Chinese Journal of Electronics
Vol.25, No.1, Jan. 2016

A (t, m, n)-Group Oriented Secret Sharing Scheme*

MIAO Fuyou, FAN Yuanyuan, WANG Xingfu, XIONG Yan and Moaman Badawy

(*School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China*)

Abstract — Basic (t, n)-Secret sharing (SS) schemes share a secret among n shareholders by allocating each a share. The secret can be reconstructed only if at least t shares are available. An adversary without a valid share may obtain the secret when more than t shareholders participate in the secret reconstruction. To address this problem, the paper introduces the notion and gives the formal definition of (t, m, n)-Group oriented secret sharing (GOSS); and proposes a (t, m, n)-GOSS scheme based on Chinese remainder theorem. Without any share verification or user authentication, the scheme uses Randomized components (RC) to bind all participants into a tightly coupled group, and ensures that the secret can be recovered only if all m ($m \geq t$) participants in the group have valid shares and release valid RCs honestly. Analysis shows that the proposed scheme can guarantee the security of the secret even though up to $m-1$ RCs or $t-1$ shares are available for adversaries. Our scheme does not depend on any assumption of hard problems or one way functions.

Key words — Threshold secret sharing, Group oriented, Randomized components, Share protection, Chinese remainder theorem.

I. Introduction

(t, n)-Secret sharing (SS) schemes were introduced by Shamir[1] and Blakley[2] independently in 1979 for protecting cryptographic keys, and now it has become a fundamental building block in many cryptographic protocols, such as threshold signature schemes, threshold encryption schemes and secure multiparty computation. In a (t, n)-secret sharing scheme, n shares are derived from a secret s by the dealer, and are distributed among n shareholders in such a way that at least t shares are required to reconstruct the secret while less than t shares are unqualified to do that. In a SS scheme, a shareholder is referred to as the member who holds a valid share; when some shareholders participate in a secret reconstruction, they are called participants.

As the most popular SS, Shamir's[1] (t, n)-SS is constructed based on a polynomial over finite field. Blakley's (t, n)-SS scheme[2] is based on hyperplane intersections and Massey's scheme[3] uses linear code to share a secret among a group of shareholders. Both Mignotte's (t, n)-SS scheme[4] and Asmuth-Bloom's (t, n)-SS scheme[5] are based on Chinese remainder theorem (CRT), which use a series of moduli in an increasing sequence and define schemes based on a specified threshold range of integers. The range is upper-bounded by the product of t smallest moduli and lower bounded by the product of $t-1$ largest moduli. Given $t-1$ shares, Mignotte's scheme leaks more information about the secret than Asmuth-Bloom's scheme, but the latter limits the secret in a smaller range when both schemes have the same threshold range.

Actually, these above basic (t, n)-SSs are far from practical. Let us consider the scenario, there are $t+1$ participants in a (t, n)-threshold secret reconstruction, and one of these participants is an adversary who does not possess any valid share. But the adversary can still restore the secret by collecting enough shares from other t participants. We call the attack Malicious participant attack. An obvious solution to the problem is user authentication[6], which guarantees only valid shareholders are allowed to participate in the secret reconstruction. However, this method makes the scheme much more complicated because each participant needs to be authenticated by another one, which means $t(t-1)$ user authentications are needed among t participants. The second solution is Verifiable secret sharing (VSS)[7]. VSS enables shareholders to prove that their shares are valid without revealing them. Although VSS can be used to check the validity of each share; but it is very complicated and requires additional information and processing time.

Without using any user authentication or VSS, Harn[8]

*Manuscript Received Apr. 1, 2014; Accepted May. 20, 2014. This work is supported by the National Natural Science Foundation of China (No.61232018, No.61572454, No.61272472, No.61472382).
 DOI:10.1049/cje.2016.01.026

proposed a (t, n) secure secret reconstruction scheme based on the property of homomorphism[9] of polynomials to prevent the malicious participant attack, but it is inflexible.

The main contributions of the paper include 1) the notion of (t, m, n)-Group oriented secret sharing (GOSS) and 2) a flexible (t, m, n)-GOSS scheme based on CRT. Without using user authentication or share verification, the (t, m, n)-GOSS scheme employs Randomized components (RC) to ensure that the secret can be recovered only if all participants have valid shares and act honestly.

The rest of this paper is organized as follows. Harn's secure secret reconstruction scheme is presented in the next section. In section III, the definition of GOSS is given; Section IV details the proposed scheme. Security analysis of the proposed scheme is presented in Section V, properties and comparisons with related schemes are given in Section VI. Finally, Section VII concludes the paper.

II. Secure Secret Reconstruction

In 2013, Harn[8] proposed a (t, n)-secure secret reconstruction scheme, which ensures that the secret can only be recovered by participants who present valid shares. It consists of 2 steps as follows.

1. Share generation

The dealer D selects $k(kt > n-1)$ random polynomials, $f_l(x)$, $l = 1, 2, \ldots, k$, having degree $t-1$ each, and generates shares, $f_l(x_r)$, $l = 1, 2, \ldots, k$, for each shareholder, U_r. For any secret s, the dealer can always find integers, $w_l, d_l, l = 1, 2, \ldots, k$, in F_p, such that $s = \sum_{l=1}^{k} d_l f_l(w_l)$, where $w_i \neq w_j$ and $w_i \notin \{x_1, x_2, \ldots, x_n\}$, for every pair of (i, j), x_i is the public information of shareholder, U_i. The dealer makes these integers w_l, d_l, $l = 1, 2, \ldots, k$, publicly known.

2. Secret reconstruction

Each participant U_r uses his shares, $f_l(x_r)$, $l = 1, 2, \ldots, k$, to compute a Lagrange component, $c_r = \sum_{l=1}^{k} d_l f_l(x_r) \prod_{v=1, v\neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$, and release it to all other participants secretly. After knowing $c_r, r = 1, 2, \ldots, j$, each participant computes $s = \sum_{r=1}^{j} c_r \bmod p$.

The scheme requires $kt > n-1$ where n is the total number of shareholders in the scheme, t is the threshold and k is the number of polynomials needed.

III. Definition of (t, m, n)-GOSS

In order to cope with the malicious participant attack in a simpler and more efficient way, we will first put forward the notion of (t, m, n)-group oriented secret sharing and then give the security requirements and formal description.

Definition 1 (t, m, n)-GOSS A secret sharing scheme is called a (t, m, n)-GOSS if it satisfies the following requirements: 1) There are totally n shareholders in the scheme; 2) Given at least $t(t < n)$ shares, the secret can be recovered while it cannot be obtained with less than t shares; 3) If $m(n \geq m \geq t)$ shareholders form a tightly coupled group in a secret reconstruction, the secret can be jointly recovered only if all the m participants have valid shares and act honestly.

Formally, assume that in a basic (t, n)-SS scheme, $s \in Z_{p_0}$ is the secret, m out of n participants, $\mathcal{U}_{I_m} = \{U_{i_j} | i_j \in I_m\}$, with the corresponding share set $\mathcal{S}_{I_m} = \{s_{i_j} | i_j \in I_m\}$, form a tightly coupled group, where $I_m \subseteq I_n = \{1, 2, \ldots, n\}$, $|I_m| = m$. $f(.)$ is a component function in the share space and $\mathcal{C}_{I_m} = \{c_{i_j} = f(s_{i_j}, U_{I_m}) | i_j \in I_m\}$ is a component set generated from $\mathcal{S}_{I_m}$. A (t, n)-SS scheme is a (t, m, n)-GOSS scheme if

$$Pr(s|\mathcal{C}_J, \mathcal{C}_J \cap \mathcal{C}_{I_m} \neq \Phi) = \begin{cases} 1, & \text{if } \mathcal{C}_J = \mathcal{C}_{I_m} \\ & t \leq |\mathcal{C}_{I_m}| = m \leq n \\ \Rightarrow 1/p_0, & \text{otherwise} \end{cases}$$

where $\Rightarrow 1/p_0$ denotes $1/p_0$ or converging to $1/p_0$, $Pr(.)$ is a probability distribution function, $\mathcal{C}_J$ is the component set available in the secret reconstruction.

It implies that, to recover the secret, $\mathcal{C}_J$, the component set used in the secret reconstruction, must be identical with $\mathcal{C}_{I_m}$, the component set of the tightly coupled group as long as $\mathcal{C}_J$ includes at least one component in common with $\mathcal{C}_{I_m}$.

Remark 1 In the formal definition of (t, m, n)-GOSS, we use the probability, $\Rightarrow 1/p_0$, to denote that a group of participants fail to reconstruct the secret. In this case, we actually loosen the definition a little bit in an asymptotical way. If we strictly limit the probability to be $1/p_0$, the underlying (t, n)-SS scheme is required to be perfectly secure[10], and thus the definition can be called perfect (t, m, n)-GOSSs.

Remark 2 A (t, m, n)-group oriented secret sharing scheme is an enhanced (t, n)-secret sharing scheme. On one hand, it has the same threshold t as a (t, n)-threshold SS when the secret is recovered directly with shares; on the other hand, the scheme allows $m(n \geq m \geq t)$ participants to compose a tightly coupled group and thus the secret can be obtained only if all the participants are legal shareholders and act honestly.

IV. Proposed (t, m, n)-GOSS Scheme

1. Security model

There are a dealer, n shareholders and 2 types of ad-

versaries, outsider and insider, in the proposed scheme. As the coordinator, the dealer is supposed to be honest and trusted by all shareholders; there is a secure channel between any shareholder and the dealer, and each pair of shareholders shares a private channel. An outsider does not have any valid share or any private channels with participants, but may obtain some components by eavesdropping. Insiders, as participants, may conspire and try to get the secret.

2. Our scheme

The (t, m, n)-group oriented secret sharing scheme consists of 3 phases, 1) Share generation, 2) Randomized component construction and 3) Secret reconstruction.

1) Share generation

The dealer first picks an integer p_0 and a sequence of pairwise coprime positive integers, $p_1 < \ldots < p_n$ such that $p_0^2 \cdot p_{n-t+2} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_t$, $\frac{np_0^3}{p_0 - 1} < p_1$ and $gcd(p_0, p_i) = 1, i = 1, 2, \ldots, n$, where p_i is the public modulus associated with each shareholder U_i, n is the total number of shareholders and t is the threshold. And then it randomly selects the secret s in Z_{p_0} and an integer, α such that $s + \alpha p_0 \in Z_{\lceil (p_1 \cdot p_2 \cdot \ldots \cdot p_t)/p_0 \rceil}$. The share for each shareholder, *e.g.*, U_i, is generated as $s_i = (s + \alpha p_0) \bmod p_i, i = 1, 2, \ldots, n$. At last, s_i is sent to U_i secretly.

2) Randomized component construction

Suppose $I_m \subseteq I_n = \{1, 2, \ldots, n\}, |I_m| = m$ and a group of $m (m \geq t)$ participants, $\mathcal{U}_{I_m} = \{U_{i_1}, U_{i_2}, \ldots, U_{i_m}\}$, with the share set $\mathcal{S}_{I_m} = \{s_{i_1}, s_{i_2}, \ldots, s_{i_m}\}$ and public modulus set $\mathcal{P}_{I_m} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_m}\}$ accordingly, wants to recover the secret, each participant $U_{i_j} (U_{i_j} \in \mathcal{U}_{I_m})$ constructs a RC as

$$c_{i_j} = (s_{i_j}(N/p_{i_j})y_{i_j} + r_{i_j}(N/p_{i_j})p_0) \bmod N$$

where $(N/p_{i_j})y_{i_j} \bmod p_{i_j} = 1$, $N = \prod_{j=1}^{m} p_{i_j}$ and r_{i_j} is uniformly distributed over Z_{p_0}.

3) Secret reconstruction

Each participant, $U_{i_j} (U_{i_j} \in \mathcal{U}_{I_m})$, broadcasts the RC c_{i_j} within $\mathcal{U}_{I_m}$. After obtaining all RCs, U_{i_j} computes the secret as

$$s = \sum_{j=1}^{m} c_{i_j} \bmod N \bmod p_0$$

3. Correctness

The correctness of our scheme means the secret can be recovered by at least t participants, which is guaranteed by the following theorem.

Theorem 1 In our (t, m, n)-GOSS scheme, t or more than t participants are able to reconstruct the secret. That is, given $m (m \geq t)$ RCs, $\mathcal{RC}_{I_m} = \{c_{i_1}, c_{i_2}, \ldots, c_{i_m}\}$, the secret can be evaluated as $s = \sum_{j=1}^{m} c_{i_j} \bmod N \bmod p_0$, where $c_{i_j} = (s_{i_j} \frac{N}{p_{i_j}} y_{i_j} + r_{i_j} \frac{N}{p_{i_j}} p_0) \bmod N$.

Proof 1

$$\begin{aligned} &\sum_{j=1}^{m} c_{i_j} \bmod N \bmod p_0 \\ &= (s + \alpha p_0 + \sum_{j=1}^{m} r_{i_j}(N/p_{i_j})p_0) \bmod N \bmod p_0 \\ &= (s + \alpha p_0 + \sum_{j=1}^{m} r_{i_j}(N/p_{i_j})p_0) \bmod p_0 \\ &= s \end{aligned} \tag{1}$$

Note that the first line of Eq.(1) is equivalent to the third line due to$(s + \alpha p_0) < N/p_0$, $\sum_{j=1}^{m} r_{i_j}(N/p_{i_j})p_0 < mp_0^2(N/p_{i_j}) < (1 - 1/p_0)N$ (for $\frac{np_0^3}{p_0 - 1} < p_1$) and thus $(s + \alpha p_0 + \sum_{j=1}^{m} r_{i_j}(N/p_{i_j})p_0) \bmod N = (s + \alpha p_0 + \sum_{j=1}^{m} r_{i_j}(N/p_{i_j})p_0)$

V. Security Analysis

In (t, m, n)-GOSS scheme, RCs are used to protect shares because each RC binds the share with all participants' public information in a secret reconstruction. To obtain the secret, adversaries use either at least t shares or m RCs. We will first demonstrate that a share cannot be derived from a given RC by Theorem 2; In this case, an outsider, without any share, has to use RCs it intercepts to recover the secret, we use Theorem 3 to prove that an outsider, even with $m - 1$ RCs, is still unable to get the secret; However, insiders, each of which holds a valid share, may conspire and try to obtain the secret using their shares instead of RCs, Theorem 4 will assure us that up to $t - 1$ insiders are still unable to reconstruct the secret. Proofs of these theorems are available on the first author's homepage.

A RC must secure its share such that an adversary is unable to derive the share from the RC more easily than to guess the secret directly in the secret space Z_{p_0}, which, in turn, means it is infeasible to obtain the secret by deriving shares from RCs.

Theorem 2 In the proposed scheme, given a RC $c_i = (s_i(N/p_i)y_i + r_i(N/p_i)p_0) \bmod N$, the probability of deriving the share s_i is $1/p_0$, where r_i is uniformly distributed over Z_{p_0}.

Proof 2 (available on first author's homepage)

Theorem 2 implies that a RC makes the share and all participants' public information inseparable and actually prevents the share from being exposed. By RCs, all participants form a tightly coupled group. As a result, the secret can be recovered only if each participant has a valid RC (*i.e.*, share) and act honestly.

As an outsider, it has neither a valid share nor secure channels with participants, and thus can only get RCs by cracking private channels between each pair of participants. Theorem 3 shows that our scheme remains secure

even if an outsider obtain as many as $m-1$ RCs.

Theorem 3 In the proposed scheme, an outsider with at most $m-1$ RCs, is unable to recover the secret if there are $m(m \geq t)$ participants in the secret reconstruction. Formally, given $m-1$ RCs, $\mathcal{RC}_{I_{m-1}} = \{c_{i_1}, c_{i_2}, \ldots, c_{i_{m-1}}\}$, the probability for an outsider to derive the secret s, $Pr(s|\mathcal{RC}_{I_{m-1}})$, converges to $1/p_0$ for sufficiently large moduli.

Proof 3 (available on first author's homepage)

In addition to using RCs, insiders, as legal participants, may also try to directly use shares they hold to obtain the secret. Our proposed scheme is able to protect the secret even though $(t-1)$ insiders conspire.

Theorem 4 In the proposed scheme, $(t-1)$ insiders are unable to recover the secret. Formally, given $t-1$ shares, $\mathcal{S}_{I_{t-1}} = \{s_{i_1}, s_{i_2}, \ldots, s_{i_{t-1}}\}$, the probability for insiders to derive the secret s, $Pr(s|\mathcal{S}_{I_{t-1}})$, converges to $1/p_0$ for sufficiently large modulus.

Proof 4 (available on first author's homepage)

Remark 3 Theorem 4 ensures that, for $t-1$ insiders, deriving the secret is almost as difficult as guessing directly within the secret space even if they have up to $t-1$ shares, not to mention less shares.

Theorem 5 Our proposed scheme is a (t, m, n)-GOSS scheme.

From Theorems 2, 3 and 4, we are assured that the proposed scheme in Section IV is a (t, m, n)-GOSS scheme.

VI. Properties and Comparisons

RCs bring our scheme the following properties compared with related schemes.

1. Properties

1) Single share

In many VSS schemes, each participant needs to release 2 items in a secret reconstruction, one is the share, and the other is the verification component. Harn's scheme[8] also requires each shareholder to possess $k(k \geq 2)$ shares. However, each participant holds only one share in our scheme, which lowers the risk of share leak.

2) Group oriented SS

In traditional (t, n)-SSs, a participant is able to recover the secret as long as it collects at least t valid shares. This type of schemes can be named as share oriented SSs. Compared with these schemes, our (t, m, n)-GOSS scheme is group oriented, that is because once $m(m \geq t)$ shareholders decide to recover the secret, they will construct RCs to form a tightly coupled group. As a result, any outside adversary, even a legal shareholder, cannot intrude the group to obtain the secret; all participants can obtain the secret if and only if all of them have valid shares and take part in the secret reconstruction honestly.

3) Security without computational assumptions

The security of our scheme does not depend on any assumption of one-way functions or hard problems, *e.g.*, factoring a large number into 2 primes or discrete logarithm problem.

2. Security comparison

In comparison with basic (t, n)-SSs such as Mignotte's SS, Asmuth-Bloom's SS, Shamir's SS and so on, the (t, m, n)-GOSS scheme has the extra security property–group orientation. However, basic (t, n)-SS schemes are unable to prevent the malicious participant attack when there are over t participants.

3. Performance

Let us use Information efficiency (IE) to denote the ratio between the size of the secret space and that of the share space. For a shareholder, IE reflects the efficiency of sharing a secret with others.

Roughly speaking, the IE in Shamir's SS is 1 because both the secret and shares are from the same domain; while in Asmuth-Bloom's SS, the IE is always less than 1 because the secret space is the smallest compared with moduli. The IE in our proposed scheme is within $(\log p_0/\log p_n, \log p_0/\log p_1)$, which can be controlled between $1/2$ and $1/3$ because we can select p_0 and p_i (i=1,2,...,n) such that ${p_0}^3 > p_i > np_0^3/(p_0-1)$, note that p_0 is much larger than n. It implies the IE of our scheme is lower than those of above traditional SSs, that is just the necessary cost our scheme pays for the improved security.

As mentioned above, Harn's (t, n)-secure secret reconstruction scheme is similar to our scheme in security but requires $kt > n-1$ to guarantee the security, where k is the number of polynomials. The IE is $1/k$ because the secret is selected from F_p and each participant has k shares also in F_p. In the case of $k \geq 3$ the IE of Harn's scheme is lower than our (t, m, n)-GOSS scheme; in the case of $k = 2$, its IE is $1/2$ which is higher than that of our scheme. Nevertheless, the requirement, $2t > n-1$, implies that at least $1/2$ of all shareholders are required to take part in the reconstruction to recover the secret; this restriction makes it impractical in applications with a large number of shareholders.

In computational effort, our (t, m, n)-GOSS scheme is almost the same as Asmuth-Bloom's SS except for the extra operation mod p_0 in the last step of secret reconstruction.

VII. Conclusion

An adversary, without any valid share, may obtain the secret in basic (t, n)-SSs when more than t participants take part in a secret reconstruction. In order to solve the problem, the paper first introduced the notion and

gives the definition of (t, m, n)-GOSS, and then proposed a (t, m, n)-GOSS scheme based on CRT. Without using user authentication or share verification, the (t, m, n)-GOSS scheme employs RC to bind all participants into a tightly coupled group and ensures that the secret can be recovered only if each participant has a valid share and releases RC honestly. Besides, the scheme does not depend on any hard problem or one way function. Analysis shows that the scheme remains to be secure even if up to $m-1$ RCs or $t-1$ shares are available for adversaries.

Moreover, the RC in our scheme also plays the role of protecting the share it contains, as a result, a shareholder is allowed to employ the same share to construct different RCs and use the share more than once without worrying about the exposition of the share. Therefore, RCs can be used to construct multi-secret sharing[11] or group authentication[12] schemes in more efficient and flexible ways.

References

[1] A. Shamir, "How to share a secret", *Communications of the ACM*, Vol.22, No.11, pp.612–613, 1979.

[2] G.R. Blakley, "Safeguarding cryptographic keys", *International Workshop on Managing Requirements Knowledge*, pp.313–313, 1899.

[3] Massey James L, "Minimal codewords and secret sharing", *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pp.276–279, 1993.

[4] M. Mignotte, "How to share a secret", *Cryptography*, pp.371–375, 1983.

[5] C. Asmuth and J. Bloom, "A modular approach to key safeguarding", *IEEE Transactions on Information Theory*, Vol.30, No.2, pp.208–210, 1983.

[6] M.L. Das, A. Saxena and V.P. Gulati, "A dynamic ID-based remote user authentication scheme", *Consumer Electronics, IEEE Transactions on*, Vol.50, No.2, pp.629–631, 2004.

[7] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, "Verifiable secret sharing and achieving simultaneously in the presence of faults", *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pp.383–395, 1985.

[8] Lein Harn, "Secure secret reconstruction and multi-secret sharing schemes with unconditional security", *Security and Communication Networks*, Vol.7, No.3, pp.567–573, 2014.

[9] J.C. Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret secret", *Advances in Cryptology-CRYPTO'86*, pp.251–260, 1987.

[10] W.A. Jackson and K.M. Martin, "Combinatorial models for perfect secret sharing schemes", *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol.28, pp.249–265, 1998.

[11] C.C. Yang, T.Y. Chang and M.S. Hwang, "A (t, n) multi-secret sharing scheme", *Applied Mathematics and Computation*, Vol.151, No.2, pp.483–490, 2004.

[12] L. Harn, "Group authentication", *IEEE Transactions on Computers*, Vol.62, No.9, pp.1893–1898, 2013.

MIAO Fuyou received his M.S. degree in Computer Science and Technology from the China University of Mining Technology (Beijing) in 1999. In 2005, he received his Ph.D. degree in Computer Science from the University of Science and Technology of China. Currently, he is an associate professor with the School of Computer Science and Technology, University of Science and Technology of China. His research interests are applied cryptography, network security and mobile computing. personal homepage: *cs.ustc.edu.cn/szdw/fjs/201012/t2010121884381.html* (Email: mfy@ustc.edu.cn)