
Todorka Alexandrova
Waseda University, Japan
Email: alexandrova@aoni.waseda.jp

Yoshiaki Suzuki
Kan Okubo
Norio Tagawa
Tokyo Metropolitan University, Japan
Email: yoshiaki.suzuki5@gmail.com, {kanne, tagawa}@sd.tmu.ac.jp

Abstract—In this paper a method for realizing a secret images sharing scheme with general access structure has been proposed. The proposed algorithm for secret images sharing is realized by applying multi-secret sharing schemes based on two-variable one-way functions.

I. INTRODUCTION

The problem of information protection has received a lot of attention in the recent years. Encryption [4] is one of the popular methods to ensure the integrity and security of the protected information. However, the information can not be recovered if the encryption key has been lost or the information has been corrupted during the transmission. Being an important tool in the cryptographic key management, secret sharing schemes [1], [16] allow us to keep the protected information secure and available.

A secret sharing scheme is a technique of sharing a secret s into n pieces, called shares, and distributing them to a set \( \mathcal{P} \) of n users, \( \mathcal{P} = \{U_1, U_2, \ldots, U_n\} \), in such a way that only certain qualified subsets of users can recover the secret by combining their shares and any unqualified subset of users can not do so. In order to define a secret sharing scheme it is necessary to describe the access structure that is characterizing it. Generalized secret sharing schemes and the idea of access structure were first studied in [6]. An access structure on \( \mathcal{P} \) is a pair \((\Gamma, \Delta)\) of collections of subsets of \( \mathcal{P} \). The set \( \Gamma(\subset 2^\mathcal{P}) \) consists of the qualified subsets, i.e., the subsets of \( \mathcal{P} \), that are able to recover the secret after combining their shares and the set \( \Delta \) consists of the unqualified subsets of \( \mathcal{P} \), those that are not able to recover the secret after combining their shares.

A special class of the secret sharing schemes are the so called threshold secret sharing schemes. A special secret sharing scheme is called a \((t, n)\) threshold secret sharing scheme for \( t \leq n \) if the following two conditions are satisfied: i) knowledge of any \( t \) or more shares makes the secret \( s \) computable; ii) knowledge of any \( t-1 \) or fewer shares leaves \( s \) completely undetermined in information theoretic sense.

An important class of secret sharing schemes are the so called perfect secret sharing schemes [18]. A secret sharing scheme is called a perfect secret sharing scheme if the following two conditions are satisfied: i) If a qualified set of users \( A \in \Gamma \) combine their shares, then they can recover the secret \( s \); ii) If an unqualified set of users \( B \in \Delta \) combine their shares, then they can obtain absolutely no information about the secret \( s \) in information theoretic sense. It has been proved that for perfect secret sharing schemes the size of the shares is at least the size of the secret [3]. Secret sharing schemes in which the size of the shares are smaller than the size of the secret are considered as ramp secret sharing schemes [2].

Security is a big concern when considering the storage of image information (e.g., satellite photos or medical images). Noar and Shamir [11] extended the secret sharing concept to the image secret sharing concept, called visual cryptography. Visual cryptography is a perfect secret sharing scheme and requires stacking of any \( t \) image shares to reveal the original image without using any cryptographic computation. However the size of the shared images is much bigger than the original image, as well as the contrast of the recovered image is lower than the original image.

The secret image sharing schemes can be defined in a similar way as the traditional secret sharing schemes. In a secret image sharing scheme, the secret image is used to generate \( n \) image shares (shadows) such that only the qualified subsets of users can recover the secret image by combining their shares and any unqualified subset of users can not do so. In a \((t, n)\) secret image sharing scheme, the secret image is used to generate \( n \) image shares (shadows) such that: i) combining any \( t \), \( (t \leq n) \) image shares the secret image can be recovered and ii) combining any \( t-1 \), or fewer image shares the secret image can not be revealed. In most of the cases these schemes are considered as ramp secret sharing schemes. An important issue in the secret image sharing schemes is the size of each image share. The size of each secret image share should be as small as possible compared to the secret image and this is an important property for the further process of the image shares, such as storage, transmission, or image hiding.

A lot of methods for \((t, n)\) secret image sharing schemes have been proposed recently [10], [14], [19], but fewer secret image sharing schemes for general access structure have been proposed [7], [8], [17].

In this paper we propose an alternative method for secret images sharing scheme that realizes a general access structure. The proposed scheme has the following properties:

- the scheme uses a multi-secret sharing scheme based on two-variable one-way functions;
- participants only need to pool their pseudo-shares instead of disclosing their secret shares when recovering secret images;
- each participant can share many secret images by holding only one secret share;
- the size of each secret share does not depend on the size...
of the secret image;
• it is a lossless multi-use scheme that can be used in different secret sharing sessions without redistributing participants’ secret shares;
• it does not generate shadow images which are difficult to manage and identify;

Integrating the above advantages, the proposed scheme is an effective, reliable and secure multi-use method to protect the secret image from getting lost, destroyed, stolen or corrupted. The scheme is a ramp multiple-secret sharing scheme.

II. BACKGROUND AND PRELIMINARIES

All the calculations in this paper are done in the finite Galois field $GF(q)$, for a large prime number $q$.

A. $(t, n)$ Multi-Secret Sharing Schemes

In order to be able to share multiple secrets, multi-secret sharing schemes were proposed [9], [12], [20]. In these multi-secret sharing schemes a set of $p$ secrets can be shared at once, such that each participant needs to keep one share, called a secret share. In a $(t, n)$ multi-secret sharing scheme combining any $t$, $(t \leq n)$ shares the $p$ secrets can be recovered at once and combining any $t-1$, or fewer shares the $p$ secrets can not be revealed. In order to reconstruct the secrets, the participants need to submit a pseudo-share computed from their secret share instead of the secret share itself. The secret shares are well protected because of the properties of the two-variable one-way function. However, these schemes are also considered as ramp secret sharing schemes.

Definition 2.1. (Two-variable one-way function) [9]. The two-variable one-way function $f(r, s)$ is a function that maps any $r$ and $s$ onto a bit string $f(r, s)$ of a fixed length. This function has the following properties:

(a) Given $r$ and $s$, it is easy to compute $f(r, s)$;
(b) Given $s$ and $f(r, s)$, it is hard to compute $r$;
(c) Having no knowledge of $s$, it is hard to compute $f(r, s)$ for any $r$;
(d) Given $s$, it is hard to find two different values $r_1$ and $r_2$ such that $f(r_1, s) = f(r_2, s)$;
(e) Given $r$ and $f(r, s)$, it is hard to compute $s$;
(f) Given pairs of $r$ and $f(r, s)$, it is hard to compute $f(r', s)$ for $r' = r$.

III. A METHOD FOR REALIZING MULTI-SECRET SHARING SCHEME WITH GENERAL ACCESS STRUCTURE

Here we describe a multi-secret sharing scheme with general access structure in which a dealer $D$ shares a set of $p$ secrets $\{K_1, K_2, \ldots, K_p\}$, among a set of $n$ participants $P = \{U_1, U_2, \ldots, U_n\}$ with access structure $(\Gamma, \Delta)$ on $P$. Let $\Gamma = \{A_1, A_2, \ldots, A_{|\Gamma|}\}$ and $A_i = \{U_1, U_2, \ldots, U_{|A_i|}\}$, $1 \leq i \leq |\Gamma|$. The proposed scheme is an alternative modification of the scheme given in [13]. The method is described in the following three steps.

1) System Setup: Dealer $D$ randomly selects $n$ distinct integers $s_1, s_2, \ldots, s_n \in GF(q)$ as participants’ secret shares and distributes them to every participant over a secure channel.

2) Secrets Distribution: $D$ performs the following steps in order to share the $p$ secrets among the $n$ users:
   a) Chooses distinct sets of $r$ random distinct integers $\{r_{i1}, r_{i2}, \ldots, r_{ip}\}$, corresponding to each qualified subset of users $A_i$, for $1 \leq i \leq |\Gamma|$;
   b) Constructs the $(p-1)$st degree polynomial
      $$h(x) = K_1 + K_2x + K_3x^2 + \ldots + K_px^{p-1}$$
   c) For each qualified subset of users $A_i = \{U_{i1}, U_{i2}, \ldots, U_{i|A_i|}\}$, $1 \leq i \leq |\Gamma|$, $D$ calculates
      $$h_{i1}^* = h((i-1)p) \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i1}, s_{i2}) \ldots \oplus f(r_{i1}, s_{i|A_i|})$$$ where “$\oplus$” stands for the exclusive-or bit by bit.
   d) Publishes $\{f(r_{i1}, s_{i1}), f(r_{i1}, s_{i2}), \ldots, f(r_{i1}, s_{i|A_i|})\}$ for $1 \leq i \leq |\Gamma|$ in any authenticated manner such as in [5], [15]. The number of the public values in this case is $2p|\Gamma|$.

As a next step we are considering the decreasing of this public values. However, we can say that the security in our case is higher compared with one of the multi-secret sharing schemes with general access structure proposed in [13] since the probability that the polynomial values $h((i-1)p), h((i-1)p + 1), \ldots, h(p(\Gamma - 1))$ have been guessed by an adversary is much lower. This can be claimed due to the fact that distinct random values $\{r_{i1}, \ldots, r_{ip}\}$ have been used.

3) Secret Reconstruction: Here we describe how a qualified subset of users $A_i = \{U_{i1}, U_{i2}, \ldots, U_{i|A_i|}\}$ can recover the $p$ secrets $\{K_1, K_2, \ldots, K_p\}$ by combining their pseudo-shares. The participants are able to calculate their pseudo-shares $f(r_{ik}, s_i)$, $i_k \leq k \leq i_p$, $1 \leq i \leq |A_i|$ by using the public value and their secret shares.

Then the values $h((i-1)p), h((i-1)p + 1), \ldots, h(p(\Gamma - 1))$ can be computed as:

$$h((i-1)p) = h_{i1}^* \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i1}, s_{i2}) \ldots \oplus f(r_{i1}, s_{i|A_i|})$$

$$h((i-1)p + 1) = h_{i2}^* \oplus f(r_{i2}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i2}, s_{i|A_i|})$$

$$\ldots$$

$$h(p(\Gamma - 1)) = h_{ip}^* \oplus f(r_{ip}, s_{i1}) \oplus f(r_{ip}, s_{i2}) \ldots \oplus f(r_{ip}, s_{i|A_i|})$$

After these $p$ polynomial values have been obtained the polynomial $h(x)$ of degree $(p-1)$ can be uniquely determined using Lagrange interpolation and the $p$ secrets $\{K_1, K_2, \ldots, K_p\}$ recovered. Analogically, every other qualified subset can recover the $p$ secrets in the same manner. It is also clear that unqualified subset of users can not recover the $p$ secrets.

IV. PROPOSED IMAGE SECRET SHARING

A. Image Characterization
An image $I$ is defined by $c$ number of colors and $d \times l$ pixels $i_{mj}$, $1 \leq i \leq d$, $1 \leq j \leq l$, which form a matrix $M$ with coefficients in $Z_c$ such that:

i) If $I$ is a black and white image, then $M$ is an $d \times l$ matrix, where $m_{ij} = 1$ if the corresponding pixel is black and
steps, \(s_1,s_2,\ldots\), chosen smallest, is the following structure based on the multi-secret sharing scheme with general access structure given in the previous section. It is described in the following three steps.

B. Proposed Method

1) System Setup: Let \(I\) be the secret image. Without loss of generality we assume \(I\) is defined by \(m \times m\) pixels and \(M\) is the \(m \times m\) matrix of it. Let also \(k = \lfloor \log_p m \rfloor\), where \(p > 1\) is any integer number chosen by the dealer. A good choice for \(p\) would be a number for which \(p(2k+1)\lfloor m \rfloor\) is one of the smallest. Later it will be seen that the number of the public values in the proposed scheme is \(p(2k+1)\lfloor |\Gamma|\rfloor\), so \(p\) should be chosen among that values that make this number small.

The dealer \(D\) selects a large prime number \(q > c\), where \(c\) is the number of the colors in \(I\) and \(n\) distinct integers \(s_1,s_2,\ldots, s_n\in GF(q)\) as participants’ secret shares, and distributes them to every participant over a secure channel.

2) Secret Image Distribution: \(D\) performs the following steps in order to share the secret image \(I\) among the \(n\) users:

(a) Chooses distinct sets of \(p\) random distinct integers \(\{r_1,\ldots, r_p\}\), corresponding to each qualified subset of users \(A_i\), for \(1 \leq i \leq |\Gamma|\).

(b) Constructs the \(2k\) polynomials of degree \(p-1\)

\[
egin{align*}
    h_1(x) &= a_0^1 + a_1^1 x + \ldots + a_{p-1}^1 x^{p-1}, \\
    h_2(x) &= a_0^2 + a_1^2 x + \ldots + a_{p-1}^2 x^{p-1}, \\
    &\vdots \\
    h_{2k}(x) &= a_0^{2k} + a_1^{2k} x + \ldots + a_{p-1}^{2k} x^{p-1},
\end{align*}
\]

(7) \(\ldots\)

(9)

where the coefficients in each polynomial are distinct and randomly selected by the dealer \(D\).

(c) For each qualified subset of users \(A_i = \{U_{i1}, U_{i2}, \ldots, U_{i|A_i|}\}\), \(1 \leq i \leq |\Gamma|\) and for each polynomial \(h_1(x), h_2(x), \ldots, h_{2k}(x)\), \(D\) calculates the following values, respectively:

\[
egin{align*}
    h_1^{(i)} &= h_1((i-1)p) \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}), \\
    h_2^{(i)} &= h_2((i-1)p+1) \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}), \\
    &\vdots \\
    h_{2k}^{(i)} &= h_{2k}((i-1)p) \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}).
\end{align*}
\]

(10) \(\ldots\)

(14)

(d) \(D\) computes the \(p^k \times p^k\) secret matrix \(M'\) as follows.

For \(k = 1\) and \(1 \leq i,j \leq p\)

\[
    m_{i,j} = (a_0^{1,1} + a_0^{2,2}) \mod c,
\]

and for \(k > 1\), and \(1 \leq i,j \leq p^k\)

\[
    m_{i,j} = \left( \sum_{r=1}^{k-1} a_r^r \left[ \frac{x^{p^{r-1}}}{p^{r-1}} \right] \right) + \sum_{r=k+1}^{2k-1} a_r^r \left[ \frac{x^{p^{(r-1)-1}}}{p^{(r-1)-1}} \right] + a_0^{(i-1) \mod p} + a_0^{(j-1) \mod p} \mod c.
\]

(15) \(\ldots\)

(18)

(e) \(D\) computes the \(m \times m\) matrix \(M''\) as follows

\[
    M'' = M + M',
\]

(19) \(\ldots\)

(22)

where \(M'\) is the following \(m \times m\) matrix

\[
    m_{i,j} = (a_0^{1,1} + a_0^{2,2}) \mod c
\]

and \(M'' = M + M'\).

(f) \(D\) publishes \(\{\{r_1, \ldots, r_p\}, \{h_1^{(1)}, h_2^{(1)}, \ldots, h_{2k}^{(1)}\}\}, \{h_1^{(2)}, h_2^{(2)}, \ldots, h_{2k}^{(2)}\}, \ldots, \{h_1^{(|\Gamma|)}, h_2^{(|\Gamma|)}, \ldots, h_{2k}^{(|\Gamma|)}\}\) for \(1 \leq i \leq |\Gamma|\) and \(M''\) in any authenticated manner such as in [5], [15].

Hence, the number of the public values is \(p(2k+1)\lfloor |\Gamma|\rfloor + m^2\).

An important feature of the proposed scheme is the fact that a single public image \(M''\) is generated for all the qualified subsets.

3) Secret Image Reconstruction: Here we describe how a qualified subset of users \(A_i = \{U_{i1}, U_{i2}, \ldots, U_{i|A_i|}\}\) can recover the secret image \(I\) by combining their pseudo-shares and using the public values.

(a) The participants are able to calculate their pseudo-shares \(f(r_{ik}, s_{ik}), 1 \leq k \leq p^k, 1 \leq l \leq l_{i|A_i|}\) by using the public values and their secret shares.

(b) Then the values \(h_1((i-1)p), h_1((i-1)p+1), \ldots, h_1(p^k-1)\) can be computed as:

\[
    h_1((i-1)p) = h_1^{(i)} \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}).
\]

(23)

\[
    h_1((i-1)p+1) = h_2^{(i)} \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}).
\]

(24)

\[
    h_1(p^k-1) = h_{2k}^{(i)} \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}).
\]

(25)

\[
    h_1(p^k) = h_1^{(i)} \oplus f(r_{i1}, s_{i1}) \oplus f(r_{i2}, s_{i2}) \ldots \oplus f(r_{i|A_i|}, s_{i|A_i|}).
\]

(26)

After these \(p\) polynomial values have been obtained the polynomial \(h_1(x)\) of degree \((p-1)\) can be uniquely determined using Lagrange interpolation and the \(p\) coefficients of the polynomial are uniquely determined.

Analogically, the values \(h_2((i-1)p), h_2((i-1)p+1), \ldots, h_{2k}((i-1)p+1)\)
1),...,h_{2k}(pi-1)} can be determined and the coefficients of the polynomials h_2(x), h_{2k}(x) uniquely determined.

(c) Then, the secret matrix M' is computed as described in Eqs. (24)-(26).

(d) The matrix M is obtained by

\[ M = M' \oplus M^*. \]  

(27)

(f) The secret image I is recovered from M.

V. EXAMPLE

Let \( P = \{U_1, U_2, U_3, U_4\} \) and \( A_1 = \{U_1, U_2\}, A_2 = \{U_3, U_4\} \) are the qualified subsets of users. Let \( q = 1031 \) and the secret image is the 256 \( \times \) 256 gray scale image of Lenna, given in Figure 1. In this example \( p = 4 \) and \( k = 4 \).

\( D \) chooses \( r_{11} = 3, r_{12} = 5, r_{13} = 98, r_{14} = 162, r_{21} = 213, r_{22} = 85, r_{23} = 11, r_{24} = 45; s_1 = 8, s_2 = 23, s_3 = 45, s_4 = 195; h_1(x) = 246 + 30x + 724x^2 + 7x^3, h_2(x) = 629 + 420x + 256x^2 + 672x^3, h_3(x) = 330 + 106x^2 + 532x^2 + 169x^4, h_4(x) = 910 + 687x^2 + 874x^2 + 786x^3, h_5(x) = 832 + 652x + 732x^2 + 710x^3, h_6(x) = 330 + 548x + 900x^2 + 56x^3, h_7(x) = 515 + 446x + 932x^2 + 649x^3, h_8(x) = 1013 + 603x + 866x^2 + 483x^3.

The public values corresponding to \( A_1 \) are:

\( \begin{align*}
(\{h_{11}, h_{12}, h_{13}, h_{14}\} & = \{224, 864, 279, 956\}, (\{h_{11}, h_{12}, h_{13}, h_{14}\} = \{611, 298, 702, 789\}; \\
(\{h_{21}, h_{22}, h_{23}, h_{24}\} & = \{34, 78, 714, 931\}, (\{h_{21}, h_{22}, h_{23}, h_{24}\} = \{854, 141, 393, 484\}; \\
(\{h_{31}, h_{32}, h_{33}, h_{34}\} & = \{533, 971, 310, 764\}, (\{h_{31}, h_{32}, h_{33}, h_{34}\} = \{995, 628, 893, 912\}.
\end{align*} \)

The public values corresponding to \( A_2 \) are:

\( \begin{align*}
(\{h_{21}, h_{22}, h_{23}, h_{24}\} & = \{839, 788, 889, 398\}; (\{h_{21}, h_{22}, h_{23}, h_{24}\} = \{860, 662, 459, 152\}; \\
(\{h_{31}, h_{32}, h_{33}, h_{34}\} & = \{454, 252, 440, 74\}; (\{h_{31}, h_{32}, h_{33}, h_{34}\} = \{13, 573, 155, 141\}; \\
(\{h_{41}, h_{42}, h_{43}, h_{44}\} & = \{119, 330, 19, 181\}; (\{h_{41}, h_{42}, h_{43}, h_{44}\} = \{1018, 88, 37, 370\}.
\end{align*} \)

The obtained 256 \( \times \) 256 secret matrix M' and the public shared image M'' are given in Fig. 2.

Fig. 1. Secret Image I (256 \( \times \) 256).

Fig. 2. Secret Matrix M' and Public Image M''.

It can be seen that from the public image M'', the secret image contents can not be figured out. However if a qualified subset of participants pool out their pseudo-shares, then they can recover in a lossless manner the original secret image I in Figure 1 using the described reconstruction procedure.

VI. CONCLUSION AND FUTURE WORK

In this paper a lossless method for realizing secret images sharing scheme with general access structure has been proposed. It is realized by applying multi-secret sharing schemes based on two-variable one-way functions. Each participant only needs to hold one secret share in order to be able to share the secret image. Moreover, the proposed scheme is a multi-use secure secret image sharing scheme and does not generate shadow images which are difficult to manage and identify.

As a future work we consider the decreasing of the number of the public values of the proposed scheme. As another direction we consider the improving of the security performance of the proposed scheme and giving a more precise and theoretical security analysis of the proposed method.

REFERENCES