A NEW GENERALIZED GROUP-ORIENTED CRYPTOSYSTEM BASED ON THE SYSTEMATIC BLOCK CODES

Hung-Yu Chien

Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan, R.O.C.

Jinn-Ke Jan

Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan, R.O.C.

Yuh-Min Tseng

Department of Information Management, NanKai College of Technology and Commerce, NanTou, Taiwan, R.O.C.

ABSTRACT

Secret Sharing has been well-studied over the past decade. From the view point of sharing policy, these schemes can be classified into two types: the threshold-based scheme and the generalized group-oriented cryptosystem. Based on the systematic block code, we had designed an efficient general threshold-based scheme[23]. In this article, based on the result of previous work, we further extend our result to the cases of the generalized group-oriented cryptosystem. This scheme has several merits: (1) It allows parallel secret reconstruction. (2) The SD can dynamically decides the number of distributed secrets depending on the requirement. (3) The construction of the generator matrix is simple and efficient. (4) Users secret shares will not be disclosed after multiple-secret reconstruction operations. (5) The computation is efficient and the quantity of public values in our scheme is low.

1. INTRODUCTION

Since 1979, Shamir [2] and Blakley [3] independently proposed the (t,n) threshold secret sharing scheme, the threshold-based schemes are among the most important issues in cryptography and have been well studied [1-7, 15-23, 33]. In a (t,n) threshold secret sharing scheme, the secret can be reconstructed using the co-operation of t or more members, while the secret cannot be reconstructed if only $t-1$ or fewer members are willing to co-operate [1].

In 1994, He and Dawson [4] proposed a multistage secret sharing scheme in which multiple secrets could be shared among n participants using the (t,n) threshold rule in a one-pass interaction. In 1995, Harn improved the He-Dawson scheme by reducing the number of public values [5]. Later, He and Dawson revised their scheme to achieve parallel secret reconstruction [6]. However, $p \cdot n + p$ public values are still required in their revised scheme. In 1995, Harn proposed a new threshold secret sharing concept [7]. In this concept, there are many secrets to be shared among n users and the security requirement of each secret is different.

Regarding to the multi-secret sharing schemes, Jackson et al. had their classification [35]. In their classification, multi-secret sharing schemes can be classified into two types: the one-time-use scheme and the multiple-use scheme. In a one-time-use scheme, the Secret Holder (SD) must redistribute fresh shares to each participant once some particular secrets have been reconstructed. On the other hand, in a multiple-use scheme, the shares owned by one participant still remain secret to others even after multiple secret reconstruction operations have been performed. The SD, therefore, does not need to redistribute fresh shares. To redistribute shares is a very costly process with respect to

both time and resources.

Based on the linear block code, Bertilsson and Ingemar proposed their secret sharing schemes [36]. However, the construction of the generator matrix is complicated and inefficient. Also based on the systematic block codes [9-10], Karnin et al. proposed their secret sharing schemes [37]. Given the secret size and the threshold value, the bound on the maximun values of trustees is discussed [37]. However, Karnin et al.' s scheme is one-time use only. That is, the SD must redistribute fresh shares to participants to initiate a new secret sharing process after a secret reconstruction process.

In 1999, based on the $G(2(p+w)-t, p+w)$ systematic block code, we proposed an efficient general threshold-based secret sharing scheme [23]. This general threshold-based scheme has several characteristics: (1) the secret sharing policy follows the threshold rule, (2) it allows multiple secrets to be distributed simultaneously, (3) the threshold value corresponding to different secret could be distinct, (4) each participant could be assigned a distinct weight value, (5) the weight value of each participant could be adjusted dynamically.

On the other hand, there are many secret sharing applications-for instance the generalized group-oriented cryptosystem ($GGOC$) [24-29, 31-32], in which some of the sharing policies can not be expressed in a threshold-based style [27]. In $GGOC$, the sharing policy is describsed by dividing the group of users into the qualified sets or the unqualified subsets. Only through the co-operation of members of one set of the qualified subsets can a secret be reconstructed. In $GGOC$, the qualified subsets of users can be determined using an *access structure* Γ_0 that consists of those *minimal authorized subgroups*. This *access structure* Γ_0 is usually denoted in disjunctive normal form (DNF). For example, $\Gamma_0 = User_1User_2 + User_3User_4$, where $User_1User_2$ and $User_3User_4$ are the *minimal authorized subgroups*. This means that those groups which consist of at least $User_1$ and $User_2$ are all qualified subsets. So are those groups consisting of at least $User_3$ and $User_4$.

For various Secret Sharing problems(the threshold-based problems or the general group-oriented cryptosystems), there have been different approaches proposed in the previous works. However, based on the same approach in our previous work [23], we will propose a new scheme to the generalized group-oriented cryptosystem. This new scheme also has several merits as our previous work: (1) It allows parallel secret reconstruction. (2) The SD can dynamically decides the number of distributed secrets depending on the requirement. (3) The construction of the generator matrix is simple and efficient. (4) Users' secret shares will not be disclosed after multiple-secret reconstruction operations. (5) The computation is efficient and the quantity of public values in our scheme is low.

This article is organized as follows. In the next section, we briefly review the systematic block codes. In Section 3, we introduce our new scheme to the $GGOC$ problem. In Section 4, the computation and communication overhead is given. Finally, Section 5 presents our conclusions.

2. INTRODUCTION OF THE SYSTEMATIC BLOCK CODES

In this section, we briefly review the systematic block codes, and then the technique based on the systematic block codes is described. A (N, K) (with $N > K$) linear block code over $GF(2^m)$ is defined by a NxK generator matrix G with symbols in $GF(2^m)$ and $K < 2^m$. In this paper, we denote the generator matrix as $G(N, K)$, where N is the length and K is the dimension of the linear block codes. Denote $D = (d_1, d_2, .., d_K)^t$ as a vector of K *information symbols* where $d_i s$ are in $GF(2^m)$ and the superscript t means vector transpose. Then $V = GD = (v_1, v_2, ..., v_n)$ is the corresponding *code*

word with $v_i s$ in $GF(2^m)$.

A systematic block code is a special type of linear block code where the first K elements in a code word are identical to the information symbols $(d_1, d_2, .., d_K)$, and the last $N-K$ elements in the code word are denoted as $(c_1, c_2, .., c_{N-K})$ and called *parity symbols*. In 1990, Ayanoglu et al. [9] designed a special type of systematic block code generator matrix $G(N,K) = \begin{bmatrix} I \\ P \end{bmatrix}$, where I is the KxK identity matrix, and P is a $(N-K)xK$ matrix $\left[g^{(i-1)(j-1)}\right]$ with g being a primitive element in $GF(2^m)$ and $K < 2^m$. **I** and **P** can be represented as follows:

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ : & : & : & : \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{P} = \begin{bmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & g & g^2 & ... & g^{K-1} \\ 1 & g^2 & g^4 & ... & g^{2(K-1)} \\ : & : & : & : & : \\ 1 & g^{N-K-1} & g^{(N-K-1)2} & ... & g^{(N-K-1)(K-1)} \end{bmatrix}$$

Since **V**=**GD**, then we have

$$c_i = \sum_{j=1}^{K} g^{(i-1)(j-1)} d_j, \quad \text{where} \quad 1 \le i \le N-K \tag{1}$$

In our schemes, we require that $K < 2^m$ to satisfy the non-singular requirement of matrix P [9]. The $(N-K)$ equations in (1) can, therefore, be viewed as linear-independent equations of indeterminants $(d_1, d_2, .., d_K)$. If these $(N-K)$ equations were presented with $(N-K) < K$, then we would not be able to uniquely determine the values for these $(d_1, d_2, .., d_K)$. However, the remaining symbols can be recovered if some of these symbols $d_j s$ are available such that the number of those missing symbols are smaller or equal to the number of equations. Based on this technique and hash function, we had proposed the general threshold-based secret sharing scheme [23]. In the next section, we extend our result to the general group-oriented cryptosystem.

3. THE NEW GENERAL GROUP-ORIENTED CRYPTOSYSTEM USING THE $G(2(q+p)-1, q+p)$ SYSTEMATIC CODE

Before introducing our new scheme for the general group-oriented cryptosystem, we first assumed that there exists a two-variable one-way function $f(r,s)$ [6] that maps a secret key s and a value r to a bit string $f(r,s)$ of fixed length. One nontrivial property of this two-variable function is its one-way property. Given $f(r_1,s)$, $f(r_2,s)$, ..., $f(r_k,s)$, and $r_{(1 \le i \le k)i}$, it is hard to calculate any $f(r,s)$ for some $r \ne r_i, 1 \le i \le k$. The formal definition and the proof of existence of such a function were given by He and Dawson [6]. They also gave some examples of the construction of such a hash function. One of them is quoted as follows. Let S be a secure signature scheme. For a message m, the signature with secure key k is denoted by $S(k,m)$. Let h be a universal one-way hash function whose existence is based on any one-to-one, one way function [38]. Let $F(x,y) = h(S(x,y))$. Then F is a two-variable one-way function.

Next comes the description of our scheme. Our scheme consists of three phases: the shadow distribution phase, the secret broadcast phase, and the secret recovery phase. In the following description, we assumed that there were p secrets to be distributed simultaneously among n users,

and the qualified subsets are specified by the access structure $\Gamma_0 = f_1 + f_2 + \ldots + f_q$, where $f_i s$ are *minimal qualified subsets*. The **shadow generation phase**, the **secret broadcasting phase** and the **secret recovering phase** are described as follows.

The Shadow Distribution Phase: Before SD distributes secrets to users, he first randomly select n secret shares $(s_1, s_2, \ldots, s_n)$ and then delivers s_i to $User_i$ over a secret channel. This procedure is executed only once in our scheme.

The Secret Broadcasting Phase:

To distribute these p secrets with the access structure $\Gamma_0 = f_1 + f_2 + \ldots + f_q$, the SD executes the following steps.

Step 1. Randomly select q integers $(r_1, r_2, \ldots, r_q)$ corresponding to the q *minimal qualified subsets* in Γ_0.

Step 2. Prepare the information vector D as follows. The length of this vector is $p+q$, where q is the number of *minimal qualified subsets* in Γ_0.

$$D = (P_1, P_2, ..., P_p, F_1, F_2, \ldots, F_q)$$

, where $F_i = \prod_{User_j \in f_i} f(r_i, s_j)$, $1 \le i \le q$.

Please notice that the multiplication operation is in $GF(2^m)$.

Step 3. Prepare the generator matrix $G(2(p+q)-1, p+q)$. Please notice that the generator matrix G can be pre-computed, and a generator matrix with a larger dimension can be easily constructed by the extension of a generator matrix with a smaller dimension.

Step 4. Compute $V = GD$. Then we have

$$V = (P_1, P_2, ..., P_p, F_1, F_2, \ldots, F_q, c_1, c_2, ..., c_{p+q-1})$$

, where c_j can be represented as follows.

$$c_i = \sum_{j=1}^{p} g^{(i-1)(j-1)} P_j + \sum_{j=p+1}^{p+q} g^{(i-1)(j-1)} F_{j-p}, \quad 1 \le i \le q + p - 1 \qquad (2)$$

Step 5. Publish $(\Gamma^0, r_1, r_2, \ldots, r_q, c_1, c_2, \ldots, c_{p+q-1})$ in an authenticated manner. For example, adding the Message Authentication Checks (MAC) [11]

The Secret Reconstruction Phase:

When those users corresponding to some *minimal qualified subsets* f_j $(1 \le j \le q)$ in Γ_0 are willing to recover the secrets $(P_1, P_2, ..., P_p)$, then they execute the following steps.

Step 1. For each $User_i \in f_j$, he computes $f(r_j, s_i)$ and contributes this value to his group. After all members of this group f_j have contributed their values, then the group computes $F_j = \prod_{User_i \in f_j} f(r_j, s_i)$.

Step 2. Now the number of missing symbols in Equations (2) is $p+q-1$ which is equal to the numbers of Equations in (2)- $p+q-1$. So, the missing symbols F_k, ($1 \le k \le q$ *and* $k \ne j$) and secrets $(P_1, P_2, ..., P_p)$ can be uniquely determined from Equations (2). Our proposed

scheme satisfies the requirement of the access structure Γ_0.

4. SECURITY AND OVERHEAD ANALYSIS

We first analyze the security of our scheme from the following different points.

1. Given the public values in each scheme, we can see that the number of unknown symbols is larger than the numbers of Equations in (2). So, an adversary has no way to derive the secrets.
2. Now we consider the case when users want to co-operate to acquire the secrets. The number of unknown symbols in Equations (2) is $p+q$, while the number of linear-independent equations in (2) is $p+q-1$. Therefore, users must acquire at least one value for those unknown symbols to derive the secrets. However, only through the co-operation of users corresponding to the minimal qualified subsets f_j ($1 \le j \le q$) can the value of the unknown symbol F_j be acquired. Our scheme therefore realizes the access structure Γ_0.
3. Our schemes will not disclose a user's secret shadow even after multiple secret reconstruction operations have been performed. Even though the pseudo shadows $f(r, s_i)$ will be exposed among the co-operating members, the actual secret shadow s_i is well protected by the two variable one-way function $f(r, s_i)$ where r is randomly selected every time.

So, our scheme is a secure realization of the access structure Γ_0. Next, we analyze the computation and the communication overhead of our scheme. To distribute multiple secrets among n users in different schemes, the SD will compute the pseudo shadows $f(r, s_i)$s and the parity symbols $c_i s$. Since the generator matrix can be pre-computed, the operations involved in the calculation of c_i are just hashing, addition and multiplication in $GF(2^m)$. On the other side of recovering the secrets, the co-operating users also compute their pseudo shadows $f(r, s_i)$ s, and then solve the corresponding linear equations in (2).

Now we consider the number of public values in the different schemes in the following. The public values are $(\Gamma^0, r_1, r_2, \ldots, r_q, c_1, c_2, \ldots, c_{p+q-1})$. The number of public values excluding Γ_0 is $p+2q-1$, while that of its counterpart [29] is $q+q \cdot p$. From the above analysis, we can see that our scheme is efficient.

Finally, we present some discussion on the cheating detection issue. It is important for any group-oriented secret sharing schemes to detect cheating and identify the cheater. There are already numerous works on this issue [13, 20, 21, 30]. Therefore, we will not reiterate on this issue in our paper. But in order to maintain users' shadows secret during the cheater identification process, there are some points that should be examined: the SD should use $f(r, s_i)$ instead of s_i in generating the public values for the cheater identification. Hence, $User_i$ just polls his pseudo shadows $f(r, s_i)$ in the cheater identification process, so that the secret share s_i will not be disclosed.

5. CONCLUSIONS

In this article, based on the systematic block codes, we have proposed a new scheme to the general group-oriented cryptosystem. As in our previous work, this new scheme to the general group-oriented cryptosystem also has several merits: (1) It allows parallel secret reconstruction. (2) The SD can dynamically decides the number of distributed secrets depending on the requirement. (3) The construction of the generator matrix is simple and efficient. (4) Users'

secret shares will not be disclosed after multiple-secret reconstruction operations. (5) The computation is efficient and the quantity of public values in our scheme is low.

6. REFERENCES

[1] D.E.R. Denning, *Cryptography and Data Security*, Addition-Wesley, 1982.

[2] A. Shamir, "How to Share a Secret," *Comm. ACM*, 22(11), pp. 612-613, 1979.

[3] G.R. Blakley, "Safeguarding Cryptographic Keys," *AFIPS 1979 Natl. Comput. Conf.*, New York, Vol. 48. pp. 313-317, 1979.

[4] J. He, and E. Dawson, "Multistage Secret Sharing Based on One-Way Function," *Electron. Lett.*, 30(19), pp. 1591-1592, 1994.

[5] L. Harn, "Comment: Multistage Secret Sharing Based on One-Way Function," *Electron. Lett.*, 31(4), pp. 262, 1995.

[6] J. He, and E. Dawson, "Multi-Secret Sharing Scheme Based on One-Way Function," *Electron. Lett.*, 31(2), pp. 93-94, 1995.

[7] L. Harn, "Efficient Sharing (Broadcasting) of Multiple Secrets," *IEE Proc.-Comput. Digit. Tech.*, Vol. 142, No. 3, pp. 237-240, May 1995.

[8] "The Digital Signature Standard Proposed by NIST," *Comm. ACM*, 35(7), pp. 36-40, 1992.

[9] E. Ayanoglu, C-L I, R.D. Citlin, and J.E. Mazo, "Diversity Coding: Using Error Control for Self-Healing in Communication Networks," *Proc. of IEEE Inform'90*, San Francisco, CA, pp. 95-104, June 5-7 1990.

[10] S. Lin, and D.J. Costello, *Jr. Error Control Coding: Fundamentals and Applications*, Prentice-Hall, Englewood Cliffs, NJ, 1983

[11] R.H. Deng, L. Gong, A.A. Lazar, and W. Guo, "Authenticated Key Distribution and Secure Broadcast Using No Conventional Encryption: A Unified Approach Based on Block Codes," *IEEE GLOBECOM'95*, pp. 1193-1197, 1995.

[12] T. Elgamal, "A Public-Key Cryptosystem and A Signature Scheme Based on Discrete Logarithm," *IEEE Trans. Inform. Theory*, 31, pp. 469-472, July 1985.

[13] K. J. Tan,, H-W. Zhu,, and S.J. Gu, "Cheater Identification in (t,n) Threshold Scheme," *Computer Communications*, 22 , pp. 762-765, 1999.

[14] L. Lamport, "Password Authentication with Insecure Communication", *Comm. ACM*, 24(11), pp. 770-772, 1981.

[15] P. Morillo, C. Padro, G. Saez, and J.L. Villar, "Weighted threshold secret sharing schemes," *Information Processing Letters 70*, pp. 211-216, 1999.

[16] D.R. Stinson, and R. Wei, "An application of ramp schemes to broadcast encryption," *Information Processing Letters 69*, pp. 131-135, 1999.

[17] H.M. Sun, and S.P. Shieh, "Secret Sharing in Graph-Based Prohibited Structures," IEEE , pp. 718-724, 1997.

[18] C. S. Laih, L. Harn, J.Y. Lee, and T.L. Hwang, "Dynamic Threshold Scheme Based on the Definition of Cross-Product in an N-dimensional Linear Space," Eurocrypt'95, pp. 286-297, 1995.

[19] T. C. Wu, and W.H. He, "A Geometric Approach for Sharing Secrets," *Computers & Security 14*, pp. 135-145, 1995.

[20] T.C. Wu, and T.S. Wu, "Cheating Detection and Cheater Identification in Secret Sharing Schemes," *IEE Proc. Comput. Digit. Tech.*, Vol 142, pp. 367-369, 1995.

[21] C.C. Chang, R.J. Hwang, "Efficient Cheater Identification Method for Threshold Schemes," *IEE Proc. Comput. Digit. Tech.*, Vol 144, No. 1, pp. 23-27, 1996.

[22] H.-M. Sung, and S.-P. Shieh, "On Dynamic Threshold Schemes," *Information Processing Letters*, pp. 201-206, 1994.

[23] H.-Y. Chien, J.K. Jan, Y.M. Tseng, "On the Generalized Threshold-Based Secret Sharing Schemes," Proceeding of *10th National Security Conference*, HwaLan, pp. 285-290, 2000.

[24] R. G. E. Pinch, "Online Multiple Secret Sharing," *Electronics Letters*, Vol. 32, No. 12, pp. 1087-1088, 1996.

[25] H.Y. Lin, and L. Harn, "A Generalized Secret Sharing Scheme with Cheater Detection," *AsiaCrypt'91*, pp. 83-87, 1991.

[26] C.S. Laih, and L. Harn, "Generalized Threshold

Cryptosystems, *AsiaCrypt' 91*, pp. 88-92, 1991.

[27] J. Benaloh, and J. Leichter, "Generalized Secret Sharing and Monotone Functions," *EuroCrypt' 90*, pp. 27-35, 1990.

[28] J.J. Tsai, T. Hwang, C.H. Wang, "New Generalized Group-Oriented Cryptosystem based on Diffie-Hellman Scheme," *Computer Communications 22*, pp. 727-729, 1999.

[29] H. M. Sung, "On-line Multiple Secret Sharing Based on A One-way Function," *Computer Communications 22*, pp. *745-748, 1999*.

[30] R. J. Hwang, W.B. Lee, and C.C. Chang, "A Concept of Designing Cheater Identification Methods for Secret Sharing," *The journal of Systems and Software 46*, pp. 7-11, 1999.

[31] C.C. Chang, and H.C. Lee, "A New Generalized Group-Oriented Cryptoscheme without Trusted Center," *IEEE J. on Selected Areas in Communications*, Vol. 11, No. 5, pp. 725-729, 1993.

[32] K.J. Tan, H.W. Zhu, "General Secret Sharing Schemes," *Computer Communications 22, pp.*755-757, 1999.

[33] S.J. Hwang, C.C. Chang, and W.P. Yang, "An Efficient Dynamic Threshold Scheme," *IEICE Trans. INF. & SYST.*, Vol. E79-D, No. 7, pp. 936-941, 1996.

[34] L. Gong, "New Protocols for Third-Party-Based Authentication and Secure Broadcast," *Proceedings of 2nd ACM Conference on Computer and Communications Security*, pp. 176-183, November 1994, Fairfax, Virginia.

[35] W.-A. Jackson, K. M. Martin, and C. M. O' Keefe, "On Sharing Many Secrets," *Asiacrypt' 94*, pp. 42-54, 1994.

[36] M. Bertilsson, and I. Ingemarsson, "A Construction of Practical Secret Sharing Schemes Using Linear Block Codes," *Auscrypt' 92*, pp. 2-21, 1992.

[37] Karnin, J. W. Greene, and M. E. Hellman, "On Secret Sharing Systems," *IEEE Trans. Inform. Theory*, IT-29, pp. 35-41, January 1983.

[38] M. Naor, and M. Yung, "Universal One-Way Hash Functions and Their Cryptographic Applications," *Proc. 21st Annual Symo. Theory of Computing*, pp. 33-43, 1989.