Hierarchical Threshold Secret Image Sharing Scheme Based on Birkhoff Interpolation and Matrix Projection

Zhenhua Tan[1]*, Danke Wu[1], Hong Li[1], Tianhan Gao[1], and Nan Guo[2]
[1]Software College
[2]School of Computer Science and Engineering
Northeastern University, Shenyang 110819, China

Abstract

This paper focuses on how to protect confidential image based on hierarchical threshold secret sharing scheme, against fake shadow attacks, collusion attacks and shadow information leakage problem. Inspired by existing research, we propose a novel hierarchical threshold secret sharing scheme based on Birkhoff interpolation and matrix projection, hierarchical secret distribution mathematical processes and hierarchical threshold reconstruction mathematical processes are proposed in detail in this paper, by designing random matrix generation, polynomial multiple derivatives, and Birkhoff interpolation method in Galois field. Simulations and analysis validate the proposed scheme can tolerate fake shadow attacks and collusion attacks, and has the ability to avoid information leakage. Experiments also prove that shadow secret embedding capacity of secret cover image is bigger than the existing schemes.

Keywords: Hierarchical Secret Sharing, Hierarchical Access Structure, Secret Image Protection, Birkhoff Interpolation, Matrix Projection

1 Introduction

Secret sharing is an important method of protecting data. It 's mainly used for the security storage, transmission and utilization of confidential information, trust evidence, confidential documents, and privacy information and so on. With the development of the Internet, how to protect secret information in cyber space has become a hot topic.

A.Shamir [8] and G.Blakley [1] proposed the $< t,n >$ threshold secret sharing scheme respectively. The scheme contain two phrases, the secret sharing phrase and the secret reconstruct phrase. In secret sharing phrase, the Dealer divided the secret data into n shadows through the rule of algorithm. Next, the Dealer shared the shadows to n participants by one-on-one. In the secret reconstruct phrase, at least k participants arbitrarily could reconstruct the secret, under the number of k participants, the participants can't get any information. These two schemes are the milestone of threshold cryptography, and are widely used in cloud storage and protection of private data.

But the participants in the traditional threshold secret sharing scheme have the same importance, the algorithm can't achieve the hierarchical authorization, and can't directly meet the requirements of the hierarchical authorization protection. For this kind of problem, the hierarchical threshold secret sharing scheme of multi-level threshold access structure is proposed, which is divided into two-layer structure secret sharing scheme[6, 11, 7, 2], and multi-level threshold sharing scheme [5, 10, 4]. The two-layer structure scheme is mainly to realize (t,s,k,n) two-level threshold access structure; The main idea of the hierarchical threshold sharing scheme is to set the threshold depend on the threshold level,

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 4, Article No. 13 (October 15, 2018)
*Corresponding author: Zhenhua Tan, Software College, Northeastern University, Shenyang 110819, China, Email: tanzh@mail.neu.edu.cn

setting the different threshold for each level of the participants, forming the hierarchical threshold scheme $< k_1, N_1 >, \cdots, < k_s, N_s >$. It is widely used in distributed data storage, key management, cloud storage, privacy data, trust data, and so on.

The existing hierarchical access structure of the threshold secret sharing scheme effectively solves the hierarchical threshold of the algorithmic mathematical process. In these scheme, the common scientific problems being studied are false data attacks, collusion attacks, and shadow secret equivalence issues. Inspired by literatures [3, 10] based on the Birkhoff interpolation and projection matrix, we proposed a multi-layer threshold secret sharing scheme. Moreover, our paper are also combined with our previous experience on the verifiability problem, collusion problem threshold scheme [9]. The algorithm and the reconstruction algorithm are designed and implemented for the secret image field. The main idea is to set the $(l+1)-th$ threshold scheme $TSet =< t_0, t_1, \ldots, t_l >$ on a finite field for n participants. Based on the hierarchical threshold $\langle t_i, N_i \rangle$ form the whole $\langle \sum_{w\in[0,l]} t_w, n \rangle$ threshold scheme. A polynomial random coefficient matrix is generated based on the projection matrix method on the finite field. Based on the hierarchical threshold setting of the participant, the shadow secret matrix is generated by the multi-order polynomial. The corresponding shadow secret data is written to the same cover image, and the distribution process is completed by the Dealer to the participants at all levels. In the process of reconstruction, the basic data is calculated based on the Birkhoff interpolation method by the Dealer, proposed algorithm reversed the operation of the shadow data Alignment to complete the final original image recovery process. The main contributions of this paper are as follows:

(1) A novel hierarchical secret sharing scheme for network space secret image protection is proposed. The projection operation based on random matrix generation, the shadow secret matrix generation by polynomial multi-order derivative, and the Brikhoff interpolation recovery operation which complete hierarchical threshold shared scheme $\langle \sum_{w\in[0,l]} t_w, n \rangle$ is formed, and the related process is demonstrated by setting the lemma to improve the security of image secret sharing.

(2) The proposed scheme has the ability to defend the fake data attack. Furthermore, the scheme has the ability to recognize whether the secret has been attacked. What's more, it has the ability to defend the collusion attack which can be regarded as multi-layer participants trying to restore the original secret. After all, the relevant ability was demonstrated.

(3) Based on the same coefficient matrix, polynomial multi-order derivative to form the shadow secret matrix with the same size and different content, which avoids the traditional basis of the polynomial. The Brikhoff interpolation scheme uses only constant information leakage problems.

2 Basic Definitions

In this paper, a new hierarchical secret image sharing scheme is proposed by using the projection matrix and Birkhoff interpolation method. In the sharing process, the secret Dealer according to the participants in the collection and the secret image information, calculate the corresponding secret data and embed it in the cover image, get the shadow of the secret information image. In the secret reconstruction process, the secret data is extracted in the shadow image which provided by the participant satisfying the threshold condition, and the polynomial is reconstructed by using the Birkhoff interpolation method. From the reconstructed polynomial to the corresponding polynomial coefficient information, calculate the corresponding projection matrix, restore the open secret matrix, and finally get the original secret pixel matrix. For ease of description, the relevant definition of the convention:

(1) Dealer: Any node in a distributed network that requires distributed data for distributed sharing, as a Dealer.

(2) Participants: n nodes that participate in secret sharing in a distributed network, whose collection

is written as: $PSet = \{p_1, \cdots, p_n\}$.

$$n = \sum_{i=0}^{l} N_i$$

(3) Multi-threshold: All participants are divided into $l+1$ layer, ie $Level = 0, \cdots, l$, the number of participants per layer is $N_0, \cdots, N_l$, and no two participants have no intersection. The minimum threshold for each participant is marked as a vector $TSet =< t_0, t_1, \cdots, t_l >$, $0 < t_0 < t_1 < \cdots < t_l$ monotonically increasing, and the last threshold is denoted by $k = t_l$. The sum of all the levels of the threshold is called $\mathbb{K} = \sum_{(w \in [0,l])} t_w$, then the hierarchical threshold scheme for each layer is $\langle t_i, N_i \rangle$, the overall hierarchical threshold scheme for $\langle \mathbb{K}, n \rangle$.

(4) Secret image: the program for data protection of the image agreement for the square matrix SI, $m \times m$ matrix:

$$SI = (s_{ij})_{m \times m} = \begin{bmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & \ddots & \vdots \\ s_{m1} & \cdots & s_{mm} \end{bmatrix}$$

(5)Finite field: In this paper, the participant number and random matrix element belongs to the finite field $F_{\mathbb{p}} = \mathbb{Z}/\mathbb{p}$, where $\mathbb{p}$ is the prime number and satisfies according to the Birkhoff interpolation:

$$\mathbb{p} > 2^{-k+2} \cdot (k-1)^{\frac{k-1}{2}} \cdot (k-1)! \cdot n^{(k-1)(k-2)/2}$$

3 Proposed Threshold Secret Distribution Model

The $m \times k$ random matrix A with the rank k on the finite field $F_p^{(m \times k)}$ is constructed and $det(A^T A) \neq 0$:

$$A = (a_{ij})_{m \times k} = \begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mk} \end{bmatrix} \tag{1}$$

Where a_{ij} is a random integer, $rank(A) = k$, column full rank matrix. $det(A^T A) \neq 0$, so $A^T A$ is reversible, then the projection matrix of matrix A is:

$$\mathbb{S}_A = (\mathfrak{s}_{ij})_{m \times m} = A(A^T A)^{-1} A^T = \begin{bmatrix} \mathfrak{s}_{11} & \cdots & \mathfrak{s}_{1m} \\ \vdots & \ddots & \vdots \\ \mathfrak{s}_{m1} & \cdots & \mathfrak{s}_{mm} \end{bmatrix} \tag{2}$$

Each element of the image SI is a positive integer, and the elements in the projection matrix $\mathbb{S}_A$ are generally floating point numbers. Therefore, the sum of each element and the distributor id of the image SI is changed so that each row of data is converted into a floating point number, that is:

$$s_{ij}^{Float} = \frac{s_{ij}}{Dealer.id + s_{ij}} \tag{3}$$

$$SI_{Float} = \begin{bmatrix} s_{11}^{Float} & \cdots & s_{1m}^{Float} \\ \vdots & \ddots & \vdots \\ s_{m1}^{Float} & \cdots & s_{mm}^{Float} \end{bmatrix} \tag{4}$$

By plotting the corresponding elements of the projection matrix $\mathbb{S}_A$ and the image floating-point matrix SI_{Float} by floating-point XOR operation, the matrix matrix R_{SI} is formed:

$$R_{SI} = (r_{ij})_{m\times m} = \begin{bmatrix} r_{11} & \cdots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mm} \end{bmatrix} \tag{5}$$

Where $r_{ij} = s_{ij} \oplus s_{ij}^{Float}$, $\oplus$ is a floating point XOR operation. Floating-point processing of the image SI is intended to protect the attacker from detecting the original image by separating the integer part, the fractional part, or the result.

After the above steps are completed, the Dealer Dealer public secret matrix R_{SI}.

Then, Constructing the full-rank random matrix $Q(k \times k)$ on the finite field $F_p^{(k\times k)}$, the column vector $\mathfrak{q}_i = [\mathfrak{q}_{i1}, \cdots, \mathfrak{q}_{ik}]^T$ linearly independent, $rank(Q) = k$:

$$Q = (\mathfrak{q}_{ij})_{k\times k} = \begin{bmatrix} \mathfrak{q}_{11} & \cdots & \mathfrak{q}_{1k} \\ \vdots & \ddots & \vdots \\ \mathfrak{q}_{k1} & \cdots & \mathfrak{q}_{kk} \end{bmatrix} \tag{6}$$

where, $\mathfrak{q}_{ij}$ is a rankly interger on the finite field $F_{\mathbb{P}}^k$. Next, the product of the matrix A and the matrix Q is calculated to obtain the $m \times k$ coefficient matrix B:

$$B = (\mathfrak{b}_{ij})_{m\times k} = \begin{bmatrix} \mathfrak{b}_{11} & \cdots & \mathfrak{b}_{1k} \\ \vdots & \ddots & \vdots \\ \mathfrak{b}_{m1} & \cdots & \mathfrak{b}_{mk} \end{bmatrix} \tag{7}$$

where $\mathfrak{b}_{ij} = \sum_{i=1}^{m}(a_{iu} \times \mathfrak{q}_{uj})$. The $m(k-1)$-order polynomials $F_i(x)$, $i \in [1,m]$ are constructed by using the random matrix B as the polynomial coefficient matrix,

$$\begin{cases} F_1(x) = \mathfrak{b}_{11} + \mathfrak{b}_{12}x + \cdots + \mathfrak{b}_{1k}x^{k-1} \\ \cdots \\ F_m(x) = \mathfrak{b}_{m1} + \mathfrak{b}_{m2}x + \cdots + \mathfrak{b}_{mk}x^{k-1} \end{cases} \tag{8}$$

Let $F_i^{(t)}(x)$ denote the t-order derivations $(k-1)$-order of polynomial $F_i(x)$. Namely, $F_i^{(t)}(x) = \frac{d^{(t)}F_i(x)}{d^{(t)}(x)}$. The t-order of all m polynomial groups is abbreviated as $F^{(t)}(x) = [F_1^{(t)}(x), F_2^{(t)}(x), \cdots, F_m^{(t)}(x)]$. Then the shadow secret of the secret matrix $\mathbb{S}_A$ is determined by the multi-order derivation of the $(k-1)$-order polynomial.

The corresponding derivative order for each participant is the same as the number of thresholds corresponding to the previous level of the participant p_i. For example, the first-level participant has a derivative order of 0 order and the second-level participant's order is t_0.

Table 1: Hierarchical threshold correspondence

Level	Participant	Threshold
0	$\{p_{l0_1}, \cdots, p_{l0_N0}\}$	t_0
1	$\{p_{l1_1}, \cdots, p_{l1_N1}\}$	t_1
$\cdots$	$\cdots$	$\cdots$
1	$\{p_{ll_1}, \cdots, p_{ll_N1}\}$	t_l

For any participant p_i, we obtain the $F^{(t_{w-1})}(x)$ of the polynomial derived order of the corresponding threshold t_{w-1} as the participant. Participants to the unique identification information is substituted into the item $p_i.ID \in F_{\mathbb{p}}$ solved in polynomial t_{w-1} on the basis of the first derivative of the distribution data vector participant secret $SS_{\mathfrak{p}_i}$.

$y_j = F_j^{(t_{w-1})}(p_i.ID)$ is the value of the t_{w-1} order derivative function of the polynomial $F_j(x)$ after the first entry $p_i.ID$. Converts each y_j value in the SS_{p_i} into a binary representation and calculates the length of all the binary strings, whichever is the longer value, to obtain the alignment length AlignLen

$$Len_{\mathfrak{p}_i} = \max_{j\in[1,m]} (y_i)^{base2}_{length} \tag{9}$$

$$AlignLen = \max_{x\in[1,m]} Len_{p_i} + \varepsilon \tag{10}$$

Where ε is a random small positive integer, all y_j binary strings are preceded by AlignLen, and the binary secret data string of participant p_i is obtained,

$$y_i^{base2} = [e_{j1}, e_{j2}, \cdots, e_{j,AlignLen}] \tag{11}$$

After all the y_j in $SS_{\mathfrak{p}_i}$ are binarized, the shadow secret distribution matrix for the participant p_i is obtained: $(e_{ij})_{m\times AlignLen}$.

$$EmbSS_{\mathfrak{p}_i} = \begin{bmatrix} e_{11} & \cdots & e_{1,AlignLen} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{m,AlignLen} \end{bmatrix} \tag{12}$$

The Dealer reserves AlignLen as the alignment key for the recovery process. Finally, The cover image CI is an image of $(U\times V)$ size, that is,

$$CI = (c_{ij})_{U\times V} = \begin{bmatrix} c_{11} & \cdots & c_{1,V} \\ \vdots & \ddots & \vdots \\ c_{U1} & \cdots & c_{UV} \end{bmatrix} \tag{13}$$

c_ij is a binary pixel value. According to the LSB minimum bit (the lowest 2 bits), the shadow of the participant p_i is embedded in the load image. The size of the load image should be satisfied $(U\times V > \frac{m\times AlignLen}{2})$ conditions. After the formation of the write load image $CI_{\mathfrak{p}_i}$. The Dealer distributes the image $CI_{\mathfrak{p}_i}$ to the corresponding participant p_i. Follow this process to complete the generation and distribution of binary secret strings for all participants.

4 Proposed Secret Reconstruction Model

From the $l+1$ layer participants in accordance with the $< t_w, N_w >$ threshold program selected by t_w participants, the highest threshold for the value of $k = t_l$. The selected $\mathbb{K} = \sum_{w\in[0,l]} t_w$ participants are labeled $\{p_{selected_i}\}_1^{\mathbb{K}}$. According to the AlignLen value, $EmbSS_{p_{selected_i}}$ is obtained from the load image of the selected participant $p_{selected_i}$ by obtaining the lower 2 bits of the pixel binary value and converted into a real number expression :

$$SS_{p_{selected_i}} = [\mathfrak{y}_1, \mathfrak{y}_2, \cdots, \mathfrak{y}_m] \tag{14}$$

$p_{selected_i}$of the shadow provided by the participant is the t_{x-1} order derivative of the m polynomial group according to the threshold value t_x corresponding to the level of the participant $p_{selected_i}.ID$ The result of the participant number $p_{selected_i}.ID$, ie:

$$SS_{p_{selected_i}} = \mathbb{F}^{t_{x-1}}(p_i.ID) = [\mathfrak{y}_1, \mathfrak{y}_2, \cdots, \mathfrak{y}_m] \tag{15}$$

The pair of $(p_{selected_i}.ID, [\mathfrak{y}_1, \mathfrak{y}_2, \cdots, \mathfrak{y}_m])$ as the input, Reconstructing the polynomial group $\{f_i(x)\}_1^m$ by using the Berkshire interpolation formula $f_i(x) = \gamma_{i1} + \gamma_{i2}x + \cdots + \gamma_{ik}x^{k-1}, i \in [1,m]$. In this process, the covariance matrix of the polynomial group $\{f_i(x)\}_1^m$ is determined by using the Birkhoff interpolation formula for the matching of the shadow secret of all participants.

$$\mathfrak{R} = (\gamma_{ij})_{m\times k} = \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1k} \\ \vdots & \ddots & \vdots \\ \gamma_{m1} & \cdots & \gamma_{mk} \end{bmatrix} \tag{16}$$

If all the secret information provided by all participants is correct, $\mathfrak{R}^T\mathfrak{R}$ is reversible and the projection matrix of $\mathfrak{R}$ is:

$$\mathbb{S}_{\mathfrak{R}} = \mathfrak{R}(\mathfrak{R}^T\mathfrak{R})^{-1}\mathfrak{R}^T = \begin{bmatrix} \mathfrak{r}_{11} & \cdots & \mathfrak{r}_{1k} \\ \vdots & \ddots & \vdots \\ \mathfrak{r}_{m1} & \cdots & \mathfrak{r}_{mk} \end{bmatrix} \tag{17}$$

The original image SI can be restored in conjunction with R_{SI} and the open matrix matrix R_{SI}, and $s_{ij} = \frac{Dealer.id}{1-r_{ij}}$. This paper defines the process as lemma 1 and makes the relevant proof.

Lemma-1: According to the projection matrix $\mathbb{S}_{\mathfrak{R}}$, the disclosed secret matrix R_{SI}, then the Dealer can rescover the original image SI, where:

$$s_{ij} = \frac{Dealer.id}{1-r_{ij}}$$

Proof:

(1)The floating-point matrix SI_{Float} of the original image is restored according to the element $r_{ij} = \mathfrak{s}_{ij} \oplus \mathfrak{s}_{ij}^{Float}$ of the open secret matrix $R_{SI} = (r_{ij})_(m \times m)$.

$$s_{ij}^{Float} = \mathfrak{s}_{ij} \oplus r_{ij} \tag{18}$$

(2)According to the properties of the Birkhoff interpolation theorem, the polynomial group is unique, and the projection matrix of the reconstructed polynomial coefficient matrix $\mathfrak{R}$ is equal to the projection matrix of the distributed coefficient matrix B:

$$\mathbb{S}_{\mathfrak{R}} = \mathfrak{R}(\mathfrak{R}^T\mathfrak{R})^{-1}\mathfrak{R}^T = B(B^TB)^{-1}B^T = \mathbb{S}_B \tag{19}$$

the projection matrix S_Bof matrix B and the projection matrix of A are given by the definition of random matrix A in the distribution process, and is A^TA reversible and $\mathfrak{q}_i = \mathfrak{q}_{i1}, \cdots, \mathfrak{q}_{ik}^T$, ie:

$$\mathbb{S}_B = B(B^TB)^{-1}B^T = A(A^TA)^{-1}A^T = \mathbb{S}_A \tag{20}$$

Therefore, the projection matrix of the matrix A is equal to the projection matrix of the matrix R, that is, $\mathbb{S}_A = (\mathfrak{s}_{ij})_{m\times m} = \mathbb{S}_{\mathfrak{R}}$, the corresponding elements are equal:

$$\mathfrak{s}_{ij} = \mathfrak{r}_{ij} \tag{21}$$

(3)According to the formula 18, 20:

$$s_{ij}^{Float} = \mathfrak{s}_{ij} \oplus r_{ij} = \mathfrak{r}_{ij} \oplus r_{ij} \tag{22}$$

(4)According to the image floating-point matrix SI_{Float} elements of the formula 3, there $s_{ij}^{Float} = \frac{s_{ij}}{Dealer.id+s_{ij}}$, therefore:

$$s_{ij} = \frac{Dealer.id}{1 - s_{ij}^{Float}} \tag{23}$$

Combining Equation 22, the element values of the original image are:

$$s_{ij} = \frac{Dealer.id}{1 - \mathfrak{r}_{ij} \oplus r_{ij}} \tag{24}$$

So to recover the original image SI, that is:

$$SI = (s_{ij})_{m \times m} = \begin{bmatrix} s_{11} & \cdots & s_{im} \\ \vdots & \ddots & \vdots \\ s_{m1} & \cdots & s_{mm} \end{bmatrix} \tag{25}$$

5 Conclusion

In this paper, we propose a new hierarchical secret image sharing scheme based on Birkhoff interpolation and projection matrix method. In the secret sharing process, we use all polynomial coefficients to share the secret information, using the projection matrix method to avoid the polynomial coefficient leakage cited part of its secret is stolen. The proposed scheme makes full use of the complete random coefficient matrix of polynomials, strengthens the defensive of information leakage. Our scheme has the ability of defensive false data attack, recognizing the secret of the attacker's tamper information, defensing collusion attack, The common model tries to maliciously restore the original secret behavior with defensive capabilities and has a good shadow image quality with information hiding capacity.

References

[1] G. R. Blakley et al. Safeguarding cryptographic keys. In *Proc. of the 1979 International Workshop on Managing Requirements Knowledge (AFIPS'79), New York, New York, USA*, volume 48, pages 313–317. IEEE, June 1979.

[2] C.-C. Chen and S.-C. Chen. Two-layered structure for optimally essential secret image sharing scheme. *Journal of Visual Communication and Image Representation*, 38:595–601, July 2016.

[3] C. C. Drăgan and F. L. Ţiplea. Distributive weighted threshold secret sharing schemes. *Information sciences*, 339:85–97, April 2016.

[4] Z. Eslami, N. Pakniat, and M. Noroozi. Hierarchical threshold multi-secret sharing scheme based on birkhoff interpolation and cellular automata. In *Proc. of the 18th CSI International Symposium on Computer Architecture and Digital Systems (CADS'15),Tehran, Iran*, pages 1–6. IEEE, October 2015.

[5] C. Guo, C.-C. Chang, and C. Qin. A hierarchical threshold secret image sharing. *Pattern Recognition Letters*, 33(1):83–91, January 2012.

[6] P. Li, C.-N. Yang, C.-C. Wu, Q. Kong, and Y. Ma. Essential secret image sharing scheme with different importance of shadows. *Journal of Visual Communication and Image Representation*, 24(7):1106–1114, October 2013.

[7] P. Li, C.-N. Yang, and Z. Zhou. Essential secret image sharing scheme with the same size of shadows. *Digital Signal Processing*, 50:51–60, March 2016.

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

[9] Z. Tan, G. Yang, W. Cheng, and X. Wang. Distributed secret sharing scheme based on personalized spherical coordinates space. *Computer Science and Information Systems*, 10(3):1269–1291, June 2013.

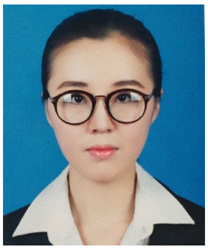
[10] T. Tassa. Hierarchical threshold secret sharing. *Journal of cryptology*, 20(2):237–264, April 2007.

[11] C.-N. Yang, P. Li, C.-C. Wu, and S.-R. Cai. Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach. *Signal Processing: Image Communication*, 31:1–9, February 2015.

Author Biography

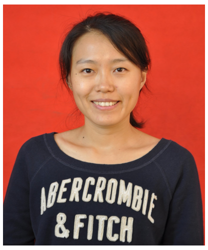
Zhenhua Tan rwas born in Hu Nan, China in 1980. He received the B.S., M.S., and Ph.D. degrees from Northeastern University, Shenyang, China, in 2003, 2006, and 2009, respectively, all in computer science. He is currently a Professor with the College of Software, Northeastern University, and became a professional Member (M) of IEEE in 2017. He holds three U.S. patents about networking and security. He has published over 30 journal articles, book chapters, and refereed conference papers. His current research interests include networking behaviors analysis and information security.

Danke Wu received the B.E. degree from Shengyang Normal University, Shengyang, China, in 2016. She is currently pursuing the M.S. degree with the Software College of Northeastern University, China. Her research interests include inforamtion diffusion and influence minimization.



Hong Li received the M.E. degree from Northeastern University, Shenyang in 2018, and B.E. degree from China University of Mining and Technology, Jiangsu, China, in 2015. Her research interests include distributed secret sharing and multi-level secret sharing.

Tianhan Gao received the B.E. in Computer Science Technology, the M.E. and the Ph.D in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained a promotion to a professor in June 2017. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He obtained the doctoral tutor qualification in 2016. He is the author or co-author of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, as well as virtual reality.(VRSJ).



Guo Nan received the B.E. in Computer Science Technology, the M.E. and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2005, respectively. She joined Northeastern University in September 2005. She has been an associate professor since 2008. She has been a visiting scholar at department of Computer Science, Purdue, from August 2010 to August 2011. Her research interests are security and privacy in social network and digital identity management. (IEICE).