A New Group-based Secret Function Sharing with Variate Threshold

Anneke Soraya Hidayat†, Dae-Soo Kim†, Eun-Jun Yoon† and Kee-Young Yoo†*
† School of Computer Science and Engineering
Kyungpook National University
Daegu, South Korea
‡ Department of Cyber Security
Kyungil University
Gyenggsan-Si, Gyeongbuk, South Korea
Email: annekesoraya@gmail.com, stairways@infosec.knu.ac.kr, ejyoon@kiu.kr, yook@knu.ac.kr*
*Corresponding Author

Abstract—Secret sharing is a cryptographic scheme that divides a secret key $s$ to $n$ participants with threshold $t$. Thus, assuring that no less than $t$ shares can reconstruct the secret. The application of secret sharing also widens not only one group but several hierarchical structure. However, the group-based secret sharing proposed by Liu et al. in 2014 has some drawbacks, which are having an equal threshold for each group and also reconstruct only partial secret when the present groups are less. In this paper, we attempt to apply a group-based hierarchical structure in secret sharing by applying derivation. The proposed scheme is the first approach of combining a hierarchical structure and a group-based secret sharing. The proposed scheme shows a better security than Liu et al. considering the structure of the group. Also, it has varied threshold in each group, which is possible for giving less threshold for high-level participants and more threshold for low-level participants.

Keywords—Secret Sharing, Group Access Control, Hierarchical, Variate Threshold

Track—Cryptographic Technologies, Secret Sharing.

I. INTRODUCTION

Secret sharing has been widely known for securing the key among a group of parties. In the traditional symmetric cryptography algorithms, such as DES [1] and AES [2], a single key is required to encrypt and decrypt the secret message among two parties. The same concept is also applied to asymmetric cryptography [3]. The problem arises when the number of parties is increased to more than two. As the problem considered in Shamir’s paper [4], we need a numerous number of keys to be shared among parties in one group for securing the documents in a cabinet, thus they can combine the keys and open the locks of the cabinet by the keys carried by the given parties. However, the number of keys and locks increases exponentially and is impossible to apply in the practical world.

In the threshold cryptography, secret sharing has been widely known for securing the key among a group of parties. Secret sharing presented as $(t, n)$—threshold in which at least $t$ number of parties among the $n$ parties in one particular group can reconstruct the secret key $s$. This system reduces the computational time required and simplifies the system. One of the world practical examples of secret sharing is its application in DNSSec [5], [6].

Secret sharing method was introduced by Shamir [4] and Blakley [7] in 1979. Both of them proposed secret sharing with different approaches, polynomial interpolation and geometry spaces, respectively. In Shamirs scheme, secret sharing divides a secret key $s$ into $n$ different pieces of shares by using a polynomial with $t - 1$ degree. The reconstruction phase is conducted by combining, at least, $t$ shares from the group and calculating altogether by using Lagrange interpolation. These schemes assure that no less than $t$ shares can reconstruct the secret key. Shamirs secret sharing is considered safe since the third party (active adversary in this context) cannot break the computational bound, in other words, this scheme is unconditionally secure. Apart from the mentioned two schemes, there are some secret sharing methods which is use different mathematical approaches [8], [9].

In the wide 30 years of secret sharing innovation, several approaches have been proposed such as Chinese Remainder Theorem based [8], [9], Boolean operation based [10]. Other secret sharing [11] which is based on the polynomial differential-based. Blundo [12] and Pang [13], which based on multi-secret sharing scheme.

The hierarchical secret sharing was first introduced by Tassa [14] in 2007. It used Birkhoff interpolation which is applied to the hierarchical system in secret sharing. Then, more schemes related to hierarchical sharing has been proposed [15]. Suppose there is a set of participants that is partitioned into several levels, where each group has threshold relation as $t_1 > t_0$. Thus, by combining shares from each group by the given threshold condition is possible.

The group-scalable secret image sharing scheme was proposed by Liu et al. in 2014 [16]. The secret image is divided to four different quality image and distributed to each group by applying secret sharing polynomial. However, this paper can only reconstruct partial secret when there is less group presence, also, the threshold in each group remains the same.

In this paper, we propose a new group-based secret function sharing with variate threshold which is the first scheme with
hierarchical and group-based secret sharing. This scheme is also an improvement from previous schemes [11], [17] which based on the polynomial differential-based. Also, we are using a secret function $g(x)$ with degree $k$ as the secret polynomial key. The variate threshold here means that this scheme can produce a different variance of threshold in several groups, which are bound to each other. Our intention is to improve the basic Shamir's secret sharing with Lagrange interpolation rather than using another mathematical approach, such as Birkhoff interpolation. We prove that it has a higher security compared to Liu et al.'s scheme.

This paper is organized as follows. Section two shows the related works. The proposed scheme is described in section three. The comparison of performances between previous works and proposed scheme is discussed in section four. Finally, some conclusions are given in section five.

II. RELATED WORKS

A. Shamir's secret sharing

Shamir's secret sharing [4] is based on linear polynomial interpolation. Suppose the dealer $D$ ought to divide the secret key $s$ to $n$ participants with the threshold value $t$. The dealer generates polynomial $f(x)$ with degree $t - 1$ with $s$ inserted as one of the variables. The polynomial equation shown as below.

$$f(x) = s + a_1x + ... + a_{t-1}x^{t-1} \mod q \quad (1)$$

$p$ is a large prime number, $s$ is the secret message and $a_i \in p, i = 1, \ldots, t - 1$ are the random number generated in $Z_p$. Meanwhile, $x$ is each participant $ID$. Each participant will receive one unique share $y_j = f(x_j), j = 1, \ldots, n$. Here, $n \leq p$ is suitable to apply, since it may reduce the collision between each participants shares. In the reconstruction phase, the dealer will collect no less than $t$ shares $(x_j, y_j)$ from a group of $n$ participants, and conduct the computation as follow.

$$f(x) = \sum_{j=1}^{m} y_j \prod_{k=1, k \neq j}^{m} \frac{x - x_k}{x_j - x_k} \mod q \quad (2)$$

Equation 2 is used to reconstruct the original polynomial $f(x)$. Variable $m$ stands for the number of available participants, where $t \leq m \leq n$. Here, it has to be noted that participants cannot be less than $t$. Otherwise, the polynomial cannot be reconstructed due to the Lagrange interpolation correctness. Finally, the secret key $s$ is equal to $f(0)$. All transmissions in this scheme between dealer and participants are assumed to be sent via a secure channel. The model of this scheme is centered; there is no interaction between participants.
B. Group Scalable Secret Image Sharing

Liu et al. proposed a grouped-scalable secret image sharing scheme in 2014 [16]. This scheme used an image as a secret key which is denoted as a secret image as shown in figure 1. The dealer divides the secret image \( S \) into 4 sub-images \( S_i, i = \{1, ..., 4\} \) by using a bit-plane decomposition by using the expression below.

\[
l_i = \{b_{i_8}b_{i_7}b_{i_6}b_{i_5}b_{i_4}b_{i_3}b_{i_2}b_{i_1}\}
\]

\[
S_1 = (S_1||b_{i_8}||b_{i_4})
\]

\[
S_2 = (S_2||b_{i_7}||b_{i_3})
\]

\[
S_3 = (S_3||b_{i_6}||b_{i_2})
\]

\[
S_4 = (S_4||b_{i_5}||b_{i_1})
\]

where \( l_i \) is the pixel of the secret image \( S \), \( b_{i_j} \) is the byte expression of each pixel \( l_i \) and \( i = 1, ..., M \times N \). \( M \) and \( N \) is the width and height of the image. Four sub-images act as secret keys for each management group and divides each by using secret sharing schemes. Before the shares are distributed to participants in each group, each share hides in a cover image to prevent detection from the third party and disclose the shares into a camouflage.

In the reconstruction phase, it simply reverses the distribution phase on each groups sub-images. Each sub-image has different quality of output, although it shows a lower quality of secret image depending on the priority of the groups. The secret images will show a better quality depending on how many groups are joined. Should any reader wishes to look at the detailed algorithm, please refer to the paper.

This scheme is only limited to four subgroups due to the bit-plane limitation. Practically, every management groups are not always in a static number and can dynamically change. Since the output is an image, each sub-group can somewhat guess the object of the image, without respect to joining with another group.

III. PROPOSED SCHEME

A. Preliminary

The dealer \( D \) generates the polynomial secret function \( h(x) \) with degree \( k \).

\[
h(x) = a_0 + a_1x + \ldots + a_kx^k \mod q \quad (3)
\]

Here, there are three important variables which have to be set in advance. \( k, r, \) and \( g \) are the polynomial secret degree, the number of round/integral which will be explained in the next subsection, and the number of total group assigns in the hierarchical structure, respectively. First, the dealer assigns the number of groups \( g \) and the secret polynomial degree \( k \). Thus, the number of rounds/integral \( r \) are shown using the relationship \( r = g - 1 \). The number of rounds/integral \( r \) purpose is to appoint the number of group.

B. Share Distribution

The dealer \( D \) computes the distribution phase by using the given variables which are assigned in the preliminary stage. The distribution algorithm will be described as follows.
Calculation Example of Distribution Phase

1. Given \( g(x) = x^2 + x + 1 \), \( k = 2 \), \( g = 4 \), and \( r = 3 \). All integers are performed in \( Z_{23} \).

2. Integral by \( r = 3 \)

\[
H(x) = \int_{a}^{b} h(x)dx = C_r + \sum_{k=0}^{t} \left( \begin{array}{c} \sum_{k=0}^{t} \frac{a_k x^{k+1}}{b} \end{array} \right) \]

3. Generate the function for groups by transform the denominators into binary polynomial \( GF(2^p) \)

\[
f_0(x) = x^5 + x^4 + x^3 + 2x^2 + 5x + 13
\]

\[
f_1(x) = x^5 + x^4 + x^3 + 2x^2
\]

\[
f_2(x) = x^4 + x^3
\]

\[
f_3(x) = x^2 + x
\]

\[
f_4(x) = x
\]

4. Calculate each shares for participants for each groups

**Assume that each participant ID \( x_i = i, i = \{1, \ldots, n\} \)**

<table>
<thead>
<tr>
<th>Group 0</th>
<th>Group 1</th>
<th>Group 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_0(1) = 0 )</td>
<td>( f_1(1) = 4 )</td>
<td>( f_2(1) = 2 )</td>
</tr>
<tr>
<td>( f_0(2) = 18 )</td>
<td>( f_1(2) = 14 )</td>
<td>( f_2(2) = 1 )</td>
</tr>
<tr>
<td>( \ldots )</td>
<td>( \ldots )</td>
<td>( \ldots )</td>
</tr>
<tr>
<td>( f_0(6) = 87 )</td>
<td>( f_1(6) = 9 )</td>
<td>( f_2(5) = 14 )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group 3</th>
<th>Group 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_3(1) = 2 )</td>
<td>( f_4(1) = 1 )</td>
</tr>
<tr>
<td>( f_3(2) = 6 )</td>
<td>( f_4(2) = 2 )</td>
</tr>
<tr>
<td>( f_3(3) = 12 )</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3. Calculation example of distribution phase

1) Integrate the secret polynomial \( h(x) \) by \( r \) rounds. Leave the coefficient’s fraction as numerator and denomin \( a/b \).

\[
H(x) = \int_{a}^{b} h(x)dx = C_r + \sum_{k=0}^{t} \left( \begin{array}{c} \sum_{k=0}^{t} \frac{a_k x^{k+1}}{b} \end{array} \right)
\]

2) Generate \( g \) sub-function \( f_i(x) \), \( i = 0, \ldots, g \) by changing the form in denominator of each variable \( a_i \) in \( G(x) \) into binary polynomial \( GF(2^p) \), generated \( g \) groups.

\[
f_i(x) = \{ \text{polynomial} \}_{GF(2^p)} \leftarrow \{ \text{denominator} \}_{10}
\]

where \( i = 1, \ldots, g \). Each sub-function \( f_i(x) \) generated a variate threshold depends on the denominator value.

3) Assign each sub-function in each group and generate shares by using each participant’s ID from the corresponding group. Here, the highest priority group should be the sub-function which has the lowest threshold degree by \( t - 1 \) and vice versa.

\[
f_{ij}(ID)
\]

4) Send the shares to the corresponding group via the private secure channel.

The example of distribution phase shown in the figure 3 with \( C_1 = 2 \), \( C_2 = 5 \) and \( C_3 = 13 \).

C. Share Reconstruction

The reconstruction phase requires all the groups to reconstruct the corresponding sub-functions in order to reconstruct secret polynomial \( g(x) \). The complete detail of reconstruction algorithm will be described as follows.

1) Collect all shares and reconstruct each groups sub-function \( f_{ij}(x) \), \( i = \{0, \ldots, g - 1\}, j = \{1, \ldots, t\} \) by using Lagrange interpolation in equation 2 according to each groups threshold value \( t \).

2) The dealer collects all the sub-functions and changes the form from polynomial into an integer in \( Z_p \).

\[
\{ \text{denominator} \}_{10} \leftarrow \{ \text{polynomial} \}_{GF(2^p)}
\]

3) Assign each integer into denominator in \( f_0(x) \), such that \( G(x) \leftarrow f_0(x) \).

4) Derive the polynomial \( f_0(x) \) \( r \) times and get the secret polynomial \( g(x) \).

\[
g(x) = \frac{d^r}{dx}(G(x))
\]

IV. Security Analysis

The Shamirs secret sharing schemes analysis has been proposed recently [18]. The correctness and privacy of Shamirs secret sharing follow the Lagrange interpolation theorem. For every, at least, \( t \) distinct values \( x_1, \ldots, x_t \) and any \( t \) values \( y_1, \ldots, y_t \), there exists a unique polynomial \( f(x) \) of degree which determines the secret. It assures that no \( t - 1 \) can reconstruct the secret. It also shows that participants ID \( x \) does not depend on the secret . The proposed scheme has an equal security level with Shamirs secret sharing as stated below.

Correctness Secret sharing assures that a pool of \( t \) or more participants can reconstruct the secret. It is obvious that a set of \( t \) participants carries \( t \) points of a polynomial
\( P \) with a degree \( t - 1 \), which can be reconstructed by computing \( s = P(0) \). Hence, we can conclude that \( P(0) = f(0) = s \). Additionally, as mentioned above, the participants \( TD \) does not depend on the secret \( s \). The correlation between \( TD \) and secret is shown in the Lagranges interpolation equation (2) linearly simplified below. The ID depends only with the pool of participants with size \( t \).

\[
\sum_{k=1}^{t} B_k \cdot y_{i_k}, \text{ where } B_k = \prod_{i \in S, j \neq k} \frac{x_{i_j}}{x_{i_j} - x_{i_k}}
\]

**Privacy** Any participants group with at most \( t - 1 \) wish to reconstruct the secret by using \( y_{i_k}, k = 1, \ldots, t - 1 \), together their shares determines a unique polynomial \( P \) with degree \( t-1 \). The polynomial determines every possible secret where \( P(0) = a \) and \( P(x_i) = y_i \), for \( i = 1, \ldots, n \). Thus, the probability is shown as below.

\[
\Pr[f(x_i) \mid y_{i_k} \leq t-1] = \frac{1}{p^{t-1}}
\]

The proposed scheme has an equal security level to Shamir’s secret sharing. However, the secret form is in the function form and the groups which have varied threshold bind the secret and make it difficult to reconstruct. The advantages of the proposed scheme are shown below.

1) The secret function \( g \) has a form of \( a_0 + a_1 x + \ldots + a_k x^k \). Each of the variables in the function \( g \) has a domain of \( p \) since all of the secrets are conducted in modular \( p \). If one of the adversaries \( A \) wants to guess the secret function, the probability of \( A \) successfully guess the function is described below.

\[
\Pr[g \mid T] = \frac{1}{p + (k - 1)p^2}
\]

where, \( T = \{y_1, y_2, \ldots, y_t\} \). It also can be extended of one of the adversaries wishes to reconstruct the secret by using \( y_{i_k} \) to put on the pool of \( k \) participants, it is nearly impossible to construct, since \( \Pr[f(x_i) \mid y_{i_k} \leq t-1] = \frac{1}{(p + (k - 1)p^2)^T} \). Meanwhile, Shamir’s secret sharing domain is only \( p \) with the probability \( \frac{1}{p} \).

2) The number of groups desired affects the threshold for the first group which acts as the function of the lowest group. Consider a big group \( G = \{t_1, t_2, \ldots, t_g\} \), the threshold relation for each group can be expressed by \( t_1 > t_2 > \ldots > t_g \). Meanwhile in Liu et al. scheme, the threshold of each group remains the same, which does not represent the hierarchical system.

V. Conclusion

In this paper, the group-based secret function sharing with variate threshold has been proposed. Based on the traditional Shamir’s secret sharing, we developed a hierarchical secret sharing system which is constructed in several groups with variate threshold in each group. Here, the secret form used is in a function form in order to increase the security and reduce the chance for an adversary to reconstruct the secret with fake shares, even only with a guess. This system requires all the group together to reconstruct the secret. The security analysis shows that the proposed scheme has a higher security compared to Liu et al. scheme.

In the future, we are trying to improve the combination for each group, allowing only a few groups to reconstruct a part of the secret by using a different approach of polynomial interpolation. Also, unlocking the static threshold, makes it possible for dealers to determine each groups threshold without considering the degree of the secret function.

**ACKNOWLEDGMENT**

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2015R1A2A2A01006824) and by the Ministry of Education(NRF-2015R1D1A1A01060801).

**REFERENCES**


