) and $u_1, \ldots, u_{k-1}$ (abbrev. $u_{[k-1]}$).

Suppose that $w_{r_{[k-1]}}$ and $u_{[k-1]}$ are fixed. The linear summation is written as

$$\sum_{i=1}^{k-1} u_i w_{r_i} = \left(\sum_{i=1}^{k-1} u_i e_{r_i,1}, \ldots, \sum_{i=1}^{k-1} u_i e_{r_i,k},\right) \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix} \tag{35}$$

$$= \left(2^{f_1} g_1, \ldots, 2^{f_k} g_k\right) \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix} \tag{36}$$

where f_j and g_j are defined as

$$f_j = \mathrm{lgd}\left(\sum_{i=1}^{k-1} u_i e_{r_i,j}\right), \quad \sum_{i=1}^{k-1} u_i e_{r_i,k} = 2^{f_j} g_j. \tag{37}$$

Let f_ι be

$$f_\iota = \min(f_1, f_2, \ldots, f_{k-1}). \tag{38}$$

Then, Eq. (36) is transformed into

$$\sum_{i=1}^{k-1} u_i w_{r_i} = \sum_{j=1}^{k} 2^{f_j} g_j z_j$$
$$= 2^{f_k} g_k z_k + 2^{f_\iota} g_\iota z_\iota + 2^{f_\iota}\left(\sum_{j=1, j\neq\iota}^{k-1} 2^{f_j - f_\iota} g_j z_j\right) \tag{39}$$

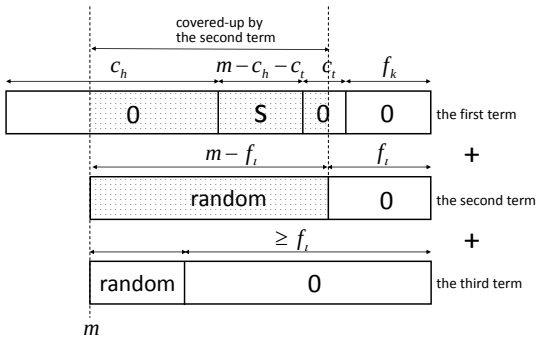

Fig. 2 The right-hand side of Eq. (39).

We focus on the right-hand side of Eq. (39), which is illustrated in Fig. 2[*3] We make three observations below.

(1) Owing to the multiplication of 2^{f_k}, the number of zero bits in the least significant bits of the first term is at least f_k.
Since the secret is located in z_k as shown in Eq. (25), the bits related to the secret appear from the (f_k+c_t)th bit of the first term. Since g_k is odd, the secret can be reconstructed from the related bits.

(2) Owing to the multiplication of 2^{f_ι}, the number of zero bits in the least significant bits of the second term is at least f_ι.
Since g_ι is odd and z_ι is chosen according to the uniform distribution on $\mathbb{Z}/2^m\mathbb{Z}$, the $(m-f_\iota)$ most significant bits of the second term are uniformly distributed on $\{0,1\}^{m-f_\iota}$. Hence, the $(m-f_\iota)$ most significant bits of the second term completely cover up that of the first term.

(3) Owing to the multiplication of 2^{f_ι}, the number of zero bits in the least significant bits of the second term is at least f_ι.
For $i=1,2,\ldots,k-1$, each z_i is independently chosen. The number of bits such that the third term covers up the first term is not larger than that of the second term. Accordingly, the third term does not contribute to cover-up of the first term.

We summarize three observations above as follows: if the inequality below holds,

$$f_k + c_t \geq f_\iota \tag{40}$$

then the second term can completely cover up the secret, that is, no information about the secret is obtained by the attack of Eq. (39).

The analysis above assumes that both of $w_{r_{[k-1]}}$ and $u_{[k-1]}$ are fixed. For $j=1,2,\ldots,k-1$, each f_j in Eq. (37) depends on both of $w_{r_{[k-1]}}$ and $u_{[k-1]}$. And now, it is desirable that c_t is small for increasing the size of the secret. Hence, $f_\iota - f_k$ is maximized with respect to $w_{r_{[k-1]}}$ and $u_{[k-1]}$. Equation (40) is modified into

$$c_t \geq \max_{w_{r_{[k-1]}},u_{[k-1]}} (f_\iota - f_k)\,.$$

When m is fixed, the maximization in the inequality above is possible in principle because the number of allowable $w_{r_{[k-1]}}$ and that of allowable $u_{[k-1]}$ are finite.

Lemma 2 Let E be the $n\times k$ encoding matrix and w_{r_i} $(r_i\in\{1,2,\ldots,n\})$ be a share as shown in Eq. (26). Consider an attack using the linear summation of $k-1$ shares such as $\sum_{i=1}^{k-1} u_i w_{r_i}$ where each $u_i\in\mathbb{Z}/2^m\mathbb{Z}$. No information about the secret is obtained by the linear summation if and only if the inequality below holds.

$$c_t \geq \max_{w_{r_{[k-1]}},u_{[k-1]}} (f_\iota - f_k)\,. \tag{41}$$

where

$$f_j = \mathrm{lgd}\left(\sum_{i=1}^{k-1} u_i e_{r_i,j}\right) \quad \text{for } j=1,2,\ldots,k,$$
$$f_\iota = \min(f_1,f_2,\ldots,f_{k-1}).$$

4. Practical Encoding Matrices

Section 3.3 described conditions to be satisfied by encoding matrices. However, given a large-size encoding matrix, it seems infeasible to check if it satisfies conditions or not. After describing the set of matrices such that it is easy to check if conditions are satisfied or not, this section shows that the special form of the Vandermonde matrix is included in the set of matrices.

4.1 Easily-Checkable Matrices

Let us consider an $n\times k$ encoding matrix E over $\mathbb{Z}/2^m\mathbb{Z}$ that satisfies two conditions below.

(I) Any k-row submatrix $E^{(r_{[k]})}$ of E is invertible. That is, for any $E^{(r_{[k]})}$, there exists a $k\times k$ matrix $D_{r_{[k]}}$ such that

$$E^{(r_{[k]})}\cdot D_{r_{[k]}} = D_{r_{[k]}}\cdot E^{(r_{[k]})} = 2^{f_{r_{[k]}}} I \tag{42}$$

where $f_{r_{[k]}}$ is given by

$$f_{r_{[k]}} = \mathrm{lgd}\left(\det\left(E^{(r_{[k]})}\right)\right) \tag{43}$$

and I denotes the $k\times k$ identify matrix.

(II) There exists an column in E such that all the elements are odd. That is, there exists c such that

$$\mathrm{lgd}\,(e_{r,c}) = 0 \quad \text{for} \quad 1\leq \forall r\leq n$$

where $e_{r,c}$ denotes the (r,c)th element of E.

The goal of Sect. 4.1.1 and Sect. 4.1.2 is to prove the following lemma.

Lemma 3 Suppose that the encoding matrix E satisfies the above-mentioned conditions (I)(II). For k shares $w_{r_1}, w_{r_2},\ldots,w_{r_k}$ (abbrev. $w_{r_{[k]}}$), if the following inequality holds,

$$\max_{w_{r_{[k]}}} \left(f_{r_{[k]}}\right) \leq c_h$$

then the reconstructability of the secret can be achieved. The confidentiality of the secret is also achieved.

[*3] In Fig. 2, each g_j is ignored.

4.1.1 Simplification of the Condition for the Reconstructability

This section shows that the condition (I) makes Lemma 1 simple. Multiplying Eq. (27) by $D_{r_{[k]}}$ gives

$$D_{r_{[k]}} \begin{pmatrix} w_{r_1} \\ w_{r_2} \\ \vdots \\ w_{r_k} \end{pmatrix} = D_{r_{[k]}} \cdot E^{(r_{[k]})} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} = 2^{f_{r_{[k]}}} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} \quad (\because \text{Eq. (42)}). \tag{44}$$

Let $d_{r,c}$ be the (r,c)th element in $D_{r_{[k]}}$. Then, the bottom row of Eq. (44) is written as

$$\sum_{i=1}^{k} d_{k,i} w_{r_i} = 2^{f_{r_{[k]}}} z_k. \tag{45}$$

Comparing Eq. (45) with Eq. (29), we see that Eq. (45) is the special case of Eq. (29). Specifically, substituting the following into Eq. (29) gives Eq. (45).

- $v_i = d_{k,i}$,
- $f_k = f_{r_{[k]}}$ and $g_k = 1$,
- For $j = 1, 2, \ldots, k-1$, $f_j = m$ (i.e., $2^{f_j} = 0$).

Hence, Eq. (34) in Lemma 1 is replaced with

$$m + \max_{w_{r_{[k]}}} \left(f_{r_{[k]}} - m \right) \le c_h,$$

which is simplified into

$$\max_{w_{r_{[k]}}} \left(f_{r_{[k]}} \right) \le c_h. \tag{46}$$

4.1.2 Simplification of the Condition for the Confidentiality

This section shows that the condition (II) makes Lemma 2 simple. The linear summation for the attack is given by Eq. (39). Without decreasing the success probability of the attack, we can assume that there exists an odd element in $u_1, u_2, \ldots, u_{k-1}$, that is, there exists u_i such that $\mathrm{lgd}\,(u_i) = 0$ where $1 \le i \le k-1$. This is for the following reason. For $i = 1, 2, \ldots, k-1$, let $u_i = 2^{a_i} b_i$ where $a_i = \mathrm{lgd}\,(u_i)$ and b_i is odd. Suppose that

$$a_\iota = \min_{1 \le i \le k-1} (a_i) > 0. \tag{47}$$

The linear summation for the attack using $u_1, u_2, \ldots, u_{k-1}$ is written as

$$\sum_{i=1}^{k-1} u_i w_{r_i} = \sum_{i=1}^{k-1} 2^{a_i} b_i w_{r_i} = a^\iota \sum_{i=1}^{k-1} 2^{a_i - a_\iota} b_i w_{r_i}.$$

Hence, the result of the attack using u_i can be obtained from the result of the attack using $2^{a_i - a_\iota} b_i$, but its reverse is not always true.

Equation (35) is written as

$$\begin{aligned} \sum_{i=1}^{k-1} u_i w_{r_i} &= \sum_{c=1}^{k} \left(\sum_{i=1}^{k-1} u_i e_{r_i,c} \right) z_c \\ &= \left(\sum_{i=1}^{k-1} u_i e_{r_i,k} \right) z_k + \left(\sum_{i=1}^{k-1} u_i e_{r_i,\rho} \right) z_\rho \\ &\quad + \sum_{c=1, c \ne \rho}^{k-1} \left(\sum_{i=1}^{k-1} u_i e_{r_i,c} \right) z_c \end{aligned} \tag{48}$$

where ρ is the column index such that

$$\mathrm{lgd}\,(e_{r_i,\rho}) = 0 \quad \text{for} \quad 1 \le \forall i \le k-1,$$

which is the condition (II). Let u_ι be the odd element in $u_1, u_2, \ldots, u_{k-1}$. The second term of right-hand side in Eq. (48) is written as

$$\left(\sum_{i=1}^{k-1} u_i e_{r_i,\rho} \right) z_\rho = u_\iota e_{r_\iota,\rho} z_\rho + \left(\sum_{i=1, i \ne \iota}^{k-1} u_i e_{r_i,\rho} \right) z_\rho. \tag{49}$$

Since u_ι and $u_{r_\iota,\rho}$ are odd elements in $\mathbb{Z}/2^m\mathbb{Z}$, $u_\iota e_{r_\iota,\rho} z_\rho$ is uniformly distributed on $\mathbb{Z}/2^m\mathbb{Z}$ because z_ρ is chosen according to the uniform distribution on $\mathbb{Z}/2^m\mathbb{Z}$. The first term of the right-hand side in Eq. (48), which involves the secret, is covered-up by the first term of the right-hand side in Eq. (49). Subsequently, no information about the secret is given by the any linear summation of any $k-1$ shares.

Since the above-mentioned case corresponds to the case of $f_\iota = 0$ in Eq. (38), Eq. (41) turns out to be

$$c_t \ge \max_{w_{r_{[k-1]}}, u_{[k-1]}} (0 - f_k).$$

Since $c_t \ge 0$ and $f_k \ge 0$, th inequality above always holds.

4.2 Vandermonde Matrix

Let E_{van} be the $n \times k$ Vandermonde matrix in which all the elements are a power of two as follows:

$$E_{\mathrm{van}} = \begin{pmatrix} 1 & 2^0 & 2^{0\cdot 2} & \cdots & 2^{0\cdot(k-1)} \\ 1 & 2^1 & 2^{1\cdot 2} & \cdots & 2^{1\cdot(k-1)} \\ \vdots & & & & \\ 1 & 2^{n-1} & 2^{(n-1)\cdot 2} & \cdots & 2^{(n-1)\cdot(k-1)} \end{pmatrix}. \tag{50}$$

Thus, the (r,c)th element of E_{van} is given by $2^{(r-1)\cdot(c-1)}$. Since E_{van} is the matrix over $\mathbb{Z}/2^m\mathbb{Z}$, the inequality below is required.

$$2^{(n-1)\cdot(k-1)} < 2^m,$$

which is simplified into

$$(n-1) \cdot (k-1) < m. \tag{51}$$

We examine the condition (I) for E_{van}. The determinant of the square Vandermonde matrix $E_{\mathrm{van}}^{(r_{[k]})}$ is given by

$$\begin{aligned} \det\left(E_{\mathrm{van}}^{(r_{[k]})} \right) &= \prod_{1 \le i < j \le k} (2^{r_j} - 2^{r_i}) \\ &= \prod_{1 \le i < j \le k} 2^{r_i} \left(2^{r_j - r_i} - 1 \right). \end{aligned}$$

Since $(2^{r_j - r_i} - 1)$ is odd, $f_{r_{[k]}}$ is given by

$$\begin{aligned} f_{r_{[k]}} &= \mathrm{lgd}\left(\det\left(E_{\mathrm{van}}^{(r_{[k]})}\right)\right) \quad (\because \text{Eq. (43)}) \\ &= \sum_{1 \le i < k} r_i. \end{aligned} \tag{52}$$

Since maximizing Eq. (52) yields

$$\begin{aligned} \max_{w_{r_{[k]}}} \left(f_{r_{[k]}}\right) &= \sum_{i=n-k}^{n-2} i \\ &= \frac{1}{2}(k-1)(2n-k-2), \end{aligned}$$

Eq. (46) turns out to be

$$\frac{1}{2}(k-1)(2n-k-2) \le c_h. \tag{53}$$

As shown in Eq. (50), E_{van} satisfies the condition (II) because all the elements in the first column is odd (i.e., 1). The analysis above is summarized as follows: for given n and k, m and c_h are chosen in such a way that Eq. (51) and Eq. (53) are satisfied. Since any non-negative value is accepted as c_t, c_t is chosen to be zero to maximize the secret size. Then, the bit length of the secret is $m - (k-1)(2n-k-2)/2$.

Scheme 2 in Sect. 2.1 and Scheme 4 in Sect. 2.2 are based on the Vandermonde matrix. Comparing Scheme 3 with Scheme 4, we see that the scheme based on the Vandermonde matrix is not optimal in terms of the secret size. This is because all the elements in E_{van} are a power of 2. Even if some elements are not a power of 2, the matrix may work well as the encoding matrix. However, it is not easy to find the maximum value of f_{r_k} for such a matrix.

5. Concluding Remarks

This article has studied k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$. The advantage of the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ is that all CPUs support modulo-2^m arithmetic operations as primary instructions. This article showed conditions to be satisfied by encoding matrices that characterize k-out-of-n secret sharing schemes. Unlike k-out-of-n secret sharing schemes over a finite field, any k-out-of-n secret sharing schemes using the linear transform over $\mathbb{Z}/2^m\mathbb{Z}$ are non-ideal. That is, the size of a share is larger than that of a secret.

Our conditions are applicable to any matrix over $\mathbb{Z}/2^m\mathbb{Z}$, but it seems infeasible to check if they are satisfied or not when the size of a given matrix is large. In addition, conditions do not suggest how to produce encoding matrices satisfying them. Hence, this article demonstrated the set of encoding matrices such that conditions can be checked efficiently. Such a set includes the Vandermonde matrix in which all the elements are a power of two. In the case of Vandermonde-based encoding matrix, the maximum size of a secret can be easily computed for n, k, and m.

However, the Vandermonde-based encoding matrix is not always optimal in terms of the size of the secret and the number of modular arithmetic operations required for sharing and reconstructing the secret. Our future work includes finding efficient methods to produce the optimal encoding matrix for given n, k, and m.

Acknowledgments This is a product of research which was financially supported in part by the Kansai University Outlay Support for Establish Research Centers, 2015 "Further development of identification technology based on device fingerprints."

References

[1] Fujii, Y., Tochikubo, K., Hosaka, N., Tada, M. and Kato, T.: (k, n) Threshold Schemes Using XOR Operations, *IEICE Technical Report*, Vol. 107, No. 44, pp. 31–38 (2007). (in Japanese).

[2] Igarashi, D., Tsuyuzaki, K. and Kawahara, Y.: SHSS: "Super High-speed (or, Sugoku Hayai) Secret Sharing" Library for Object Storage Systems, *IPSJ SIG Technical Report*, Vol. 2015-CSEC-70, No. 16, pp. 167–174 (2015). (in Japanese).

[3] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T.: A New (k, n)-Threshold Secret Sharing Scheme and Its Extension, *Information Security and Cryptology - ISC 2008, Lecture Notes in Computer Science*, Vol. 5222, pp. 455–470 (2008).

[4] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T.: On a Fast (k, n)-Threshold Secret Sharing Scheme, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E91-A, No. 9, pp. 2365–2378 (2008).

[5] Matsuo, M. and Muto, K.: (k, n)-Threshold Secret Sharing Scheme Using Exclusive OR, *Panasonic Technical Journal*, Vol. 59, No. 2, pp. 29–34 (2013). (in Japanese).