Wireless Pers Commun (2014) 78:271–282
DOI 10.1007/s11277-014-1751-x

Multipartite Secret Sharing Based on CRT

Ching-Fang Hsu · Lein Harn

Published online: 4 April 2014

Abstract Secure communication has become more and more important for system security. Since avoiding the use of encryption one by one can introduce less computation complexity, secret sharing scheme (SSS) has been used to design many security protocols. In SSSs, several authors have studied multipartite access structures, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role. Access structures realized by threshold secret sharing are the simplest multipartite access structures, i.e., unipartite access structures. Since Asmuth–Bloom scheme based on Chinese remainder theorem (CRT) was presented for threshold secret sharing, recently, threshold cryptography based on Asmuth–Bloom secret sharing were firstly proposed by Kaya et al. In this paper, we extend Asmuth–Bloom and Kaya schemes to bipartite access structures and further investigate how SSSs realizing multipartite access structures can be conducted with the CRT. Actually, every access structure is multipartite and, hence, the results in this paper can be seen as a new construction of general SSS based on the CRT. Asmuth–Bloom and Kaya schemes become the special cases of our scheme.

Keywords Secret sharing schemes · Multipartite access structures · Chinese remainder theorem · Asmuth–Bloom secret sharing

This work was supported by the Nature Science Foundation of China (Nos. 61100221, 61003192).

C.-F. Hsu (✉)
Computer School, Central China Normal University, Wuhan 430079, China
e-mail: cherryjingfang@gmail.com

L. Harn
Department of Computer Science Electrical Engineering, University of Missouri,
Kansas City, MO 64110, USA
e-mail: harnl@umkc.edu

1 Introduction

Secret sharing was first introduced by Blakley [1] and Shamir [2] independently in 1979, which was widely used to design security protocols until now (see [3–7]). In a secret sharing scheme (SSS), a dealer distributes a piece of information (called a share) about a secret to each participant such thatauthorized subsets of participants can reconstruct the secret but unauthorized subsets of participants cannot determine the secret. If any unauthorized subset of participants can not obtain any information about the secret, then the scheme is called perfect. The set of authorized subsets of participants is called access structure and the set of unauthorized subsets of participants is called prohibited structure. In the literature, different mathematical tools have been used to design SSSs including Shamir scheme [2] based on polynomial interpolation, Blakley scheme [1] based on hyperplane geometry, Asmuth–Bloom scheme [8] based on the Chinese Remainder Theorem (CRT), Bloom scheme [9] and McEliece et al. scheme [10] based on a linear code. These schemes are all threshold secret sharing (SS), in which any t or more shares can recover the secret, but any $t-1$ or less shares can obtain no information about the secret. Among these SSs, Shamir scheme [2] is the most popular SS. Shamir scheme is very simple and most straightforward but Asmuth–Bloom scheme needs to understand the CRT. In recent years, attention has been devoted to research of CRT-based SSs and applications [11–15].

Information rate (i.e., the ratio between the size of the secret in bits and the maximum size of a share in bits) is usually used to measure the efficiency of a SSS. A scheme is ideal if the information rate is equal to 1. The central research questions in SS are both the construction of efficient SSSs for several classes of access structures, and finding bounds on the possible efficiency that any such scheme can achieve for a certain access structure. In this paper, we deal with multipartite access structures. An access structure is multipartite if its set of participants can be divided into several parts in such a way that all participants in the same part play an equivalent role in the structure. Because of its practical interest, SS for multipartite access structures has been studied by several authors. Since we can always consider as many parts as participants, every access structure is multipartite. More accurately, we can consider in any access structure the partition that is derived from a suitable equivalence relation on the set of participants. Therefore, we are not restricting ourselves to a family of access structures, but we study the general access structures under a different point of view.

Multipartite access structures were first introduced by Shamir [2] in his seminal work, in which weighted threshold access structures were considered. These structures have been studied also in [16,17] and a characterization of the ideal weighted access structures has been presented in [18]. Brickell [19] constructed ideal SSSs for several different kinds of multipartite access structures, called multilevel and compartmented, that had been previously considered by Simmons [20]. Other constructions of ideal schemes for these and other multipartite structures have been presented in [21–24], where some complexity issues related to the construction of those ideal schemes are studied. A complete characterization of ideal bipartite access structures was given in [17] and, independently, in [25,26]. Partial results on the characterization of ideal tripartite access structures have been presented in [18,21,27]. A complete characterization of ideal tripartite access structures were given by Farras and Marti-Farre [28].

Access structure realized by the threshold SS is the simplest multipartite access structure, i.e., unipartite access structures. Most well-known CRT-based SSSs were constructed for threshold access structures, such as Asmuth–Bloom scheme [8], Mignotte's scheme [29] and Kaya's schemes [11,12]. Other CRT-based SS of general access structures in which compartmented access structures and weighted threshold access structures are considered is

proposed in [13]. But these structures in [13] only belong to two types of multipartite access structures [28]. Due to the fact that every access structure can be viewed as multipartite access structure, this motivates us to explore the design of CRT-based sharing schemes realizing multipartite access structures.

Instead of studying SSS realizing a particular family of access structures, in this paper, we study CRT-based general SSS from the perspective of multipartite SSS. We extend both Asmuth–Bloom and Kaya schemes to bipartite access structures and investigate the design of CRT-based SSSs realizing multipartite access structures. The result presented in this paper is a new way to construct CRT-based general secret sharing. Thus, Asmuth–Bloom and Kaya schemes become special cases in our proposed approach. The main contributions of our paper are summarized below:

(a) Using the characterizations of multipartite access structures, we propose the first CRT-based multipartite SSS;
(b) Due to the fact every access structure is multipartite, our result is a new way to construct CRT-based general SS;
(c) Our proposed CRT-based multipartite SSS is perfect and unconditionally secure since there has not any computational assumption based on.
(d) Our proposed scheme can be widely applied to wireless communications to ensure its security.

The rest of this paper is organized as follows: In the next section, we give some preliminaries. In Sect. 3, we propose a multipartite SSS based on CRT. We analyze functional sharing schemes in Sect. 4. Performance evaluation of the proposed scheme is discussed in Sect. 5. We conclude in Sect. 6.

2 Definitions and Preliminaries

In this section we review some basic definitions and notations that will be used through the paper.

2.1 Secret Sharing Schemes

Let $P = \{p_i : 1 \leq i \leq n\}$ be the set of participants. The dealer is denoted by D and we assume $D \notin P$. $\mathcal{K}$ is the secret set (i.e. the set of all possible secrets) and $\mathcal{S}$ is the share set (i.e. the set of all possible shares). Let Γ be a set of subsets of P: this is denoted mathematically by the notation $\Gamma \subseteq 2^P$. The subsets in Γ are those subsets of participants that should be able to reconstruct the secret. Γ is called an access structure and the subsets in Γ are called authorized subsets. Accordingly, $\Delta = 2^P \backslash \Gamma$ is called a prohibited structure and the subsets in Δ are called unauthorized subsets.

When a dealer D wants to share a secret $K \in \mathcal{K}$, he will give each participant a share from $\mathcal{S}$. The shares should be distributed secretly, so no participant knows the share given to another participant. At a later time, a subset of participants will attempt to reconstruct K from the shares they collectively hold. Using Shannon's entropy function, we will say that a scheme is *a perfect SSS* realizing the access structure Γ provided the following two properties are satisfied:

1. *Validity* $H(K|A) = 0, \forall A \in \Gamma$. (Any authorized subset of participants $A \in \Gamma$ who pool their shares together can reconstruct the secret K),

2. *Security* $H(K|A) = H(K), \forall A \in \Delta$. (Any unauthorized subset of participants $A \in \Delta$ who pool their shares together obtain no information on K).

The security of cryptographic schemes/protocols can be classified into two types, computational security and unconditional security. Computational security assumes that the adversary has bounded computing power that limits the adversary solving hard mathematical problem, such as factoring a large composite integer into two primes. Unconditional security means that the security holds even if the adversary has unbounded computing power. If a scheme is unconditional secure [30], then no matter how much computational power the attacker cannot break this scheme. Research on developing cryptographic schemes/protocols with unconditional security has received wide attention recently. In this paper, we propose to design a perfect and unconditionally secure SSS.

Suppose that $B \in \Gamma,\ B \subseteq C \subseteq P$, and the subset C wants to determine K. Since B is an authorized subset, it can already determine K. Hence, the subset C can determine K by ignoring the shares of the participants in $C \backslash B$. Stated another way, a superset of an authorized set is again an authorized set. What this says is that the access structure should satisfy the monotone increasing property

$$\text{if } B \in \Gamma \quad \text{and} \quad B \subseteq C \subseteq P, \quad \text{then} \quad C \in \Gamma.$$

If Γ is an access structure, then $B \in \Gamma$ is a minimal authorized subset if $A \notin \Gamma$ whenever $A \subseteq B,\ A \neq B$. The set of minimal authorized subsets of Γ is denoted Γ_0 and is called the basis of Γ. Since Γ consists of all subsets of P that are supersets of a subset in the basis $\Gamma_0,\ \Gamma$ is determined uniquely as a function of Γ_0. Expressed mathematically, we have

$$\Gamma = \{C \subseteq P :\ B \subseteq C,\ B \in \Gamma_0\}.$$

Symmetrically, the prohibited structure Δ should satisfy the monotone decreasing property

$$\text{if } B \in \Delta \quad \text{and} \quad C \subseteq B \subseteq P, \quad \text{then} \quad C \in \Delta.$$

We say $B \in \Delta$ is a maximal unauthorized subset if $A \notin \Delta$ whenever $B \subseteq A,\ A \neq B$.The set of maximal unauthorized subsets of Δ is denoted Δ_1. Since Δ consists of all subsets of P that are subsets of a subset in $\Delta_1,\ \Delta$ is determined uniquely as a function of Δ_1. Expressed mathematically, we have

$$\Delta = \{C \subseteq P :\ C \subseteq B,\ B \in \Delta_1\}.$$

The efficiency of a SSS is measured by the information rate. Suppose $\mathcal{F}$ is a set of distribution rules for a SSS. For $1 \leq i \leq n$, define

$$\mathcal{S}_i = \{f(p_i) : f \in \mathcal{F}\}.$$

f represents a possible distribution rule and $f(p_i)$ is the share given to p_i. $\mathcal{S}_i$ represents the set of possible shares that p_i might receive, of course, $\mathcal{S}_i \subseteq \mathcal{S}$. Now, since the secret K comes from a finite set $\mathcal{K}$, we can think of K as being represented by a bit string of length $\log_2 |\mathcal{K}|$ by using a binary encoding, for example. In a similar way, a share given to p_i can be represented by a bit string of length $\log_2 |\mathcal{S}_i|$. Intuitively, p_i receives $\log_2 |\mathcal{S}_i|$ bits of information (in his or her share), but the information content of the secret is $\log_2 |\mathcal{K}|$ bits. The information rate of the scheme denoted by ρ is the ratio

$$\rho = \frac{\log_2 |\mathcal{K}|}{\log_2 \max\{|\mathcal{S}_i|\}}$$

2.2 Multipartite Access Structures

We write $\mathcal{P}(P)$ for the power set of the set P. An r-partition $\Omega = \{P_1, \ldots, P_r\}$ of a set P is a disjoint family of r nonempty subsets of P with $P = P_1 \cup \cdots \cup P_r$. Let $\Lambda \subseteq \mathcal{P}(P)$ be a family of subsets of P. For a permutation σ on P, we define $\sigma(\Lambda) = \{\sigma(A) : A \in \Lambda\} \subseteq \mathcal{P}(P)$. A family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is said to be Ω-partite if $\sigma(\Lambda) = \Lambda$ for every permutation σ such that $\sigma(P_i) = P_i$ for every $P_i \in \Omega$. We say that Λ is r-partite if it is Ω-partite for some r-partition Ω. These concepts can be applied to access structures, which are actually families of subsets.

For every integer $r \geq 1$, we consider the set $J_r = \{1, \ldots, r\}$. Let $\mathbb{Z}_+^r$ denote the set of vectors $u = (u_1, \ldots, u_r) \in \mathbb{Z}^r$ with $u_i \geq 0$ for every $i \in J_r$. For a partition $\Omega = \{P_1, \ldots, P_r\}$ of a set P and for every $A \subseteq P$ and $i \in J_r$, we define $\Omega_i(A) = |A \cap P_i|$. Then the partition Ω defines a mapping $\Omega : \mathcal{P}(P) \to \mathbb{Z}_+^r$ by considering $\Omega(A) = (\Omega_1(A), \ldots, \Omega_r(A))$. If $\Lambda \subseteq \mathcal{P}(P)$ is Ω-partite, then $A \in \Lambda$ if and only if $\Omega(A) \in \Omega(\Lambda)$. That is, Λ is completely determined by the partition Ω and the set of vectors $\Omega(\Lambda) \subset \mathbb{Z}_+^r$.

If $u, v \in \mathbb{Z}_+^r$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J_r$, and we write $u < v$ if $u \leq v$ and $u \neq v$. The vector $w = u \vee v$ is defined by $w_i = \max(u_i, v_i)$. The modulus of a vector $u \in \mathbb{Z}_+^r$ is $|u| = u_1 + \cdots + u_r$. For every subset $X \subseteq J_r$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^{|X|}$ and $|u(X)| = \sum_{i \in X} u_i$.

2.3 Asmuth–Bloom SSS

The Asmuth–Bloom SSS has shares distribution and secret reconstruction phases for unipartite access structures as follows:

Shares Distribution To distribute n shares of a secret K among the set of participants $P = \{p_i : 1 \leq i \leq n\}$, the dealer D does the following:

1. A set of integers $\{p,\ m_1 < m_2 < \cdots < m_n\}$, where $0 \leq K < p$, is chosen subject to the following:

$$\begin{aligned} \gcd(m_i, m_j) &= 1 \quad \text{for } i \neq j, \\ \gcd(p, m_i) &= 1 \quad \text{for all } i, \\ \prod_{i=1}^{t} m_i &> p \prod_{i=1}^{t-1} m_{n-i+1}. \end{aligned} \tag{1}$$

2. Let $M = \prod_{i=1}^{t} m_i$. The dealer computes

$$y = K + ap,$$

where a is a positive integer generated randomly subject to the condition that $0 \leq y < M$.

3. The share of the ith participant, $1 \leq i \leq n$, is

$$y_i = y \bmod m_i.$$

Secret Construction Assume C is a coalition of t participants to construct the secret. Let $M_C = \prod_{i \in C} m_i$.

1. Given the system

$$y \equiv y_i \pmod{m_i}$$

for $i \in C$, solve y in $GF(M_C)$ uniquely using the CRT.

2. Compute the secret as

$$K = y \bmod p.$$

According to the CRT, y can be determined uniquely in $GF(M_C)$. Since $y < M \leq M_C$, the solution is also unique in $GF(M)$.

3 The Proposed Schemes

In this section we extend the Asmuth–Bloom SSS from unipartite to bipartite access structures and further investigate how SSSs realizing multipartite access structures can be conducted with the CRT. At the same time, the validity and security proofs of our scheme are given.

3.1 Bipartite SS Based on CRT

Let an access structure Γ be Ω-partite for a partition $\Omega = \{P_1, P_2\}$ of $P = \{p_i : 1 \leq i \leq n\}$, where $|P_1| = n_1$, $|P_2| = n_2$ and $n_1 + n_2 = n$. Then the partition Ω defines a mapping $\Omega : \mathcal{P}(P) \to \mathbb{Z}_+^2$. Let Γ_0 and Δ_1 be the corresponding minimal access structure and maximal prohibited structure respectively, from which we can determine $\Omega(\Gamma_0) \subset \mathbb{Z}_+^2$ and $\Omega(\Delta_1) \subset \mathbb{Z}_+^2$.

The secret sharing scheme for Γ has shares distribution and secret reconstruction phase as follows:

Shares Distribution To distribute n shares of a secret K among $P = \{p_i : 1 \leq i \leq n\}$, the dealer D does the following:

1. A set of integers $\{p,\ m_1 < m_2 < \cdots < m_{n_1},\ m_{n_1+1} < m_{n_1+2} < \cdots < m_n\}$, where $0 \leq K < p$, is chosen subject to the following:

$$\begin{gathered}
\gcd(m_i, m_j) = 1 \quad \text{for } i \neq j, \\
\gcd(p, m_i) = 1 \quad \text{for all } i, \\
M_1 = \min\left(\prod_{i=1}^{u_1} m_i \prod_{j=1}^{u_2} m_j,\ \text{for all } (u_1, u_2) \in \Omega(\Gamma_0)\right), \\
M_2 = \max\left(\prod_{i=1}^{v_1} m_{n_1+i-1} \prod_{j=1}^{v_2} m_{n_2+j-1},\ \text{for all } (v_1, v_2) \in \Omega(\Delta_1)\right), \\
M_1 > pM_2. \qquad (2)
\end{gathered}$$

2. The dealer computes

$$y = K + ap$$

where a is a positive integer generated randomly subject to the condition that $0 \leq y < M_1$.

3. The n_1 shares,

$$y_i = y \bmod m_i \quad \text{for } i = 1, \ldots, n_1,$$

are distributed randomly to participants in P_1 with one to one correspondence, and the n_2 shares,

$$y_{n_1+j} = y \bmod m_{n_1+j} \quad \text{for } j = 1, \ldots, n_2,$$

are distributed randomly to participants in P_2 with one to one correspondence. Hence, the shares distribution defines a mapping $f : \{y_1, \ldots, y_n\} \to P$.

Secret Construction Assume C is a coalition of participants in Γ to construct the secret. Let $M_C = \prod_{f(y_i)\in C} m_i$.

1. Given the system

$$y \equiv y_i \pmod{m_i}$$

for $f(y_i) \in C$, solve y in $GF(M_C)$ uniquely using the CRT.
2. Compute the secret as

$$K = y \bmod p.$$

Theorem 1 *The proposed bipartite SSS is a perfect SSS.*

Proof According to the *Chinese remainder theorem (CRT)* [31], in which given the following system of equations as

$$\begin{aligned} x &= s_1 \bmod p_1; \\ x &= s_2 \bmod p_2; \\ &\vdots \\ x &= s_t \bmod p_t, \end{aligned}$$

there is one unique solution as $x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \cdot s_1 \bmod N$, where $\frac{N}{p_i} \cdot y_i \bmod p_i = 1$, and $N = p_1 \cdot p_2 \cdot \ldots \cdot p_t$, if all moduli are pairwise coprime (i.e., $\gcd(p_i, p_j) = 1$ for every $i \neq j$).

From the above CRT, in our bipartite scheme y can be determined uniquely in $GF(M_C)$. Since $y < M_1 \leq M_C$, the solution is also unique in $GF(M_1)$. Hence, it holds that $H(K|C) = 0, \forall C \in \Gamma$. (Any authorized subset of participants $C \in \Gamma$ who pool their shares together can reconstruct the secret K).

At the same time, we assume that a coalition C' of malicious participants in Δ has gathered. Let y' be the unique solution for y in $GF(M_{C'})$. According to (2) and $M_2 > M_{C'}$, we obtain $M_1/M_{C'} > p$, hence $y' + jM_{C'}$ is smaller than M_1 for $0 \leq j < p$. Since $\gcd(p, M_{C'}) = 1$, all $(y' + jM_{C'}) \bmod p$ are distinct for $0 \leq j < p$, and there are p of them. That is, K can be any integer from $GF(p)$, and the coalition C' obtains no information on K. Hence, it holds that $H(K|C') = H(K), \forall C' \in \Delta$. (Any unauthorized subset of participants $C' \in \Delta$ who pool their shares together obtain no information on K).

Therefore, according to the definition in Sect. 2.1, the proposed bipartite SS is a perfect SSS. □

As a consequence, based on the CRT, the SSS realizing bipartite access structures is constructed.

3.2 Multipartite SS Based on CRT

This construction method can be extended to the general case, i.e., the SSSs realizing multipartite access structures.

Let an access structure Γ be Ω-partite for a partition $\Omega = \{P_1, \ldots, P_r\}$ of $P = \{p_i : 1 \leq i \leq n\}$, where $|P_1| = n_1, \ldots, |P_r| = n_r$ and $n_1 + \cdots + n_r = n$. Then the

partition Ω defines a mapping $\Omega : \mathcal{P}(P) \to \mathbb{Z}_+^r$. Let Γ_0 and Δ_1 be the corresponding minimal access structure and maximal prohibited structure respectively, from which we can determine $\Omega(\Gamma_0) \subset \mathbb{Z}_+^r$ and $\Omega(\Delta_1) \subset \mathbb{Z}_+^r$.

The SSS for Γ has shares distribution and secret reconstruction phase as follows:

Shares Distribution To distribute n shares of a secret K among $P = \{p_i : 1 \le i \le n\}$, the dealer D does the following:

1. A set of integers $\{p,\ m_1 < \cdots < m_{n_1},\ m_{n_1+1} < \cdots < m_{n_1+n_2},\ \ldots,\ m_{n-n_r+1} < \cdots < m_n\}$, where $0 \le K < p$, is chosen subject to the following:

$$\begin{aligned} &\gcd(m_i, m_j) = 1 \text{ for } i \neq j, \\ &\gcd(p, m_i) = 1 \text{ for all } i, \\ M_3 &= \min\left(\prod_{j=1}^{r}\prod_{i=1}^{u_j} m_i,\ \text{for all } (u_1, \ldots, u_r) \in \Omega(\Gamma_0)\right), \\ M_4 &= \max\left(\prod_{j=1}^{r}\prod_{i=1}^{v_j} m_{n_j+i-1},\ \text{for all } (v_1, \ldots, v_r) \in \Omega(\Delta_1)\right), \\ &M_3 > pM_4. \end{aligned} \tag{3}$$

2. The dealer computes

$$y = K + ap$$

where a is a positive integer generated randomly subject to the condition that $0 \le y < M_3$.

3. For $j = 1, \ldots, r$, the n_j shares,

$$y_i = y \bmod m_i \quad \text{for } i = 1, \ldots, n_j,$$

are distributed randomly to participants in P_j with one to one correspondence. Hence, the shares distribution defines a mapping $f : \{y_1, \ldots, y_n\} \to P$.

Secret Construction Assume C is a coalition of participants in Γ gathered to construct the secret. Let $M_C = \prod_{f(y_i)\in C} m_i$.

1. Given the system

$$y \equiv y_i \pmod{m_i}$$

for $f(y_i) \in C$, solve y in $GF(M_C)$ uniquely using the CRT.

2. Compute the secret as

$$K = y \bmod p.$$

Theorem 2 *The proposed SS realizing multipartite access structures is a perfect SSS.*

Proof According to the *CRT* [31], in which given the following system of equations as

$$\begin{aligned} x &= s_1 \bmod p_1; \\ x &= s_2 \bmod p_2; \\ &\vdots \\ x &= s_t \bmod p_t, \end{aligned}$$

there is one unique solution as $x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \cdot s_1 \bmod N$, where $\frac{N}{p_i} \cdot y_i \bmod p_i = 1$, and $N = p_1 \cdot p_2 \cdot \ldots \cdot p_t$, if all moduli are pairwise coprime (i.e., $\gcd(p_i, p_j) = 1$ for every $i \neq j$).

From the above CRT, we obtain that in our multipartite scheme y can be determined uniquely in $GF(M_C)$. Since $y < M_1 \leq M_C$, the solution is also unique in $GF(M_1)$. Hence, it holds that $H(K|C) = 0, \forall C \in \Gamma$ (Any authorized subset of participants $C \in \Gamma$ who pool their shares together can reconstruct the secret K).

At the same time, we assume that a coalition C' of malicious participants in Δ has gathered. Let y' be the unique solution for y in $GF(M_{C'})$. According to (3) and $M_4 > M_{C'}$, we obtain $M_3/M_{C'} > p$, hence $y' + jM_{C'}$ is smaller than M_3 for $0 \leq j < p$. Since $\gcd(p, M_{C'}) = 1$, all $(y' + jM_{C'}) \bmod p$ are distinct for $0 \leq j < p$, and there are p of them. That is, K can be any integer from $GF(p)$, and the coalition C' obtains no information on K. Hence, it holds that $H(K|C') = H(K), \forall C' \in \Delta$ (Any unauthorized subset of participants $C' \in \Delta$ who pool their shares together obtain no information on K).

Therefore, according to the definition in Sect. 2.1, the proposed multipartite SS is a perfect SSS. □

As a consequence, based on the CRT, the SSS realizing multipartite access structures is constructed.

Remark 1 In a verifiable SSS the validity of the shares can be verified, hence participants are not able to cheat. Based on our scheme, we can further construct an ideal verifiable multi-SSS by adding the existing verifiability methods where the intractability of discrete logarithm problem is frequently used.

4 Functional Sharing Schemes Based on Our Scheme

Besides dealing with the problem of sharing a secret, a further requirement of a cryptosystem can be that the subject function (e.g., a digital signature) should be computable without the participants disclosing their secret shares. This is known as the functional sharing problem. A function sharing scheme (FSS) requires distributing the function's computation according to the underlying SSS such that each part of the computation can be carried out by a different participant and then the partial results can be combined to yield the functional value without disclosing the individual secrets. Several protocols for functional sharing [3–7] have been proposed in the literature. Nearly all existing solutions for functional sharing are based on the Shamir SSS. In [11], Kaya et al. firstly show how sharing of threshold cryptographic functions can be achieved using the Asmuth–Bloom SSS. They proposed two novel FSSs, one for the RSA signature and the other for the ElGamal decryption functions, both based on the Asmuth–Bloom SSS. Since our scheme is the extension of Asmuth–Bloom SSS, the construction of FSSs based on our scheme, such as FSSs for the RSA signature and the ElGamal decryption functions, may be similar to Kaya et al.'s scheme. Due to this fact, we will not describe it in details. As a consequence, cryptography based on our SSS can extend Kaya scheme from the threshold case to the general case.

5 Discussion of Our Scheme

In our scheme, the information rate is

$$\frac{\log_2 p}{\log_2 \max\{m_i, \text{ for} 1 \leq i \leq n\}},$$

where the secret and the shares are chosen from finite fields $GF(p)$ and $GF(m_i)$ respectively.

Except the generation algorithm of the set of integers $\{p,\ m_1 < \cdots < m_{n_1},\ m_{n_1+1} < \cdots < m_{n_1+n_2}, \ldots, m_{n-n_r+1} < \cdots < m_n\}$, the performance of our scheme is the same as the performance of Asmuth–Bloom SSS. The monotone increasing property of access structures, the monotone decreasing property of prohibited structures and estimates of the density of primes show that one could find primes $m_i (1 \leq i \leq n)$ and p to satisfy (3). To find composite $m_i (1 \leq i \leq n)$ and p is still easier. A specific algorithm for generating $m_i (1 \leq i \leq n)$ and p is deferred to our future work.

6 Conclusion

In this paper, we extend Asmuth–Bloom and Kaya schemes to bipartite access structures and further present how SSSs realizing multipartite access structures can be conducted with the CRT. Due to the fact that every access structure is multipartite, the results in this paper can be seen as a new construction of general SS based on the CRT. Asmuth–Bloom and Kaya schemes become the special cases of our scheme.

References

1. Blakley, G. R. (1979). Safeguarding cryptographic keys. In *Proceedings of AFIPs I979 national computer conference, New York* (Vol. 48, pp. 313–317).
2. Shamir, A. (1979). How to share a secret. *Communication of the ACM*, *22*(11), 612–613.
3. Guo, C., & Chang, C.-C. (2012). An authenticated group key distribution protocol based on the generalized Chinese remainder theorem. *International Journal of Communication System*. doi:10.1002/dac.2348.
4. He, D., Chen, C., Ma, M., Chan, S., & Bu, J. (2011). A secure and efficient password-authenticated group key exchange protocol for mobile ad hoc networks. *International Journal of Communication System*. doi:10.1002/dac.1355.
5. Xie, Q. (2012). A new authenticated key agreement for session initiation protocol. *International Journal of Communication System*, *25*, 47–54. doi:10.1002/dac.1286.
6. Chang, C.-C., Cheng, T.-F., & Wu, H.-L. (2012). An authentication and key agreement protocol for satellite communications. *International Journal of Communication System*. doi:10.1002/dac.2448.
7. Li, J.-S., & Liu, K.-H. (2011). A hidden mutual authentication protocol for low-cost RFID tags. *International Journal of Communication System*, *24*, 1196–1211. doi:10.1002/dac.1222.
8. Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, *29*(2), 208–210.
9. Bloom, J. R. (1981). Threshold schemes and error-correcting codes. In *Abstract of papers presented to America Mathematical Society* (Vol. 2, p. 230).
10. McEliece, R. J., & Sarwate, D. V. (1981). On sharing secret and Reed–Solomon codes. *Communication ACM*, *24*, 583–584.
11. Kaya, K., & Selçuk, A. A. (2007). Threshold cryptography based on Asmuth–Bloom secret sharing. *Information Sciences*, *177*, 4148–4160.
12. Kaya, K., & Selçuk, A. A. (2008). Robust threshold schemes based on the Chinese remainder Ttheorem. In *Advances in cryptography—AFRICACRYPT 2008. Lecture notes in computer sciences* (Vol. 5023, pp. 94–108).
13. Iftene, S. (2007). General secret sharing based on the Chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science*, *186*, 67–84.
14. Harn, L., Fuyou, M., & Chang, C. C. (2013). Verifiable secret sharing based on the Chinese remainder theorem. *Security and Communication Networks*. doi:10.1002/sec.807.
15. Liu, Y., Harn, L., & Chang, C.-C. (2014). An authenticated group key distribution Mechanism using theory of numbers. *International Journal of Communication Systems*.
16. Morillo, P., Padro, C., Saez, G., & Villar, J. L. (1999). Weighted threshold secret sharing schemes. *Information Processing Letters*, *70*, 211–216.

17. Padro, C., & Saez, G. (2000). Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, *46*, 2596–2604.
18. Beimel, A., Tassa, T., & Weinreb, E. (2005). Characterizing ideal weighted threshold secret sharing. In *Second theory of cryptography conference, TCC 2005. Lecture notes in computer science* (Vol. 3378, pp. 600–619).
19. Brickell, E. F. (1989). Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, *9*, 105–113.
20. Simmons, G. J. (1990). How to (really) share a secret. In *Advances in cryptology CRYPTO '88. Lecture notes in computer science* (Vol. 403, pp. 390–448).
21. Herranz, J., & Sáez, G. (2006). New results on multipartite access structures. *IEE Proceedings-Information Security, 153*(4), 153–162.
22. Ng, S.-L. (2006). Ideal secret sharing schemes with multipartite access structures. *IEE Proceedings-Communications*, *153*, 165–168.
23. Tassa, T. (2004). Hierarchical threshold secret sharing. In *First theory of cryptography conference, TCC 2004. Lecture notes in computer science* (Vol. 2951, pp. 473–490).
24. Tassa, T., & Dyn, N. (2006). Multipartite secret sharing by bivariate interpolation. In *33rd international colloquium on automata, languages and programming, ICALP 2006. Lecture notes in computer science* (Vol. 4052, pp. 288–299).
25. Ng, S.-L. (2003). A representation of a family of secret sharing matroids. *Designs, Codes and Cryptography*, *30*, 5–19.
26. Ng, S.-L., & Walker, M. (2001). On the composition of matroids and ideal secret sharing schemes. *Designs, Codes and Cryptography*, *24*, 49–67.
27. Collins, M. J. (2002). A note on ideal tripartite access structures. *IACR Cryptology ePrint Archive, 2002*, 193.
28. Farràs, O., Martí-Farré, J., & Padró, C. (2012). Ideal multipartite secret sharing schemes. *Journal of Cryptology*, *25*(3), 434–463.
29. Mignotte, M. (1983). How to share a secret. In T. Beth (Ed.), *Cryptography-proceedings of the workshop on cryptography, Burg Feuerstein, 1982. Lecture notes in computer science* (Vol. 149, pp. 371–375).
30. Chaum, D., Crépeau, C., & Damgard, I. (1998). Multiparty unconditionally secure protocols[C]. In *Proceedings of the twentieth annual ACM symposium on theory of computing* (pp. 11–19). ACM.
31. Cohen, H. (2000). *A course in computational algebraic number theory, 4th ed., Ser. Graduate texts in mathematics*. Berlin: Springer.

Ching-Fang Hsu was born in Hubei, China, on November 22, 1978. She received the M.Eng. and the Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010 respectively. From September 2010 to March 2013, she was a research fellow at the Huazhong University of Science and Technology. She is currently an Assistant Professor at Central China Normal University, Wuhan, China. Her research interests are in cryptography and network security, especially in secret sharing and its applications.

Lein Harn received the B.S. degree in electrical engineering from the National Taiwan University in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota in 1984. In 1984, he joined the Department of Electrical and Computer Engineering, University of Missouri- Columbia as an assistant professor, and in 1986, he moved to Computer Science and Telecommunication Program (CSTP), University of Missouri, Kansas City (UMKC). While at UMKC, he went on development leave to work in Racal Data Group, Florida for a year. His research interests include cryptography, network security, and wireless communication security. He has published a number of papers on digital signature design and applications and wireless and network security. He has written two books on security. He is currently investigating new ways of using secret sharing in various applications.