Randomized Component and Its Application to (t,m,n)-Group Oriented Secret Sharing

Miao Fuyou Xiong Yan Wang Xingfu Moaman Badawy

***Abstract*— A basic (t,n)-secret sharing (SS) scheme allows a secret s to be divided into n shares and shared among n shareholders. In the scheme, any t or more than t shareholders can recover the secret while fewer than t shareholders cannot obtain the secret s. But an adversary without any valid share may obtain the secret if there are over t participants in the secret reconstruction. To address this type of attack, 1) we first introduce the notion of Randomized Component (RC), which binds a share with all participants and protects the share from being exposed to outside without any computational assumption; at the same time, RCs can be used to reconstruct the secret. 2) As one of the applications of RCs, a (t,m,n)-Group Oriented SS scheme is proposed to cope with the attack in basic (t,n)-SSs, in which once m ($m \geq t$) participants form a tightly couple group by generating RCs, the secret can be recovered only if all m RCs are correct, which requires each participant to have a valid share in advance. Moreover, the scheme can secure the secret without any user authentication or share verification. Analyses show the proposed (t,m,n)-Group Oriented SS is asymptotically perfect and unconditionally secure. RCs can also be applied to build other schemes in a simple way, such as multi-secret sharing, group authentication and so on.**

***Keywords*—Threshold Secret Sharing, Group Oriented Secret Sharing, Randomized Component, Share Protection, Asymptotically Perfect.**

I. INTRODUCTION

As a solution to safeguard cryptographic keys, Secret Sharing (SS) Schemes were first proposed separately by Shamir [1] and Blakley [2] in 1979 and later were studied extensively in the literature. Today, SS has become a basic cryptographic tool which is widely used in group based applications such as group signature [3],[4], group encryption [5], secure multi-party computation [6] etc. As the most popular SS, Shamir's (t,n) SS is constructed based on the Lagrange interpolation polynomial. In the Shamir's (t,n) SS, the dealer, a trusted third party, divides a secret s into n shares and distributes each share to a shareholder secretly. The scheme guarantees that any group of t or more than t shareholders are able to reconstruct the secret s while less than t shareholders cannot do that.

In addition to Shamir's SS, other types of SSs were also proposed based on different mathematical tools. For example, Blakely's scheme [2] is based on geometry; Massey's scheme [7] is based on linear codes while Mignotte's scheme [8] and Asmuth-Bloom's scheme [9] are based on the Chinese remainder theorem (CRT). Blakley's scheme [2] defines a threshold scheme based on hyperplane intersections, the hyperplanes of t dimensions allow any group of t hyperplanes to intersect at a single point in a finite field. Massey's scheme [7] uses a linear code to split a secret into equal-size shares, the minimal codewords in the dual code completely specify the access structure of the secret-sharing scheme, and conversely; Mignotte's (t,n) SS scheme [8] and Asmuth-Bloom's (t,n) SS scheme [9] use a series of moduli in an increasing sequence and define schemes based on a specified threshold range of integers. The upper bound and the lower bound of the range are the product of t smallest moduli and the product of $t-1$ largest moduli respectively. If $t-1$ shares are known, Mignotte's scheme leaks more information about the secret than Asmuth-Bloom's scheme does, but the latter scheme limits the secret in a smaller range when both schemes have the same threshold range.

Most SSs, such as Shamir's (t,n) SS, Mignotte's (t,n) SS and Asmuth-Bloom's (t,n) SS, are unconditionally secure. Unconditional security means that the security holds even if the adversary has unbounded computing power. Research on developing cryptographic schemes/protocols with unconditionally secure has received wide attention recently.

Actually, these above basic (t,n) SSs are far from practical. Let us consider the scenario, there are m $(m \geq t+1)$ participants in a secret reconstruction, and one of these participants is an adversary who does not possess any valid share. However, the adversary can still obtain the secret by collecting enough valid shares from the other $m-1 \geq t$ participants to restore the secret.

That is, it is possible for an adversary without any valid share to figure out the secret when there are more than t participants in the secret reconstruction. In some cases, legal participants care more about secret leak rather than recovering the correct secret. i.e. they would rather give up recovering the secret than leak it to adversaries. Therefore, how to prevent

This work was supported in part by the National Natural Science Foundation of China (No.61232018,61170233,61272472,61202404).

Miao Fuyou, School of Computer Science and Technology, University of Science and Technology of China, City of Hefei, Anhui, China, 230027, (email: mfy@ustc.edu.cn; phone: +8613866166896; fax: +86-55163600689).

Xiong Yan, School of Computer Science and Technology, University of Science and Technology of China, City of Hefei, Anhui, China, 230027, (email: yxiong@ustc.edu.cn; phone/fax: +86-55163600689).

Wang Xingfu, School of Computer Science and Technology, University of Science and Technology of China, City of Hefei, Anhui, China, 230027, (email: wangxfu@ustc.edu.cn; phone:+86-55163607858).

Moaman Badawy, School of Computer Science and Technology, University of Science and Technology of China, City of Hefei, Anhui, China, 230027. (email: moahba@yahoo.com;)

the above adversary from obtaining the secret is of great importance.

A solution to the above problem is user authentication, which guarantees only valid shareholders can participate in the secret reconstruction. However, this method makes the scheme more complicated because each participant needs to be authenticated by another one, which means $t(t-1)$ user authentications are needed among t participants. To prevent illegal users from participating in a secret reconstruction, in 1985, Chor et al. [10] proposed the notion of verifiable secret sharing (VSS). VSS enables shareholders to prove that their shares are valid without revealing them. There are many papers on VSS [11]-[15] in the literature. Feldman in [11] pointed out that problems such as secret bidding, fair voting, leader election and flipping a fair coin have simple one-round reductions to VSS. There is a constant-round reduction from Byzantine Agreement to non-interactive VSS. Harn and Liu [12] proposed a strong (n,t,n) VSS, which ensures that any subset of t shares can recover the same secret. Pederson in [13] gave a non-interactive (t,n) VSS with the information rate 1/2 and the distribution of the secret in Z_q together with the verification of a share needs no more than $2|q|t$ multiplication modulo p. In [14], a perfect verifiable (t,n)-SS based on symmetric bivariate polynomial was proposed that supports less than $n/4-1$ adversaries. Besides, a result was shown in [15] that less than n/3 adversaries are allowed to exist in an information-theoretically secure (t,n)-VSS. Although VSS can be used to check the validity of each share; but it is very complicated and requires additional information and processing time.

To prevent the above attack in a simpler way, Harn [16] proposed a (t,n) secure secret reconstruction scheme using the linear combination of shares based on the property of homomorphism [17] of Lagrange interpolation polynomials. The scheme uses k $(k \geq 2)$ polynomials to generate k shares for each shareholder, i.e. each shareholder holds k shares. It requires $kt > n-1$, which means the total number of coefficients of all polynomials has to be no less than that of shareholders. In other words, the threshold t is restricted by the numbers of polynomials and shareholders, and thus Harn's scheme is not flexible enough.

Perfect secrecy [18],[19] is an important metric of the security in a SS scheme. It means that any unqualified subset of participants does not have any more information about the secret than an outsider to the scheme. Quisquater et al.[18] developed the notion of asymptotically perfect secrecy, and pointed out that both Mignotte's scheme [8] and Asmuth-Bloom's scheme [9] are neither perfect nor asymptotically perfect. Moreover, they proved that the SS scheme in [23] is asymptotically perfect; the scheme is based on CRT with consecutive prime moduli.

In this paper, we first propose the notion of randomized component (RC) which binds a participant's share with the public information of all participants during the secret reconstruction. A RC can protect the share from being exposed to the outside and enable a shareholder to use its share more than once if necessary. RCs can also be used to build multi-SS schemes [20],[24] and group authentication schemes [21] in a simple and efficient way. As one of the applications, a (t,m,n) -group oriented SS scheme is proposed. In the scheme, once m ($m \geq t$) participants form a tightly coupled group by generating RCs, recovering the secret requires a participant to collect all m correct RCs, which in turn requires each participant to possess a valid share in advance. Moreover, the proposed scheme does not depend on user authentication or share verification mechanism, and is asymptotically perfect and unconditionally secure.

The rest of the paper is organized as follows. Some preliminaries are given in the next section. In Section III, we introduce the notion of randomized components and construct an example based on polynomial. As one of the applications of RCs, the (t,m,n)-group oriented SS is proposed in section IV. In section V, security analyses of the proposed scheme are given, section VI makes some comparisons with related work, and section VII concludes the paper.

II. PRELIMINARIES

In this section, we will introduce some definition related to secret sharing. The following notations will be used throughout the paper, I_n is the integer set {1,2,…n}, p,q are positive prime numbers, $F_p = Z_p = \{0,1,2,...,p-1\}$ is a finite field with p elements, $F_p^* = \{1,2,...,p-1\}$ is the multiplicative group of F_p ; $r \in_R Z_q$ means that r is randomly and uniformly selected in Z_q , i.e. r has a uniform distribution in Z_q ; Ω is the set of all shares generated by a SS scheme, $\mathcal{S}$ denotes the secret space and $\mathcal{S}_i$ is referred to as the share space.

A. Some Definitions

Informally, in a (t,n)- secret sharing scheme, n shares are generated from a secret s and each share is distributed to the corresponding shareholder privately. Any subset of at least t shareholders can reconstruct the secret s with their shares while fewer than t shareholders cannot get the secret.

Definition 1.((t,n) SS) Let integers p , q ($p \geq q$) be security parameters, $\mathcal{S} = Z_q$ and $\mathcal{S}_i = Z_p$ denote the secret space and the share space respectively; a (t,n) SS is a pair of algorithms {G, R}:

Share Generation algorithm -- $G_{(p,q,t,n)}(s,\mathcal{U})$ is a probabilistic polynomial time algorithm taking as input a secret $s \in \mathcal{S}$ as well as a group of shareholders $\mathcal{U} = \{U_i \mid U_i \in Z, i \in I_n\}$, with the corresponding public information $\mathcal{X} = \{x_i \mid x_i \in Z_p, i \in I_n\}$, and generating as output a set of n shares $\Omega = \{s_i \mid s_i \in \mathcal{S}_i, i \in I_n\}$;

Secret Reconstruction algorithm -- $R_{(p,q,t,n)}(\Omega_{I_m}, \mathcal{U}_{I_m})$ is a polynomial time algorithm taking as input any share set $\Omega_{I_m} = \{s_i \mid s_i \in \mathcal{S}_i, i \in I_m\}$ in combination with the

corresponding shareholder set $\mathcal{U}_{I_m}=\{U_i \mid U_i \in Z, i \in I_m\}$ and producing the secret s as output, where $I_m \subseteq I_n, |I_m| = m \geq t$, $|I_m|$ is the cardinality of I_m.

Now we need to introduce some basic terms in information theory, suppose X is a discrete-time discrete valued random variable with a sample space $\mathcal{SP}$. The entropy of X is denoted as

$$H(X)=E(-\log_2 P(X))=\sum_{x\in\mathcal{SP}} -P(x)\log_2 P(x) \quad .$$

Where E is the expectation operator and $P(.)$ is the probability distribution function of X. In following part of this paper, we will write $\log_2 P(x)$ as $\log P(x)$ for simplicity.

Definition 2. (Perfect (t,n) SS) Let H(.) be the information entropy function, $\Delta(s;a)$ denotes the entropy loss of s generated by the knowledge of a. A (t,n) SS, $\{ G_{(p,q,t,n)}(s,\mathcal{U}), R_{(p,q,t,n)}(\Omega_{I_m},\mathcal{U}_{I_m}) \}$, with the share set $\Omega=\{ s_i \mid s_i \in \mathcal{S}_i, i \in I_n \}$, is perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$ if

1) $H(s) \geq 0$ and

2) $\Delta(s;\Omega_J)=H(s)-H(s \mid \Omega_J)=0$,

where J is a subset of I_n with $|J|<t$, $\Omega_J=\{ s_i \mid s_i \in \Omega, i \in J \}$ denotes any subset of less than t shares.

Informally, compared with an outside adversary who does not have any valid share, any subset of less than t shareholders gets no additional information of the secret in a perfect (t,n) SS. Loosening the perfect (t,n) SS a little bit, we get the definition of asymptotically perfect (t,n) SS as follows.

Definition 3. (Asymptotically Perfect (t,n) SS [13]) A (t,n) SS, $\{ G_{(p,q,t,n)}(s,\mathcal{U}), R_{(p,q,t,n)}(\Omega_{I_m},\mathcal{U}_{I_m}) \}$, with the share set $\Omega=\{ s_i \mid s_i \in \mathcal{S}_i, i \in I_n \}$, is asymptotically perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$ if , for any positive value ε, there exists an integer q_0 such that for all $\mathcal{S}=Z_q$ with $q>q_0$ and all $J \subseteq I_n$ with $|J|<t$, we have

1) $H(s)>0$ and

2) $|\Delta(s;\Omega_J)|<\varepsilon$.

Where $\Omega_J=\{ s_i \mid s_i \in \Omega, i \in J \}$ denotes any subset of less than t shares.

Remark 2.1 In some cases, $\Delta(s;\Omega_J)$ may be negative, but it is positive and the absolute value operator can be removed if the secret s is uniformly distributed on $\mathcal{S}$.

B. Shamir's (t, n)-SS Scheme [1]

Shamir's (t,n) SS scheme is based on a polynomial of degree at most $t-1$, in which there are n shareholders, $\mathcal{U}=\{U_1,U_2,\ldots U_n\}$ and a dealer D.

Share Generation

The dealer D picks a random polynomial $f(x)$ of degree at most $t-1$: $f(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1} \bmod p$, such that the secret is $s=f(0)=a_0$ and all coefficients, a_i $(i=0,1,\ldots,t-1)$ are in the finite field F_p, where p is a large prime number. D generates the share set, $\Omega=\{ s_i \mid s_i=f(x_i), i \in I_n \}$, where x_i is the public information associated with shareholder U_i. Then, it distributes each share s_i to the corresponding shareholder U_i secretly. This step corresponds to the algorithm $G_{(p,p,t,n)}(a_0,\mathcal{U})$.

Secret Reconstruction

If m participants $\mathcal{U}_{J_m}=\{U_j \mid U_j \in \mathcal{U}, j \in J_m\}$ need to recover the secret s, they pool their shares $\Omega_{J_m}=\{ s_j \mid s_j \in \Omega, j \in J_m \}$ privately to compute the secret as $s=f(0)=\sum_{j\in J_m} s_j \prod_{r\in J_m, r\neq j} \frac{-x_r}{x_j-x_r} \bmod p$. where $J_m \subseteq I_n, |J_m| = m, t \leq m \leq n$.

This step actually corresponds to the algorithm $R_{(p,p,t,n)}(\Omega_{J_m},\mathcal{U}_{J_m})$.

Shamir's (t,n) SS is unconditionally secure since the scheme works without any computational assumption, such as DLP assumption or one-way function assumption.

Proposition 1. The above Shamir's (t,n) SS, $\{ G_{(p,p,t,n)}(a_0,\mathcal{U}), R_{(p,p,t,n)}(\Omega_{J_m},\mathcal{U}_{J_m}) \}$, is not perfectly secure if the polynomial $f(x)$ is exactly of degree $t-1$. Formally, there exists some K, $K \subseteq I_n$ with $|K|<t$ such that, if the coefficient a_{t-1} in the polynomial is not zero, we have

1) $H(s)>0$ and

2) $|\Delta(s;\mathcal{S}_K)|>0$.

Where $\mathcal{S}_K$ denotes $\{ s_k \mid s_k \in \Omega, k \in K \}$, some set of less than t shares.

Proof: Here we need only to consider the case that $t-1$ participants conspire to reconstruct the secret. If the entropy loss of the secret generated by the knowledge of $t-1$ shares is larger than zero, we are assured that the Shamir's (t,n) SS is not perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$.

Suppose $f(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1} \bmod p$ is the polynomial in the Shamir's (t,n) SS, $K \subset I_n$ with $|K|=t-1$ and $\mathcal{S}_K=\{ s_k \mid s_k \in \Omega, k \in K \}$ is any group of $t-1$ shares generated by $f(x)$. We will examine, $P(s \mid \mathcal{S}_K)$, the probability of the secret s with the knowledge of $t-1$ shares in the case of $a_{t-1} \neq 0$.

The $t-1$ shareholders, $\mathcal{U}_K=\{U_k \mid U_k \in \mathcal{U}, k \in K\}$, with $t-1$ shares $\mathcal{S}_K$ can reconstruct a new polynomial of degree at most $t-2$, $g(x)=b_0+b_1x+\ldots+b_{t-2}x^{t-2} \bmod p$, using the Lagrange interpolation, with $s_k=f(x_k)=g(x_k)$ $(k \in K)$ but $f(0) \neq g(0)$, where x_k $(x_k \neq 0)$ is the public information

of the shareholder U_k. That is because if $f(0)=g(0)$ holds [19], $a_{t-1}=0$ will happen, which contradicts the precondition $a_{t-1}\neq 0$. In this case, the $t-1$ shareholders $\mathcal{U}_K$, can exclude $g(0)\in F_p$ from the secret space, and thus $P(s\mid \mathcal{S}_K)$, the probability of the secret now becomes $1/(p-1)$. Thus we have

$$\Delta(s;\mathcal{S}_K)=H(s)-H(s|\mathcal{S}_K)=\log p-\log(p-1)=\log\frac{p}{p-1}>0$$

(2-1).

Therefore, we conclude that (t,n) Shamir's SS is not perfect in the case of $a_{t-1}\neq 0$ [19].

C. Secure Secret Reconstruction Scheme

To cope with the above mentioned attack without using user authentication or VSS, Harn [16] proposed a (t,n) secure secret reconstruction scheme in 2013. It consists of the following 2 steps.

Share generation

Suppose there are n shareholders U_r $(r=1,2,\ldots,n)$, the dealer D selects k $(kt>n-1)$ random polynomials $f_l(x)$ $(l=1,2,..,k)$ with degree $t-1$ each and generates shares, $f_l(x_r)$, $l=1,2,..,k$, for each shareholder U_r $(r=1,2,..,n)$. For any secret s, the dealer can always find integers w_l,d_l $(l=1,2,..,k)$ 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 and j, x_i is the public information of shareholder U_i. The dealer makes these integers w_l,d_l $(l=1,2,..,k)$ publicly known.

Secret reconstruction

Suppose j out of n shareholders U_{r_i} $(i=1,2,\ldots,j)$ want to recover the secret, each participant U_{r_i} uses his shares $f_l(x_{r_i})$ $(l=1,2,..,k)$ to compute and release one Lagrange component, $c_{r_i}=\sum_{l=1}^{k}d_l f_l(x_{r_i})\prod_{v=1,v\neq i}^{j}\frac{w_l-x_{r_v}}{x_{r_i}-x_{r_v}} \bmod p$, to all other participants secretly.

After knowing $c_{r_i},i=1,2,..,j$, each participant computes $s=\sum_{i=1}^{j}c_{r_i} \bmod p$.

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

III. RANDOMIZED COMPONENT

From the attack, we are motivated to protect each share by binding it with public information of all participants in a secret reconstruction. We use Randomized Components to attain this goal.

A. Definition of Randomized Component

Definition 4. (Randomized Component-RC) In the (t,n) SS scheme ($G_{(p,q,t,n)}(s,\mathcal{U})$, $R_{(p,q,t,n)}(\Omega_{I_m},\mathcal{U}_{I_m})$), suppose $\mathcal{C}=Z_p$ is the space of randomized components and $g:\mathcal{S}_i\times\mathcal{U}\times Z_q\to\mathcal{C}$ is a function, $c_i=g(s_i,INF_{I_m},r_i)$ is called the Randomized Component of the participant, U_i $(U_i\in\mathcal{U}_{I_m})$, where s_i is the share of U_i; INF_{I_m} is the public information of $\mathcal{U}_{I_m}$, the group of all m participants in a secret reconstruction; r_i is a random integer uniformly distributed in Z_q.

A RC should have the following properties:

Property 1. (Share Inseparability) Suppose $c_i=g(s_i,INF_{I_m},r_i)$ is a randomized component, $s_i\in\mathcal{S}_i$ and $r_i\in_R Z_q$, given c_i, we have

$P\{s_i\mid c_i=g(s_i,INF_{I_m},r_i)\}=1/q$.

Remark 3.1 The property of share inseparability implies that the RC, c_i, binds the share s_i with INF_{I_m}, which actually represents the whole group of all m participants, and thus all these m participants form a tightly coupled group I_m. Roughly speaking, given c_i, one cannot figure out the share s_i when q is extremely large. Thanks to this property, on one hand, the share s_i is protected by the RC c_i and can be used more than once in several secret sharing based schemes, such as multi-secret sharing [20], multi-group authentication [21] and so on. On the other hand, the RC c_i binds the share s_i with the group $\mathcal{U}_{I_m}$, as a result, it can be used in some group-oriented applications, such as group authentication [21] schemes and the (t,m,n) group-oriented secret sharing scheme which will be given in section IV.

Property 2. (Secret Recoverability) suppose there are totally m $(m\geq t)$ RCs in a secret reconstruction, the secret can be recovered only with all m RCs; otherwise, the secret cannot be obtained. Formally, suppose that $\mathcal{C}_{I_m}=\{c_i\mid c_i=g(s_i,INF_{I_m},r_i),\ i\in I_m\}$ is the RC set generated by all m shareholders in $\mathcal{U}_{I_m}$ and $\mathcal{C}'$ is the RC set available in the secret reconstruction with $\mathcal{C}'\cap\mathcal{C}_{I_m}\neq\Phi$, the probability of deriving the secret s from $\mathcal{C}'$ is

$$P(s\mid\mathcal{C}')\begin{cases}=1 & \text{if } \mathcal{C}'=\mathcal{C}_{I_m},|\mathcal{C}_{I_m}|=m\geq t\\ \triangleright 1/q & \text{otherwise}\end{cases},$$

where $\triangleright 1/q$ denotes converging to $1/q$ while q converges to infinity.

B. Polynomial-based Randomized Component (PRC)

As an instance, a type of RC for (t,n) SS scheme can be constructed based on polynomial interpolation as follows.

Setup: Suppose there are n shareholders, $\mathcal{U}=\{U_1,U_2,\ldots U_n\}$, and a dealer D in the system. D picks a random polynomial: $f(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1} \bmod p$,

such that the secret is $s = f(0) = a_0 \in F_q$, other coefficients, a_i, $i = 1,...t-1$, are in the finite field F_p with $a_{t-1} \neq 0$ and $p > q + nq^2$, both p and q are primes.

Share Generation: D computes n shares, $f(x_i)$, $i = 1,2,...n$, where x_i is the public information associated with shareholder U_i. Then, D distributes each share, e.g., $f(x_i)$, to the corresponding shareholder U_i secretly.

Share Randomization: If m $(m \geq t)$ participants, $\mathcal{U}_{A_m} = \{U_{a_1}, U_{a_2}, ...U_{a_m}\}$, $(\mathcal{U}_{A_m} \subseteq \mathcal{U})$, need to recover the secret s, each participant, e.g. U_{a_i}, $(U_{a_i} \in \mathcal{U}_{A_m})$, constructs the RC as

$$c_{a_i} = (f(x_{a_i}) \prod_{v=1, v\neq i}^{m} \frac{-x_{a_v}}{x_{a_i} - x_{a_v}} + r_{a_i} q) \bmod p, \qquad (r_{a_i} \in_R Z_q). \tag{3-1}$$

In term of the definition of RC, $c_i = g(s_k, INF_{I_m}, r_i)$, $\prod_{v=1, v\neq i}^{m} \frac{-x_{a_v}}{x_{a_i} - x_{a_v}}$ in (3-1) corresponds to INF_{I_m}, the public information of all participants in $\mathcal{U}_{A_m}$.

Now let us first observe the property 1 of RC, the property 2 will be proved in section V.

Theorem 1. For a polynomial-based RC $c_i = (f(x_i) \prod_{v=1, v\neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q) \bmod p$, suppose p, q are primes with $p > nq^2 + q$, integer r_i is uniformly distributed in F_q, and the share $f(x_i)$ is in F_p. Given c_i, the RC of participant U_i, the probability of deriving the share $f(x_i)$ is $1/q$, where x_i is the public information of participant U_i. Formally,

$$P(f(x_i) \mid c_i) = 1/q.$$

Proof: From $c_i = (f(x_i) \prod_{v=1, v\neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q) \bmod p$, we have

$$f(x_i) = (\prod_{v=1, v\neq i}^{m} \frac{-x_v}{x_i - x_v})^{-1} (c_i - r_i q) \bmod p \tag{3-2}$$

Let $h(r) = (c_i - rq) \bmod p$ be a function with respect to r $(r \in F_q)$, with the domain $\mathcal{D} = F_q$ and the range $\mathcal{R} = \{h(r) \mid r \in F_q\}$. Hence, $h(r)$ is a 1-to-1 function from $\mathcal{D}$ to $\mathcal{R}$, which means, given c_i, p and q, $h(r_i) = h(r_j)$ if and only if $r_i = r_j$ for $r_i, r_j \in F_q$.

To prove the necessity, let us assume there exist r_i and r_j in F_q, $h(r_i) = h(r_j)$ means $(r_i - r_j)q = kp$ for some integer k. It follows $p \mid (r_i - r_j)$ since p, q are primes, thus we have $r_i = r_j$ for $r_i, r_j \in F_q$ and $p > nq^2 + q$.

To prove the sufficiency, given $r_i = r_j$, $(r_i, r_j \in Z_q)$, it obviously follows that $h(r_i)$ is equivalent to $h(r_j)$.

If we view r as a variable for a specific x_i, (3-2) can be rewritten as

$$f_{x_i}(r) = (\prod_{v=1, v\neq i}^{t} \frac{-x_v}{x_i - x_v})^{-1} h(r) \bmod p \tag{3-3}$$

Now that $h(r)$ is a 1-to-1 function with respect to $r \in F_q$, each distinct r produces a different value of $f_{x_i}(r)$ in (3-3) since the specific value $(\prod_{v=1, v\neq i}^{t} \frac{-x_v}{x_i - x_v})^{-1} \bmod p$ is coprime to p, which means the probability of deriving $f_{x_i}(r)$ in (3-3), i.e. $f(x_i)$ in (3-2) from c_i is $1/q$ because r is uniformly distributed in F_q.□

Theorem 1 implies that, given the RC c_i, an adversary never has a chance more than $1/q$ to obtain the covered share $f(x_i)$, which is not easier than directly guessing the secret s in F_q, if s is uniformly distributed in the secret space, $\mathcal{S} = F_q$. Therefore, the polynomial based RC possesses the properties of Share Inseparability.

We will demonstrate property 2, secret recoverability, in the following (t,m,n) – Group Oriented SS scheme.

IV. (t,m,n) – Group Oriented SS Scheme based on Randomized Component

As one of applications of RCs, the (t,m,n) – Group Oriented SS is proposed in this section to prevent an adversary without any valid share from obtaining the secret when there are more than t participants in the secret reconstruction.

A. Definition of (t,m,n) – Group Oriented SS

Definition 5. ((t,m,n) – Group Oriented SS) Let primes p and q, ($p \geq q$), be security parameters, $\mathcal{S} = F_q$, $\mathcal{S}_i = F_p$ and $\mathcal{RC} = F_p$ denote the secret space, share space and randomized component space respectively; a (t,m,n) – Group Oriented SS scheme is a group of algorithms {G, C, R}:

Share Generation algorithm -- $G_{(p,q,t,n)}(s, \mathcal{U})$ is a probabilistic polynomial time algorithm taking as input a secret $s \in \mathcal{S}$ as well as a group of shareholders $\mathcal{U} = \{U_i \mid U_i \in Z_p, i \in I_n\}$ and generating as output a set of n shares $\Omega = \{s_i \mid s_i \in \mathcal{S}_i, i \in I_n\}$;

Randomized Component Construction algorithm-- $C_{(p,q,t,n)}(\Omega_{I_m}, \mathcal{U}_{I_m})$ is a probabilistic polynomial time algorithm taking any share set $\Omega_{I_m} = \{s_i \mid s_i \in \mathcal{S}_i, i \in I_m\}$ and the corresponding shareholder set $\mathcal{U}_{I_m} = \{U_i \mid U_i \in \mathcal{U}, i \in I_m\}$ as input and producing a RC set $\mathcal{C}_{I_m} = \{c_i \mid c_i \in \mathcal{RC}, i \in I_m\}$ as output, where $I_m \subseteq I_n$ and $t \leq \mid I_m \mid = m \leq n$.

Secret Reconstruction algorithm -- $R_{(p,q,t,n)}(\mathcal{C}_{I_m})$ is a polynomial time algorithm taking the above RC set $\mathcal{C}_{I_m}$ as input and producing the secret s as output.

The $(t,m,n)-$ Group Oriented SS, $\{ G_{(p,q,t,n)}(s,\mathcal{U}) , C_{(p,q,t,n)}(\Omega_{I_m},\mathcal{U}_{I_m}) , R_{(p,q,t,n)}(\mathcal{C}_{I_m}) \}$, possesses the following property:

$$P(s = R_{(p,q,t,n)}(\mathcal{C}')) \begin{cases} =1 & if\ \mathcal{C}' = \mathcal{C}_{I_m}, |\mathcal{C}_{I_m}| = m \geq t \\ \triangleright 1/q & otherwise \end{cases},$$

where $\mathcal{C}'$ is the RC set available in the secret reconstruction and $\mathcal{C}' \cap \mathcal{C}_{I_m} \neq \Phi$, $\triangleright 1/q$ denotes converging to $1/q$ while q converges to infinity.

Remark 4.1 Compared with basic SS schemes, a $(t,m,n)-$ Group Oriented SS possesses the extra property of security, that is, once m $(m \geq t)$ shareholders form a tightly coupled group by generating RCs, recovering the correct secret requires a participant to collect all the m valid RCs, which, in turn, requires each participant in the group to have a valid share in advance even if m is much larger than t. Otherwise, figuring out the secret is almost as hard as guessing it randomly in the secret space. That is, if the secret is recovered by RCs instead of shares, the threshold actually becomes m, the number of participants. Of course, the threshold t still requires that a qualified tightly coupled group consists of at least t shareholders, i.e. the number of participants m is no less than the threshold t. However, for a basic (t,n) SS scheme such as Shamir's (t,n) SS, the secret can be reconstructed by using any group of t valid shares and the reconstruction does not require all available shares to be used substantially when more than t shares can be used.

In the following, a $(t,m,n)-$ Group Oriented SS scheme will be proposed based on PRC.

B. Entities and Model

In the proposed $(t,m,n)-$ Group Oriented SS, there are 3 types of entities: 1) one dealer, 2) n shareholders and 3) some adversaries.

1) Dealer

The dealer is the coordinator trusted by all shareholders, and responsible for the initialization of the scheme such as deciding system parameters, choosing the secret, generating and distributing shares and so on. The dealer is supposed to be honest, which means that it selects parameters to make the scheme secure enough, keeps critical parameters secret, generates and distributes shares securely.

2) Shareholders

In a $(t,m,n)-$ Group Oriented SS, there are totally n shareholders. We call shareholders participants when they are participating in a secret reconstruction; there is a dedicated private channel between each pair of shareholders, but some of these channels may be cracked by adversaries. Each shareholder also has a secure channel with the dealer and the channel is assumed to be secure, because in our scheme the channel is used only for share distribution which can be accomplished off-line. We also assume that a share is always kept private within a shareholder, i.e. the share can never be obtained from inside the shareholder.

Each shareholder receives a share from the dealer via the secure channel. To recover the secret, m $(m \geq t)$ shareholders first form a tightly coupled group by generating a RC each for the secret, then each releases its RC to the others through private channels and finally reconstructs the secret.

3) Adversaries

In our scheme, adversaries are divided into 2 types according to whether they have valid shares or not.

a) Outsider: an adversary without any valid share. There are 2 cases with an Outsider, i) an Outsider stays outside the tightly coupled group, but it could crack some private channels of the group and intercept RCs transmitted over these channels. In this case, we assume that all Outsiders could obtain no more than m-1 correct RCs in a secret reconstruction, note that m may be much larger than the threshold t. ii) an Outsider may also manage to personate some absent participant in the group but without the required valid share. In this case, the Outsider acts as a malicious participant and can communicate with the others to obtain at most m-1 correct RCs. The proposed scheme aims to prevent Outsiders from obtaining the secret even if they may have access to up to m-1 RCs.

b) Insider: an Insider is actually a legal shareholder with a valid share. However, less than t shareholders may conspire and try to recover the secret. In this case, these misbehaved shareholders are called Insiders. We assume that at most $t-1$ Insiders conspire in the proposed $(t,m,n)-$ Group Oriented SS scheme.

Of course, within a tightly coupled group, if a dishonest participant (with a valid share) releases a wrong RC to the others but uses the correct RC to recover the secret for itself, then only it can obtain the correct secret while the others recover a wrong one. This is actually about Cheater Detection/Identification [25] and Fairness in secret sharing, which goes beyond the scope of the paper.

C. Our proposed scheme

Our scheme focuses on how to simply employ RCs to prevent Outsiders from obtaining the secret even if there are over t participants in the secret reconstruction.

The proposed scheme needs to keep the basic properties of SS schemes, i.e. i) any group of at least t legal shareholders is able to recover the secret, but ii) less than t legal shareholders cannot obtain the secret.

Moreover, the scheme needs to ensure that, in order to recover the secret, all participants must be legal shareholders necessarily (i.e. have a valid share each). Otherwise, the secret should not be figured out.

To achieve these goals, each participant cannot simply release the share and compute the secret as it does in basic (t,n) SS schemes. Instead, every participant must bind its share with the whole group and make them inseparable. In this case, recovering the correct secret requires all participants to necessarily have a valid share each.

The proposed scheme consists of 3 algorithms, 1) *Share Generation* 2) *Randomized Component Construction* and 3) *Secret Reconstruction* as indicated in Figure 1.

Entities:

Dealer: D ;

Set of n shareholders: $\mathcal{U} = \{U_1, U_2, \ldots U_n\}$ with respective public information $\{x_1, x_2, \ldots x_n\}$;

Group of m participants: $\{U_{i_1}, U_{i_2}, \ldots U_{i_m}\} \subseteq \mathcal{U}, (m \geq t)$

Parameters:

Primes: p, q with $p > q + nq^2$;

Polynomial in F_p : $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod p$, $a_i \in F_p$, for $i = 1, \ldots t-1$, $a_{t-1} \neq 0$, $a_0 \in F_q$;

Secret: $s = a_0$;

Algorithms:

A. Share Generation

D computes and sends share $s_i = f(x_i)$ to U_i secretly, for $i = 1, 2, \ldots n$.

B. Randomized Component Construction

Given $\{U_{i_1}, U_{i_2}, \ldots U_{i_m}\} \subseteq \mathcal{U}$, each participant, e.g., $U_{i_j}, (1 \leq j \leq m)$, constructs the RC, c_{i_j} and releases it to the others through private channels:

$$c_{i_j} = \left(f(x_{i_j}) \prod_{v=1, v \neq j}^{m} \frac{-x_{i_v}}{x_{i_j} - x_{i_v}} + r_{i_j} q \right) \bmod p$$

$(r_{i_j} \in_R F_q$, for $j = 1, 2, \ldots m)$

C. Secret Reconstruction

Each participant, e.g., $U_{i_j}, (1 \leq j \leq m)$, computes the secret as $s = \left(\sum_{j=1}^{m} c_{i_j} \bmod p \right) \bmod q$.

Fig.1. (t, m, n) – Group Oriented SS based on PRC

1) Share Generation

Suppose there are n shareholders, $\mathcal{U} = \{U_1, U_2, \ldots U_n\}$, and a dealer D. D chooses 2 positive prime numbers p and q with $p > q + nq^2$, and a polynomial $f(x)$: $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod p$, with the secret $s = a_0 \in F_q$ and coefficients, $a_i \in_R F_p$, for $i = 0, 1, \ldots t-1$, with $a_{t-1} \neq 0$. D computes n shares, $f(x_i)$, $(i = 1, 2, \ldots n)$, and distributes each share, e.g. $f(x_i)$, to the corresponding shareholder U_i secretly, where x_i is the public information associated with U_i.

This step corresponds to the algorithm $G_{(p,q,t,n)}(a_0, \mathcal{U})$ and the output is the share set $\Omega = \{ f(x_i) \mid i \in I_n \}$.

2) Randomized Component Construction

If a group of m shareholders, $\mathcal{U}_{I_m} = \{U_{i_j} \mid U_{i_j} \in \mathcal{U}, i_j \in I_m\}$, $(I_m \subseteq I_n, |I_m| = m \geq t)$, wants to recover the secret s, each participant, e.g. U_{i_j} $(i_j \in I_m)$, randomly picks an integer r_{i_j} in F_q, (i.e., $r_{i_j} \in_R F_q$), and computes the RC as

$$c_{i_j} = \left(f(x_{i_j}) \prod_{v=1, v \neq j}^{m} \frac{-x_{i_v}}{x_{i_j} - x_{i_v}} + r_{i_j} q \right) \bmod p .$$

This step corresponds the algorithm $C_{(p,q,t,n)}(\Omega_{I_m}, \mathcal{U}_{I_m})$, where Ω_{I_m} denotes the share set $\{ f(x_{i_j}) \mid i_j \in I_m \}$; the output is the RC set $\mathcal{C}_{I_m} = \{ c_{i_j} \mid i_j \in I_m \}$.

3) Secret Reconstruction

Each participant, e.g. U_{i_j} $(i_j \in I_m)$, releases its RC, $c_{i_j} \in \mathcal{C}_{I_m}$, to all the other participants through private channels. After receiving $(m-1)$ RCs from the others, it computes the secret as

$$s = f(0) = \left(\sum_{i_j \in I_m} c_{i_j} \bmod p \right) \bmod q .$$

This step corresponds to the algorithm $R_{(p,q,t,n)}(\mathcal{C}_{I_m})$.

Due to the following fact, the (t, m, n) – Group Oriented SS is bound to restore the secret s correctly.

$$\left(\sum_{i_j \in I_m} c_{i_j} \bmod p \right) \bmod q$$

$$= \sum_{j=1}^{m} \left(f(x_{i_j}) \prod_{v=1, v \neq j}^{m} \frac{-x_{i_v}}{x_{i_j} - x_{i_v}} + r_{i_j} q \right) \bmod p \bmod q$$

$$= \left(f(0) + \sum_{j=1}^{m} r_{i_j} q \right) \bmod p \bmod q \qquad (4-1)$$

$$= \left(f(0) + \sum_{j=1}^{m} r_{i_j} q \right) \bmod q \qquad (4-2)$$

$$= f(0)$$

Step (4-1) is equivalent to step (4-2) because of $f(0) \in F_q$, $\sum_{j=1}^{m} r_{i_j} q \leq \sum_{j=1}^{n} r_{i_j} q < nqq = nq^2$ and thus $\left(f(0) + \sum_{j=1}^{m} r_{i_j} q \right) < q + nq^2 < p$.

V. Security Analysis

In the (t, m, n) – Group Oriented SS scheme, we use RCs to protect the share of each participant because each RC binds the share and all participants' public information together in the secret reconstruction. To obtain the secret, adversaries use either at least t shares or m ($m \geq t$) RCs if there are totally m participants in the secret reconstruction. We have already demonstrated that a share cannot be derived from a given RC by Theorem 1. In this case, Outsiders, without any valid share, have to use RCs it collects by interception or personation to recover the secret, we use Theorem 2 to prove that Outsiders, even with $m-1$ RCs, are still unable to get the secret. However, Insiders, with a valid share each, may collaborate and try to obtain the secret by using their shares instead of RCs, Theorem 3 assures us that up to $t-1$ Insiders are still unable to reconstruct the secret.

As stated in the security model, Outsiders have access to at most $m-1$ RCs in a secret reconstruction with m participants. The following theorem 2 demonstrates the security of our scheme against Outsiders.

Lemma 1. Suppose that random variable x is uniformly distributed in F_p, for any value $t \in F_p^*$, xt has a uniform distribution over F_p.

Proof: It is easy to see that $t \in F_p$ and $gcd(t,p)=1$ are true. Suppose x_1 and x_2 are 2 distinct values of x in F_p, $tx_1, tx_2 \in F_p$ follows; if $tx_1 = tx_2 \bmod p$ holds, then we have $p \mid (x_1 - x_2)$ due to $gcd(t,p)=1$; it is followed by $x_1 = x_2$ because of $x_1, x_2 \in F_p$, which is contradictory to $x_1 \neq x_2$. Therefore, $tx_1 \neq tx_2 \bmod p$ holds if $x_1 \neq x_2$. That is, all values of xt is a permutation of $\{0,1,2,\ldots,p-1\}$ because x is uniformly distributed in F_p, i.e., xt is also uniformly distributed over F_p. □

Lemma 2. Suppose that p is a prime number and random variables $x[i],(i=1,2,..k)$, are uniformly distributed in F_p, $\sum_{i=1}^{k} t_i x[i]$ has a uniform distribution in F_p for values $t_i \in F_p^*, i=1,2,\ldots k$.

Proof: Let us first consider the case of $k=2$, then generalize it to the case of k being any value.

1). From Lemma 1, we know that both $t_1 x[1]$ and $t_2 x[2]$ are uniformly distributed in F_p, to prove $t_1 x[1] + t_2 x[2]$ is uniformly distributed in F_p, we assume that $x[1]_1$ and $x[1]_2$ are 2 random distinct values of variable $x[1]$. It is obvious that $t_1 x[1]_1$ and $t_1 x[1]_2$ are also distinct in F_p for $gcd(t_1,p)=1$. Besides, $t_1 x[1]_1 + t_2 x[2]$ is a permutation of $t_2 x[2]$ in F_p, which is also a permutation of $x[2]$ over F_p, while $t_1 x[1]_2 + t_2 x[2]$ is a distinct permutation of $x[2]$ in F_p. That is, for any value, e.g., $x[1]_i$ of random variable $x[1]$, $t_1 x[1]_i + t_2 x[2]$ is bound to be a permutation of $x[2]$ in F_p. i.e., $t_1 x[1] + t_2 x[2]$ is a sequence such that each value $x_i \in F_p$ appears p times during the search for all values of $t_1 x[1] + t_2 x[2]$ in F_p. Therefore, $t_1 x[1] + t_2 x[2]$ is uniformly distributed in F_p.

2). Now that $t_1 x[1] + t_2 x[2]$ is uniformly distributed in F_p, by iterating the process in 1), we have the result that $\sum_{i=1}^{k} t_i x_i$ has a uniform distribution in F_p. □

Corollary 1. If p is a prime number, random variables, $x[i],(i=1,2,..k)$, are uniformly distributed over F_p and random variable y is uniformly distributed in Z_w, (w is an integer with $w < p$), then $\sum_{i=1}^{k} t_i x[i] + y$ has a uniform distribution in F_p for values $t_i \in F_p^*, i=1,2,\ldots k$.

Theorem 2. Suppose there are m ($m \geq t$) participants collaborating to recover the secret s in our proposed (t,m,n)-Group Oriented SS; For an Outsider with less than m RCs, the scheme is asymptotically perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$. Formally, suppose the participants' RC set is Θ with $|\Theta| = m$, and an Outsider has already known $\mathcal{C}_{I_k} = \{ c_{i_j} \mid c_{i_j} \in \Theta, i_j \in I_k, |I_k| = k < m \}$, any subset of Θ with k $(k < m)$ RCs. For any positive value ε, there exists an integer q_0 such that for any $q > q_0$ with $\mathcal{S} = Z_q$, we have

$$\Delta(s; \mathcal{C}_{I_k}) = H(s) - H(s \mid \mathcal{C}_{I_k}) \leq \varepsilon.$$

Proof: First, suppose there are m participants, $\{U_1, U_2, \ldots U_m\}$ $(m \geq t)$, with m RCs, $\{c_1, c_2, \ldots c_m\}$. Without losing generality, we assume that the Outsider have obtained k $(k < m)$ out of m RCs, e.g., $\mathcal{C}_{I_k} = \{c_1, c_2, \ldots c_k\}$, and recovered the value s' as $s' = \sum_{i=1}^{k} c_i \bmod p \bmod q$, where $c_i = (f(x_i) \prod_{v=1, v \neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q) \bmod p$, $r_i \in_R Z_q$ and x_i is the public information of U_i $(1 \leq i \leq m)$.

Let us examine the probability of $s = s'$, e.g., $P(s \mid \mathcal{C}_{I_k})$, the probability of the secret s with the knowledge of $\mathcal{C}_{I_k}$.

$s = s'$ means $\sum_{i=1}^{m} c_i \bmod p \bmod q = \sum_{i=1}^{k} c_i \bmod p \bmod q$, that is

$$(\sum_{i=k+1}^{m} c_i \bmod p + \sum_{i=1}^{k} c_i \bmod p) \bmod p - \sum_{i=1}^{k} c_i \bmod p = \lambda q \qquad (5\text{-}1),$$

where λ is an integer.

Remark 5.1 $s = s'$ means $\sum_{i=1}^{m} c_i \bmod p \bmod q = \sum_{i=1}^{k} c_i \bmod p \bmod q$. On one hand, as we will prove later, $\sum_{i=1}^{m} c_i \bmod p$, $\sum_{i=1}^{k} c_i \bmod p$ and $(\sum_{i=1}^{m} c_i - \sum_{i=1}^{k} c_i) \bmod p$ are uniformly distributed over F_p ; moreover, each RC contains a random multiple of q. To some extent, it means s and s' are virtually independent of each other. On the other hand, RCs make shares inseparable from all participants' public information. As a result, Outsiders are unable to use shares contained in these RCs directly as they do in Shamir's SS but are forced to use RCs themselves. Therefore, there is no better way for Outsiders to get the secret except to assume $s' = s$.

Second, we will show that $\sum_{i=k+1}^{m} c_i \bmod p$ is uniformly distributed over F_p when some coefficients of $f(x)$ are uniformly distributed in F_p. To begin with, let us examine the probability distribution of

$$c_i = (f(x_i) \prod_{v=1, v \neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q) \bmod p, \text{ for } i = 1,2,\ldots m.$$

(1) Note that, for the Outsider, $f(x_i)$ has the form of $f(x_i) = \sum_{j=0}^{t-1} a_j x_i^j \bmod p$ with a_j $(j = 1,\ldots t-2)$ uniformly distributed in F_p and $gcd(x_i^j, p) = 1$ holds for $j = 1,\ldots t-1$ due to $x_i \in F_p^*$ and the primality of p, (i.e.,

$x_i^j \in F_p^*$). As a result, $f(x_i) = \sum_{j=0}^{t-1} a_j x_i^j \bmod p$ is uniformly distributed over F_p according to Corollary 1.

(2) Let Π be $\prod_{v=1,v\neq i}^{m} \frac{-x_v}{x_i - x_v} \bmod p$, Π is a fixed value for a specific group of participants and also coprime to p due to the properties of a field. More specifically, for $x_v \in F_p, x_v \neq 0$, $(v = 1,..m)$ and prime number p, we have, i) $(-x_v) \bmod p \in F_p^*$ $(v = 1,2,...,m)$ and ii) $(x_i - x_v) \bmod p \in F_p^*$ due to $x_i \neq x_v$ and the additive closure of F_p. Consequently, $(x_i - x_v)^{-1} \bmod p \in F_p^*$ is true because it is the multiplicative inverse of $(x_i - x_v) \bmod p$. It follows from i) and ii) that $\frac{-x_v}{x_i - x_v} \bmod p \in F_p^*$ (for $v = 1,2,...,m, x_v \neq x_i$) and $\prod_{v=1,v\neq i}^{m} \frac{-x_v}{x_i - x_v} \bmod p \in F_p^*$ hold due to the multiplicative closure of F_p^*.

From (1) and (2), we further have that $f(x_i) \prod_{v=1,v\neq i}^{m} \frac{-x_v}{x_i - x_v} \bmod p$ is uniformly distributed over F_p for the Outsider in the light of Lemma 1. Moreover, for a specific RC, e.g. $c_i = (f(x_i) \prod_{v=1,v\neq i}^{m} \frac{-x_v}{x_i - x_v} + r_i q) \bmod p$, c_i also has a uniform distribution in F_p from the proof of Lemma 2. As a result, $\sum_{i=k+1}^{m} c_i \bmod p$ is uniformly distributed in F_p according to the additive closure of the field F_p.

Third, let us observe the probability $P(s \mid \mathcal{C}_{I_k})$, i.e., the probability with which (5-1) holds, where $\mathcal{C}_{I_k}$ is any subset of Θ with k RCs. Now that $\sum_{i=k+1}^{m} c_i \bmod p$ has a uniform distribution in F_p, the left side of (5-1) varies uniformly within the range $(-\sum_{i=1}^{k} c_i \bmod p, p - \sum_{i=1}^{k} c_i \bmod p)$, which consists of p consecutive integer values. As a result, the largest number of possible values of λ in (5-1) is $\lfloor p/q \rfloor + 1$ and thus $P(s \mid \mathcal{C}_{I_k})$ is at most $(\lfloor p/q \rfloor + 1)/p$. Recall $s = a_0 \in_R F_q$ and $P(s) = 1/q$, therefore, the entropy loss of the secret satisfies

$$\Delta(s; \mathcal{C}_{I_k}) = H(s) - H(s \mid \mathcal{C}_{I_k}) \leq \log q - \log \frac{p}{\lfloor p/q \rfloor + 1}$$

$$= \log \frac{q(\lfloor p/q \rfloor + 1)}{p} < \log \frac{p+q}{p} = \log \frac{p/q + 1}{p/q} < \varepsilon \qquad (5\text{-}2)$$

That is, $\Delta(s; \mathcal{C}_{I_k})$ converges to zero as q converges to infinity because p/q is a value larger than $1 + nq$ due to $q + nq^2 < p$. As a result, our proposed scheme is asymptotically perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$. □

Remark 5.2 (5-2) denotes that $\Delta(s; \mathcal{C}_{I_k})$, the entropy loss of the secret caused by the knowledge of less than m RCs, basically equals zero for sufficiently large prime number q. That is, knowing up to $(m-1)$ RCs hardly helps Outsiders obtain the secret.

Remark 5.3 Theorem 2 also indicates that the secret can be restored only if all RCs used are correct, which further requires each participant to have a valid share; otherwise, it is almost impossible to obtain the secret more easily than to guess it directly in the secret space. This attribute is obviously enabled by the properties of RCs.

An Insider is actually a legal shareholder and up to $t-1$ Insiders may form a group and try to recover the secret. As Theorem 3 indicates, the proposed (t,m,n) -Group Oriented SS remains secure even if up to $t-1$ Insiders conspire.

Theorem 3. In our proposed (t,m,n)-Group Oriented SS, for less than t Insiders, the scheme is asymptotically perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$. Formally, suppose that the set of the shares available for Insiders is $\mathcal{S}_{K_d} = \{ s_{k_i} = f(x_{k_i}) \mid s_{k_i} \in \Omega, k_i \in K_d \}$, $(K_d \subseteq I_n, \mid K_d \mid = d < t)$, for any positive value ε, there exists an integer q_0 such that for any $q > q_0$ with $\mathcal{S} = Z_q$, we have

$$\Delta(s; \mathcal{S}_{K_d}) = H(s) - H(s \mid \mathcal{S}_{K_d}) \leq \varepsilon.$$

Proof: Note that our proposed (t,m,n) -Group Oriented SS uses the polynomial, $f(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1} \bmod p$, with $a_i \in F_p$, for $i = 1,...t-1$, $a_{t-1} \neq 0$, the secret $s = a_0 \in F_q$ and $p > q + nq^2$. Suppose there are d $(d = \mid K_d \mid < t)$ Insiders, $\mathcal{U}_{K_d} = \{ U_{k_i} \mid U_{k_i} \in \mathcal{U}, k_i \in K_d \}$, with d shares $\mathcal{S}_{K_d} = \{ s_{k_i} = f(x_{k_i}) \mid k_i \in K_d \}$, where x_{k_i} is the public information of U_{k_i}. $\mathcal{U}_{K_d}$ can conspire to compute

$$s' = \sum_{k_i \in K_d} s_{k_i} \prod_{\substack{k_j \in K_d \\ k_j \neq k_i}} \frac{-x_{k_j}}{x_{k_i} - x_{k_j}} \bmod p.$$

Next, the upper bound of $P(s \mid \mathcal{S}_{K_d})$, the probability of the secret with the knowledge of $\mathcal{S}_{K_d}$, will be identified.

We just need to consider the case of $d = t-1$, in which $P(s \mid \mathcal{S}_{K_d})$, has the largest value .

In this case, if $s' < q$ happens, we are assured that $s' \neq s$ is true from proposition 1. As a result, the maximum $P(s \mid \mathcal{S}_{K_d})$ is $1/(q-1)$ since the value s' can be excluded from the secret space $\mathcal{S} = F_q$. Recall that s is randomly selected in F_q and thus $P(s)$ is $1/q$. As a result, we have

$$\Delta(s; \mathcal{S}_{K_d}) = H(s) - H(s \mid \mathcal{S}_{K_d})$$

$$\leq \log q - \log(q-1) = \log \frac{q}{q-1} < \varepsilon \qquad (5\text{-}3).$$

That is, $\Delta(s;\mathcal{S}_{K_d})$ converges to zero as q converges to infinity. Therefore, the proposed (t,m,n)-Group Oriented SS, for less than t Insiders, is asymptotically perfect with respect to the set of probability distributions $P(.)$ on the secret space $\mathcal{S}$. □

Theorem 4. The proposed (t,m,n)-Group Oriented SS is asymptotically perfect with respect to the set of probability distributions on the secret space.

In our security model, we conclude from Theorem 2 and 3 that the proposed (t,m,n)-Group Oriented SS is asymptotically perfect with respect to the set of probability distributions on the secret space, because both types of adversaries hardly get any information when they fail to have enough correct RCs or valid shares available. Formally, entropy losses of the secret for both types of adversaries converge to zero as the secret space converges to infinity.

VI. Properties and Comparisons

RCs bring our scheme new features although the scheme is based on Shamir's SS. Distinct from Verifiable SSs and similar to the proposed scheme, Harn's scheme [16] is the one solving the above mentioned attack without user authentication or share verification. In this section, we will summarize the properties of our scheme and make some comparisons with Harn's scheme and traditional SS schemes.

A. Properties

1) Single share

Harn's scheme [16] uses k ($k \geq 2$) polynomials and each shareholder holds k shares; but our proposed scheme requires each participant to hold only one share. In many VSS schemes, share verification is required. As a result, each participant needs 2 items in a secret reconstruction, one is the share, and the other is the verification component.

2) Group oriented

In basic (t,n)-SSs, a participant is able to recover the secret as long as it collects no less than t valid shares, i.e., it does not have to get all the shares of all participants in the reconstruction. This type of SSs can be called share oriented ones. Compared with this type, the proposed scheme can be called group oriented SS, that is because all participants form a tightly coupled group before the secret reconstruction by generating a RC each, which binds a participant with the others in the group. Recovering the correct secret requires each participant to not only have a valid share but also belong to the group (i.e. a participant U_i belonging to a group means the public information x_i of U_i is used by all participants in the group when constructing their RCs). Otherwise, a shareholder, even with a valid share but outside the group, is unable to generate a correct RC of the group and thus cannot recover the secret within the group.

It is the group oriented property which prevents an adversary without a valid share (e.g. the Outsider in our scheme) from obtaining the secret.

3) Unconditionally secure

The security of our scheme does not depend on any assumptions of hard problems such as Discrete Logarithm Problem or one way functions, i.e. its security holds even if the adversary have infinite computing power or storage capacity.

4) Without user authentication or share verification

The proposed scheme solves the problem in basic (t,n)-SSs without using any user authentication or share verification needed in most Verifiable SSs.

B. Security comparisons

Compared with basic (t,n)-SSs, such as Shamir's SS, Mignotte's SS, Asmuth-Bloom's SS and so on, our proposed (t,m,n)-Group Oriented SS possesses extra security property, which guarantees that once a group of m $(m > t)$ shareholders, agrees to work together, the secret can be reconstructed only if each participant necessarily has a valid share.

However, basic (t,n)-SSs allow the secret to be recovered as long as there are at least t valid shares available, it is possible for a participant without a valid share to obtain the secret when more than t shareholders participate in the secret reconstruction.

Moreover, the RC in our scheme also plays the role of protecting the share it contains. Therefore, RCs can be used to construct some other secret sharing based schemes such as multi-secret SS[16], Group authentication[21] and so on. .

C. Performance comparisons

Let us use the ratio of the size of the secret space to that of the share space to measure the information ratio of SS schemes. For a shareholder, information ratio reflects the efficiency of sharing a secret with others.

Roughly speaking, In Shamir's SS, the information ratio is 1 because both the secret and the share are from the same domain; while in Asmuth-Bloom's SS, the information ratio is always less than 1 because the secret space is the smallest compared with moduli of shareholders. The information ratio of our proposed scheme is $\log q / \log p$, which can be controlled between 1/2 and 1/3 because we can select p and q such that $q^3 > p > nq^2 + q$, note that q is much larger than n. It means the information ratio of our scheme is lower than that of Shamir's SS, which is just the cost our scheme pays for the above extra security.

As mentioned above, Harn's (t,n)-secure secret reconstruction scheme provides the security similar to our scheme, but each participant in Harn's scheme uses multiple shares to form a component before recovering the secret. The scheme uses k polynomials over F_p to generate k shares for each shareholder and requires $kt > n-1$ to guarantee the security, where n is the total number of shareholders, t is the threshold. Consequently, the information ratio of Harn's scheme is $1/k$. In the case of $k > 3$, the information ratio is lower than that of our proposed scheme; In the case of $k = 2$, its information ratio is 1/2 which is a little higher than

that of our scheme, however, $2t > n-1$ means that, to recover the secret, at least one half of shareholders are required to participate in the secret reconstruction. This restriction makes it impractical in applications with a large number of shareholders.

In computation effort, the proposed scheme is almost the same as Shamir's (t,n)-SS except for the extra operation $mod\ q$ in the last step of secret reconstruction.

VII. CONCLUSION

We observed an attack against basic (t,n)-SS schemes, in which a malicious participant, even without a valid share, may obtain the secret when there are more than t participants in the secret reconstruction. To cope with the attack, we first introduced the notion of Randomized Components. A randomized component binds the share with the information of all participants and can protect the share from being exposed; at the same time, randomized components can be used to reconstruct the secret. As one of the applications of Randomized Components, a (t,m,n)-Group Oriented SS scheme was proposed. In the scheme, once m ($m \geq t$) participants form a tightly coupled group by generating RCs; the secret can be recovered only if all participants necessarily have valid shares. The scheme does not depend on any user authentication or share verification mechanism and is unconditionally secure. Analyses show the scheme is asymptotically perfect.

Moreover, the Randomized Component can be viewed as a tool and used in some other scenarios. For example, multi-SSs allow a group of members, with only one or two shares each, to collaborate to reconstruct more secrets. In this case, each participant can use the RC instead of the share to recover each secret while keeping the share secure. Group authentication allows one to authenticate a group of members in only one step rather than authenticate them one by one. The Inseparability of RC can also simplify the design of group authentication.

REFERENCES

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

[2] Blakeley G R. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, New York: AFIPS Press,1979: 313-317.

[3] Boldyreva A. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme, Public key cryptography—PKC 2003. Springer Berlin Heidelberg, 2002: 31-46.

[4] Harn L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature, IEE Proceedings-Computers and Digital Techniques, 1994, 141(5): 307-313.

[5] Desmedt Y G. Threshold cryptography. European Transactions on Telecommunications, 1994, 5(4): 449-458.

[6] Damgård I, Nielsen J B. Universally composable efficient multiparty computation from threshold homomorphic encryption, Advances in Cryptology-Crypto 2003. Springer Berlin Heidelberg, 2003: 247-264.

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

[8] Mignotte, M. How to share a secret. Cryptography. Springer Berlin Heidelberg, 1983. 371-375.

[9] Asmuth C, Bloom J. A modular approach to key safeguarding, IEEE transactions on information theory, 1983, 30(2): 208-210.

[10] Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneously in the presence of faults. Proceedings of 26th IEEE Symp. On Foundations of Computer Science 1985; 383–395.

[11] Feldman P. A practical scheme for non-interactive verifiable secret sharing, Foundations of Computer Science, 1987. 28th Annual Symposium on. IEEE, 1987: 427-438.

[12] Harn L, Lin C. Strong (n, t, n) verifiable secret sharing scheme, Information Sciences 2010; 180(16): 3059–3064.

[13] Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing, Advances in Cryptology-Crypto'91, LNCS 576, Springer-Verlag: 1992; 129–40.

[14] D.R. Stinson and R. Wei. Unconditionally secure proactive secret sharing schemes with combinatorial structures. In SAC '99, volume 1758 of Lecture Notes in Computer Science, Springer-Verlag, 2000; 200–214.

[15] M. Ben-Or, S. Golwasser, and A. Widgerson. Completeness theorems for noncryptographic fault-tolerant distributed computation. In Proceedings of ACM STOC '88, 1988; 1–10.

[16] Lein Harn, Secure secret reconstruction and multisecret sharing schemes with unconditional security, Security and communication networks, 2014,7(3):567-573.

[17] Benelux JC. Secret sharing homomorphism: keeping shares of a secret secret, Advances in Cryptology-Crypto '86, LNCS 263, Springer-Verlag: 1987; 251–260.

[18] Quisquater M, Preneel B, Vandewalle J. On the security of the threshold scheme based on the Chinese remainder theorem, Public Key Cryptography, Springer Berlin Heidelberg, 2002: 199-210.

[19] Ghodosi H, Pieprzyk J, Safavi-Naini R. Remarks on the multiple assignment secret sharing scheme, Information and Communications Security, 1997: 72-80.

[20] Yang C C, Chang T Y, Hwang M S. A (t, n) multi-secret sharing scheme. Applied Mathematics and Computation,2004,151(2): 483-490.

[21] Harn L. Group authentication, Computers, IEEE Transactions on, 2013, 62(9): 1893-1898.

[22] Capocelli R M, De Santis A, Gargano L, et al. On the size of shares for secret sharing schemes, Journal of Cryptology, 1993, 6(3): 157-167.

[23] Goldreich O, Ron D, Sudan M. Chinese remaindering with errors, Proceedings of the thirty-first annual ACM symposium on Theory of computing,ACM, 1999: 225-234.

[24] Yun Song, Zhihui Li, Yongming Li and Jing Li, A new multi-use multi-secret sharing scheme based on the duals of minimal linear codes, Security and Communication Networks, MAR 2014. DOI: 10.1002/sec.972

[25] Martin, Keith M., Challenging the adversary model in secret sharing schemes, Coding and Cryptography II. Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts. 2008. p. 45-63.

Miao Fuyou received his PhD in Computer Science from the University of Science & Technology of China (USTC). Currently, he is an associate professor at the School of Computer Science and Technology, USTC. His research interests include applied cryptography, network security and mobile computing.

Xiong Yan received the PhD degrees from USTC in 1990. He is a professor in the School of Computer Science and Technology, USTC; his research interests include distributed processing, mobile computing and information security.

Wang Xingfu received the Bachelor degree from Beijing Normal University of China in 1988. He is an associate professor in the School of Computer Science and Technology, USTC; his research interests include information security, data management and WSN.

Moaman Badawy, a master student, received the master degree in the School of Computer Science and Technology, USTC in 2014. His research interests include information security and cryptography.