Multilevel Threshold Secret Sharing using the Chinese Remainder Theorem

Oğuzhan Ersoy[*‡], Kamer Kaya[**], Kerem Kaşkaloğlu[***]

[*]Department of Intelligent Systems, Delft University of Technology, The Netherlands.
[**]Computer Science and Engineering, Sabancı University, Turkey.
[***]College of Engineering and Technology, American University of the Middle East, Kuwait.
[‡] Corresponding Author; e-mail: o.ersoy@tudelft.nl

ORCID ID: 0000-0002-6428-4212, 0000-0001-8678-5467, 0000-0002-0023-0514
Research Paper Received: 23.04.2019 Revised: 04.06.2019 Accepted: 14.06.2019

Abstract—In *multilevel secret sharing*, a secret is shared among a set of hierarchically organized participants in a way that the members of the superior compartments are more powerful and can replace the participants of an inferior one to form an authorized coalition during secret reconstruction. In this work, we first show that the only existing multilevel threshold secret sharing scheme based on the Chinese Remainder Theorem (CRT) is not secure and fails to work with certain natural threshold settings on compartments. As the main contribution, we propose a secure CRT-based scheme that works for all threshold settings. In the proposed scheme, we employ a refined version of Asmuth-Bloom secret sharing with a special and generic Asmuth-Bloom sequence called the *anchor sequence*.

Keywords—Secret sharing, multilevel cryptography, Chinese Remainder Theorem.

1. Introduction

The concept of secret sharing is being used in many cryptographic protocols such that group key aggreement and multi-party computation schemes which have many important applications in practice. As independently proposed by Shamir [20] and Blakley [4], a *secret-sharing scheme* (SSS) involves a *dealer* who has a *secret* s, a set of *participants* $\mathcal{U}$ that the secret is shared amongst, and a collection $\mathcal{A}$ of the authorized subsets of the $\mathcal{U}$ which is called the *access structure*. In a SSS, the dealer distributes the shares to the participants such that only the subsets in $\mathcal{A}$ can reconstruct the secret from the corresponding shares. Furthermore, a SSS is called *perfect* if all the subsets not in $\mathcal{A}$ will have the same probability of guessing the secret as if they had no shares. We refer the reader to a comprehensive survey [2] for practical applications of secret sharing such as building authentication protocols which stay secure even under the leakage of a number of servers' data. In *threshold secret sharing*, the access structure is defined by a threshold on the cardinality of authorized subsets: a (t, n)-SSS refers to a scheme in which any t out of n participants can recover the secret.

Given the universal participant set $\mathcal{U}$, a partition of $\mathcal{U}$ into disjoint subsets, i.e., *compartments*, is used to define a *multipartite access structure* on $\mathcal{U}$. Unlike

traditional threshold secret sharing that has only one threshold, different thresholds and conditions may be imposed for different compartments to define the access structure. Although there exist methods for general access structures, e.g., [12], [11], [5], the schemes designed for specific access structures are almost always more efficient and hence, more practical. Such an access structure which has applications in practice is the *multilevel/hierarchical access structure*, a special form of the multipartite case, that employs a hierarchy between the compartments where the members of a superior compartment are more powerful and can replace the participants of an inferior one following the hierarchy definition of Simmons [21] that is further studied in [7].

CRT-based secret sharing schemes and their variants have been popular in recent years; for example, in 2014, Kaya and Selçuk [15] proposed a CRT-based joint-random SSS, and Guo and Chang [8] proposed an authenticated group key distribution protocol based on the generalized CRT. Later, Liu et al. [16] pointed out the security problems of Guo and Chang's protocol and proposed a simpler scheme based on CRT. Moreover, there have been several proposals for CRT-based verifiable secret sharing scheme [17], [13], which are analyzed in [6].

In a recent work of Harn and Fuyou [9], the first CRT-based (disjunctive) multilevel threshold SSS is proposed for an access structure involving a hierarchy of compartments as in the definition of Simmons. In this work, we focus on the same problem and propose a novel CRT-based multilevel threshold SSS. Our contribution is four-fold:

1 We show that the Harn-Fuyou scheme cannot be applied (i.e., is not well-defined) for all the access structures $\mathcal{A}$ in the multilevel setting. Furthermore it is not secure, i.e., the secret can be reconstructed by an unauthorized coalition that is not in $\mathcal{A}$.
2 By using *anchor Asmuth-Bloom sequences*, we propose a simpler and novel CRT-based threshold SSS for the multilevel, disjunctive access structures which does not suffer from these drawbacks.
3 By using anchor sequences, we propose the first CRT-based threshold SSS for the multilevel, conjunctive access structures.
4 We show that the proposed schemes can be adopted to build function sharing schemes which have many applications such as multiparty encryption and digital signatures.

After covering some preliminary definitions and schemes in Section 2, we point out some shortcomings of the Harn-Fuyou scheme in Section 3. We present our conjunctive and disjunctive multilevel secret sharing schemes in Section 4. Section 5 concludes the paper.

2. Background and Preliminaries

Given the following system of congruences

$$\begin{aligned} x &= s_1 \, mod \, p_1, \\ x &= s_2 \, mod \, p_2, \\ &\vdots \\ x &= s_n \, mod \, p_n, \end{aligned}$$

the Chinese Remainder Theorem states that there is a unique solution $x \in \mathbb{Z}_P$ such that

$$x = \sum_{i=1}^{n} \frac{P}{p_i} I_i s_i \bmod P,$$

where $P = lcm(p_1, p_2, \ldots, p_n)$ and I_i is the inverse of P/p_i in modulo p_i, i.e., $\frac{P}{p_i} I_i \mod p_i = 1$. Thus when the p_i values are chosen pairwise coprime (or all prime) P becomes $p_1 p_2 \ldots p_n$. The reason of choosing pairwise coprime p_i values is to guarantee the uniqueness of the solution.

Apart from Shamir's Lagrange interpolation-based scheme [20] and Blakley's scheme utilizing the idea that any n nonparallel $(n-1)$-dimensional hyperplanes intersect at a specific point [4], Chinese Remainder Theorem (CRT)-based threshold schemes by Mignotte [18] and Asmuth and Bloom [1] also exist. While Mignotte's (t, n) scheme is not perfect in the sense that less than t shares reveal information about the secret, Asmuth-Bloom's scheme attains a better security level with a careful choice of parameters. Here we briefly define Mignotte's and Asmuth-Bloom's SSSs and refer the reader to [19] for an extensive study on the security of CRT based SSSs.

2.1. Mignotte's secret sharing

In Mignotte's SSS with n participants and a threshold $t \leq n$, given the sequence of pairwise coprime positive integers $p_1 < p_2 < \ldots < p_n$, the secret s is chosen s.t.

$$\prod_{i=1}^{t-1} p_{n-i+1} < s < \prod_{i=1}^{t} p_i.$$

Here the product on the left hand side is the maximum CRT modulo an adversarial, unauthorized coalition can obtain with less than t shares. The one the right is the minimum such value an authorized coalition can have.

The share of each participant u_i is $s_i = s \mod p_i$. Since s is greater than the product of the greatest $t-1$ primes, a set of $t-1$ participants cannot (uniquely) reconstruct the secret. On the other hand, t or more participants can reconstruct s since it is smaller than the product of the smallest t primes. As all the parameters except the private shares s_i are public, the secret reconstruction is a straightforward application of CRT. It is important to notice that the Mignotte (t, n)-threshold secret-sharing scheme is not perfect in the sense that a set of less than t shares reveals some information (w.r.t. a modulo) about the secret.

2.2. Asmuth-Bloom's secret sharing

Let p_0 be a prime which defines the secret space and $s \in \mathbb{Z}_{p_0}$ be the secret. Let M be $\prod_{i=1}^{t} p_i$, and $p_0 < p_1 < p_2 < \ldots < p_n$ be a sequence of primes such that

$$p_0 \prod_{i=1}^{t-1} p_{n-i+1} < M. \tag{1}$$

To share the secret, the dealer first chooses a random positive integer α such that $0 \leq y = s + \alpha p_0 < M$. The share of the participant u_i is equal to $s_i = y \mod p_i$. Let $A \in \mathcal{A}$ be a coalition of t participants and let $M_A = \prod_{i \in A} p_i$. Then the shared integer y can be uniquely reconstructed in $\mathbb{Z}_{M_A}$ since $y < M \leq M_A$. Hence, the secret s can later be obtained by computing $y \mod p_0$.

Asmuth Bloom's SSS has better security properties when compared to Mignotte's. When a non-authorized coalition A' with $t-1$ shares tries to reconstruct the secret, due to (1), there will be at least $\frac{M}{M_{A'}} > p_0$ candidates for y. Furthermore, since p_0 is relatively prime with $M_{A'}$, there will be at least one y candidate valid for each possible secret candidate in $\mathbb{Z}_{p_0}$. Thus, $t-1$ or fewer participants cannot narrow down the secret space. However, since the number of y candidates for two secret candidates may differ (by one), the secret candidates are not equally probable, resulting in an imperfect distribution [14]. To solve this problem, Kaya et al. proposed to use the equation

$${p_0}^2 \prod_{i=1}^{t-1} p_{n-i+1} < M \tag{2}$$

instead of (1), which forms a *statistically secure scheme* with respect to the definition given in [2]. We will follow the same idea in this work. Even with (1), the proposed scheme will be secure in the

sense that the secret can be any of the candidates in $\mathbb{Z}_{p_0}$ from the adversary's point of view. However, the probability of a candidate being a secret may differ slightly (depending on $\frac{M}{M_{A'}}$) for two candidates.

TABLE 1
Notation

Notation	Explanation
$\mathcal{U}$	The set of participants.
$\mathcal{A}$	The collection of authorized subsets of $\mathcal{U}$.
n	The number of total participants.
m	The number of levels\compartments.
u_k	The kth participant.
L_i	The ith level\compartment.
n_i	The number of participants in L_i.
t_i	The threshold, the minimum number of users required to construct the secret for level L_i.
U_i	$\sum_{k=1}^{i} L_k$.
s	The secret to be shared.
s_k^j	$y_j \bmod p_k$, the share of user $u_k \in L_j$.
Δs_k^i	$y_i - h_k(s_k^j, i) \bmod p_k$, the public information of user u_k for L_i.
M_i	The modulus of smallest t_i ones, $\prod_{j=1}^{t_i} p_j$.
M_A	The modulus of coalition A, $\prod_{u_i \in A} p_i$.
p_0	A prime; specifies the domain of $s \in \mathbb{Z}_{p_0}$.
p_i	The prime modulus for user i.
y_i	$s_i + \alpha_i \cdot p_0$, where α_i is the blinding factor.

For the rest of the paper, we will use the notation given in Table 1.

2.3. Multilevel threshold secret sharing

We employ Simmons' multilevel threshold secret sharing (MTSS) definition, which assumes a multipartite access structure and a hierarchy on it such that the members of the superior compartments (higher-level members) can replace the ones from inferior compartments (lower-level members). Throughout the paper, the terms *level* and *compartment* are used interchangeably for our context.

Let $\mathcal{U}$ be a set of all participants composed of disjoint subsets called *levels*, i.e, $\mathcal{U} = \bigcup_{i=1}^{m} L_i$ where $L_i \cap L_j = \emptyset$ for all $1 \leq i, j \leq m$. Here L_1 is the highest level and L_m is the lowest one. Thus, a participant in L_1 can take place of all other participants, and a participant in L_m can only take place of the participants in L_m. Let the integers $0 < t_1 < t_2 < \ldots < t_m$ be a sequence of threshold values such that $t_j \leq |L_1| + |L_2| + \ldots + |L_j|$ for all $1 \leq j \leq m$. When considered in the disjunctive setting, the access structure is defined by using the disjunction of the m conditions on m compartments as described below[1]:

Definition 1. *A (t, n) disjunctive multilevel threshold secret sharing scheme assigns each participant $u \in \mathcal{U}$ a secret share such that the access structure is defined as*

$$\mathcal{A} = \{A \subset \mathcal{U} : \exists i \in \{1, 2, \ldots, m\} \text{ s.t. } |A \cap (\bigcup_{j=1}^{i} L_j)| \geq t_i\}.$$

On the other hand, under the conjunctive setting, all the threshold conditions of the compartments need to be satisfied. We use the same access structure definition as of [22].

Definition 2. *A (t, n) conjunctive multilevel threshold secret sharing scheme assigns each participant $u \in \mathcal{U}$ a secret share such that the access structure is defined as*

$$\mathcal{A} = \{A \subset \mathcal{U} : \forall i \in \{1, 2, \ldots, m\} \text{ s.t. } |A \cap (\bigcup_{j=1}^{i} L_j)| \geq t_i\}.$$

1. Simmons gave the following example: **In the disjunctive setting**, assume that a bank transfer requires authorization where *two vice presidents (VP)* or *three senior tellers (ST)* are required for authorization. In this example, there are two compartments (VPs and STs) where a VP can replace an ST. That is *a VP together with two STs* are able to approve the transfer as well. **In the conjunctive setting**, suppose a bank transfer now requires the authorization of *two VPs and an ST*. Unlike the disjunctive scheme, a coalition needs to satisfy all the thresholds in the conjunctive form. Hence, with this requirement, *a VP and two STs* or *three STs* cannot authorize a transfer as they could in the disjunctive case. However, *three VPs* can, since a VP has more authorization power than an ST and can act as one.

2.4. The Harn-Fuyou MTSS scheme

Assume that the participants are partitioned into m levels L_i, $i = 1, 2, \ldots, m$. Let $|L_i| = n_i$ be the number of participants in L_i and let $t_i < n_i$ define a threshold on it. The threshold of a higher-level is always smaller than the threshold of a lower-level (i.e., $t_j < t_i$ for $j < i$) consistent with the above MTSS definition. The disjunctive MTSS of Harn and Fuyou has two phases:

- *Share generation:* The dealer first selects a prime p_0, defining the secret space as $s \in \mathbb{Z}_{p_0}$. For each subset L_i having n_i participants, she selects a sequence of pairwise coprime positive integers (or primes), $p_1^i < p_2^i < \ldots < p_{n_i}^i$, such that
$$p_0 \prod_{j=1}^{t_i-1} p_{n_i-j+1}^i < \prod_{j=1}^{t_i} p_j^i$$
and $gcd(p_0, p_k^i) = 1, k = 1, 2, \ldots, n_i$, where p_k^i is the public information associated with participant u_k^i, who is the kth member of the subset L_i. For each such sequence, the dealer selects an integer α_i such that the value $s+\alpha_i p_0$ is in the t_i-*threshold* range [9]. That is, α_i is chosen such that
$$\prod_{j=1}^{t_i-1} p_{n_i-j+1}^i < s + \alpha_i p_0 < \prod_{j=1}^{t_i} p_j^i$$
in order to prevent the recovery of the value $s + \alpha_i p_0$ with fewer than t_i shares.
For each participant u_k^i, the private share s_k^i is generated as $s_k^i = s+\alpha_i p_0 \mod p_k^i$. This share can directly be used within compartment L_i. In order to enable its use in a compartment L_j ($j > i$), the dealer first selects a prime $p_{k,j}^i$ such that $p_{t_j}^j < p_{k,j}^i < p_{n_j-t_j+2}^j$. She then computes
$$\Delta s_{k,j}^i = (s + \alpha_j p_0 - s_k^i) \mod p_{k,j}^i$$
and broadcasts it with $p_{k,j}^i$ as a public information.
All selected $p_{k,j}^i$s during this phase must be relatively coprime to all other moduli. At the end of the phase, each participant $u_k^i \in L_i$ keeps a single private share $s_k^i \in \mathbb{Z}_{p_k^i}$ accompanied with the public information $(\Delta s_{k,j}^i, p_{k,j}^i)$ for $j \in \{i+1, i+2, \ldots, m\}$.
- *Secret reconstruction:* The secret can be recovered by a coalition of participants if there are at least t_j participants in the coalition from levels L_i where $1 \leq i \leq j$. By using the corresponding shares, a system of equations regarding CRT can be established on the joined shares; if the participant u_k^i belongs to L_j, i.e., $i = j$, she can use her share s_k^i and the modulus p_k^i directly. Otherwise, i.e., if $i < j$, her share needs to be modified as $s_k^i + \Delta s_{k,j}^i$ to be used in the lower level L_j and the operations for this modified share need to be performed in modulo $p_{k,j}^i$ while constructing the system of CRT equations. Using all these shares and a standard CRT construction, a unique solution $y = s + \alpha_j p_0$ can be obtained. Then the secret can be reconstructed by computing $s = y \mod p_0$.

3. A First Analysis of Harn-Fuyou MTSS Scheme

Although the Harn-Fuyou scheme employs interesting and useful mini-mechanisms resulting in the first MTSS scheme employing CRT, the proposed scheme is not applicable in a generic setting and not secure. The weaknesses of the scheme can be summarized as follows:

- *Access Structure:* The first problem is its mismatch with the multilevel access structure of Simmons.
- *Prime Generation:* It is not suitable for the cases where the compartment threshold com-

poses at least one more than the majority of the participants.

- *Unauthorized Secret Recovery:* Due to the public information, an adversarial coalition can narrow down possible secret candidates, even to a unique value.

Here, we formulate each problem in a technical way with its proof. The examples in the Appendix illustrate the problems in a real implementation.

Remark 3. *The Harn-Fuyou scheme is not generic since there are practical cases for which it cannot be employed. In general, the range of the threshold values t_i are given such as $1 \leq t_i \leq \sum_{j=1}^{i} |L_j|$ for $i = 1, 2, \ldots, m$. Hence, t_i can be greater than $n_i = |L_i|$ as $\sum_{j=1}^{i} |L_j| > |L_i|$. Nonetheless, in the Harn-Fuyou scheme, the specified primes $p_1^i < p_2^i < \ldots < p_{n_i}^i$ cease at the index n_i, resulting in the condition*

$$p_0 \prod_{j=1}^{t_i-1} p_{n_i-j+1}^i < \prod_{j=1}^{t_i} p_j^i$$

being unclear for large enough t_i that exceeds n_i.

We refer the reader to Example 10 in the Appendix which illustrates this problem in a toy setting.

Lemma 4. *The Harn-Fuyou scheme is not suitable for the cases where the compartment threshold composes at least one more than the majority of the participants, i.e., $t_j \geq \lceil \frac{n_j}{2} \rceil + 1$.*

Proof: In the *share generation* phase, there are additional $p_{k,j}^i$ values associated with each participant u_k^i for each level L_j lower than her's. These numbers need to fulfill the condition $p_{t_j}^j < p_{k,j}^i < p_{n_j-t_j+2}^j$ and hence, the scheme implicitly compels the dealer to initially select the primes $p_1^j < p_2^j < \ldots < p_{n_j}^j$ with a gap allowing sufficient number of primes in between $p_{t_j}^j$ and $p_{n_j-t_j+2}^j$ so that $p_{k,j}^i$s can fill in. In addition to the gap, $p_{t_j}^j < p_{k,j}^i < p_{n_j-t_j+2}^j$ explicitly states that $t_j < n_j - t_j + 2$. □

Hence, placing the primes $p_{k,j}^i$ between $p_{t_j}^j$ and $p_{n_j-t_j+2}^j$ requires a condition which is not guaranteed to hold in a generic setting; it simply may be the case that $p_{t_j}^j > p_{n_j-t_j+2}^j$, i.e., $t_j > \lceil \frac{n_j}{2} \rceil + 1$. That is, the existence of some interval in between the primes is not ensured since there is no order whatsoever among the primes of different compartments. We refer the reader to Example 11 in the Appendix which illustrates this problem. To show that even a basic fix for this problem does not make the scheme secure, we propose the following straightforward modification.

3.1. A straightforward (yet insecure) modification

One can make the Harn-Fuyou MTSS scheme suitable for any number of participants and threshold values by removing the necessity of the additional primes: In the share generation phase, instead of using a sequence with n_i primes $p_1^i < p_2^i < \ldots < p_{n_i}^i$ for compartment L_i, the dealer can use a sequence with U_i primes $p_1^i < p_2^i < \ldots < p_{U_i}^i$ where $U_i = \sum_{j=1}^{i} n_j$. For security, the condition to be satisfied for this prime set is

$$p_0 \prod_{j=1}^{t_i-1} p_{U_i-j+1}^i < \prod_{j=1}^{t_i} p_j^i \tag{3}$$

that is well defined for any valid value of t_i. Here, the first n_i primes can be used for the participants in L_i and the extra primes p_ℓ^i for $\ell > n_i$ can be used for $p_{k,j}^i$s for the participants in higher compartments. The random integers $\alpha_i, 1 \leq i \leq m$ are chosen such that $0 \leq s + \alpha_i p_0 < p_1^i p_2^i \ldots p_{t_i}^i$. The share s_k^i for participant u_k^i is generated as $s_k^i = s + \alpha_i p_0 \mod p_{k,j}^i$ as before.

This approach indeed eliminates the need for $p^i_{k,j}$ to fill in to a possibly non-existing gap in between $p^j_{t_j} < p^i_{k,j} < p^j_{n_j - t_j + 2}$. As this is the only distinction we describe herein, the rest of the share generation phase and the secret reconstruction phase remains essentially intact, and can be performed in a similar fashion as described before.

Unfortunately, the modified scheme does not provide security as the following theorem and practical example illustrate. Although the example is given for the modified version, the same weakness also exists in the original MTSS scheme of Harn-Fuyou since the public information with different prime modulos for a certain participant reveals extra information as we show in the following theorem.

Theorem 5. *An adversarial coalition can narrow down possible secret candidates, even to a unique value, by using the public information.*

Proof: While extending a share of a participant into another level, a new prime is generated and public information is computed for that prime. Since different primes have been used for the same participant, an adversary can extract some information about the secret.

Let s^i_k be $y_i \bmod p^i_k$. For a lower level L_j, the corresponding public information is $\Delta s^i_{k,j} = (y_j - s^i_k) \bmod p^i_{k,j}$. The equation can be rewritten as

$$y_j \equiv \Delta s^i_{k,j} + s^i_k \bmod p^i_{k,j}.$$

At this point, anyone can observe that $y_j \bmod p^i_{k,j}$ is between $\Delta s^i_{k,j}$ and $\Delta s^i_{k,j} + p^i_k$. If $p^i_k < p^i_{k,j}$, some of the possible $y_j \bmod p^i_{k,j}$ values can be discarded by using the public information. In other words, anyone will acquire critical information about y_j.

In addition to public leakage above, an adversarial coalition A in L_j also knows $y_j \bmod M_A$, thereby they can reduce the number of possible candidates into

$$\frac{\prod_{j=1}^{t_i} p^i_j - \prod_{j=1}^{t_i - 1} p^i_{n_i - j + 1}}{M_A}.$$

Without the public information, thanks to the (semi) perfectness of Asmuth-Bloom SSS, the adversary cannot obtain information on the secret. However, with public information $\Delta s^i_{k,j}$, the adversary can eliminate some of the remaining candidates if they do not fall into $\Delta s^i_{k,j}$ and $\Delta s^i_{k,j} + p^i_k$ in modulo $p^i_{k,j}$. The more public information, the less candidates survive, and sometimes a unique value. □

An basic threshold setting, where the set of secret candidates is narrowed down to a unique value can be found in Example 12 of the Appendix.

4. Proposed Multilevel Threshold Secret Sharing Schemes

As described before, we are given a secret $s \in \mathbb{Z}_{p_0}$ and a set of primes such that

$$p_0 \prod_{i=1}^{t-1} p_{n-i+1} < \prod_{i=1}^{t} p_i, \tag{4}$$

i.e., the *Asmuth-Bloom condition* holds. We will refer to the prime sequence $p_0 < p_1 < p_2 < \ldots < p_n$ satisfying the Asmuth-Bloom condition as a (t, n)-*Asmuth-Bloom sequence*. As the fallacies of the Harn-Fuyou scheme show, having the Asmuth-Bloom condition for all the compartments independently while keeping the level structure and being secure is not an easy task. We solve this problem by using a single *anchor Asmuth-Bloom sequence* as defined below so that each participant of the MTSS has only one prime modulus that can be used for all the levels she can contribute to.

Definition 6. *An anchor Asmuth-Bloom sequence is a sequence of primes* $p_0 < p_1 < p_2 < \ldots < p_n$

satisfying

$$p_0{}^2 \prod_{i=1}^{\lfloor n/2 \rfloor - 1} p_{n-i+1} < \prod_{i=1}^{\lfloor n/2 \rfloor} p_i. \quad (5)$$

As one can notice, an anchor sequence is a valid $(\lfloor n/2 \rfloor, n)$-Asmuth-Bloom sequence. We show that, it can be used not only for $t = \lfloor n/2 \rfloor$ but also for other t values:

Theorem 7. *An anchor Asmuth-Bloom sequence can be employed for any CRT-based (t, n) secret sharing scheme. That is an anchor prime sequence satisfies the Asmuth-Bloom condition for any $1 \leq t \leq n$.*

Proof: We will investigate the theorem in two cases:

1 ($t \leq \lfloor n/2 \rfloor$): To have (4) from (5) for a threshold value $t \leq \lfloor n/2 \rfloor$, one can remove $\lfloor n/2 \rfloor - t$ primes from each side of (5). For each prime p_i removed from the right side, one needs to remove p_{n-i+2} from the left. Since $i \leq \lfloor n/2 \rfloor$ for all the primes removed, $n-i+2 > i$ which implies $p_{n-i+2} > p_i$. Thus, given the anchor inequality (5), the Asmuth-Bloom condition (4) is also satisfied for a threshold $t \leq \lfloor n/2 \rfloor$ with the same set of primes.

2 ($t > \lfloor n/2 \rfloor$): This case is similar to the former case except that to have (4) from (5), we need to add $t - \lfloor n/2 \rfloor$ primes to each side of (5). For each prime pair (p_{n-i+2}, p_i) added to the left and right of the anchor inequality, respectively, $p_{n-i+2} < p_i$ since $i > \lfloor n/2 \rfloor$. Thus given (5), (4) is also satisfied for a threshold value $t > \lfloor n/2 \rfloor$ with the same prime sequence.

□

4.1. A novel CRT-based multilevel threshold (disjunctive) SSS

Let $n = \sum_{i=1}^{m} n_i$ be the number of total participants. Let $h_i : \mathbb{Z}_{p_i} \times \mathbb{Z}_m \to \mathbb{Z}_{p_i}$ for $i \in \{1, \ldots, n\}$ be a family of efficiently computable one-way hash functions. We employ an anchor sequence of n primes as follows:

- *Initialization:* The dealer first generates an anchor prime sequence $p_0 < p_1 < p_2 < \ldots < p_n$ satisfying (5) and assigns each prime p_i to a participant u_i. In our scheme, this will be the only prime modulus that will be used for the participant[2].
- *Share generation:* Given a secret $s \in \mathbb{Z}_{p_0}$, the dealer chooses α_i's for all $1 \leq i \leq m$ such that

  $$0 \leq y_i = s + \alpha_i p_0 < M_i = p_1 p_2 \ldots p_{t_i}.$$

  For level L_i, the shares and the public information are generated as follows: Let u_k be a participant in L_i; the original share s_k^i for u_k is generated as $s_k^i = y_i \mod p_k$.
  If u_k is a participant in a higher compartment L_j, i.e., $j < i$; to enable the use of s_k^j in L_i, the dealer computes $\Delta s_k^i = (y_i - h_k(s_k^j, i)) \mod p_k$ and broadcasts it as the public information. This information will be used if u_k participates in the secret reconstruction within L_i.
- *Secret reconstruction:* Let A be a coalition gathered to reconstruct the secret. A is an authorized coalition if it has t_i or more participants from L_i or higher compartments for $1 \leq i \leq m$. If the participant is from L_i, her share s_k^i can be used as is. Any other share s_k^j of u_k from a higher level needs to be modified as $(h_k(s_k^j, i) + \Delta s_k^i)$

2. While describing the proposed schemes, we will denote the primes and participants with a single subscript as opposed to the notation in Harn-Fuyou scheme. We believe this is more clear thanks to the compactness of the anchor sequence we employ.

and is used with the modulus p_k while constructing the system of congruences. Using the standard CRT, a unique solution y_i can be obtained. Then, the secret s is recovered by computing $s = y_i \mod p_0$.

An authorized coalition can obtain the secret since with the help of public information, the coalition will have enough shares for a compartment L_i. Thanks to CRT, the corresponding y_i value and hence $s = y_i \bmod p_0$ can be computed.

4.1..1 Security analysis of the proposed MTSS

The security of the proposed MTSS solely depends on the security of the Asmuth-Bloom scheme. First, we show that, unlike the Harn-Fuyou scheme, the proposed MTSS scheme does not reveal any information on the secret with the public information used. Then, we will prove that an adversarial coalition cannot have any information on the secret.

Our security analysis is based on the random oracle model (ROM) [3]. In this manner, hash functions are replaced by random oracles, which outputs a truly random value for each unique query to the function.

To generate the public information, the proposed MTSS scheme employs a hash function for each participant. Let u_k be a participant in L_j. If the adversary corrupts u_k she will have s_k^j and she can compute the shares for all levels L_j, $j \leq i \leq m$. If u_k remains uncorrupted, the adversary will only have the public information for u_k. Let L_i be a level lower than j; the adversary will have

$$\Delta s_k^i = (s_k^i - h_k(s_k^j, i)) \mod p_k \qquad (6)$$

Hence, assuming the hash function h_k behaves like a random oracle, Δs_k^i will be random. Thus the adversary cannot learn anything on the shares of u_k for lower compartments. Furthermore, although the same hash function h_k is used to compute Δs_k^i and $\Delta s_k^{i'}$ for two lower levels L_i and $L_{i'}$, $j \leq i, i' \leq m$, these two values cannot be combined (as they could be without the hash function), since h_k takes i and i', respectively, as an input.

Theorem 8. *Given that the hash functions used in the MTSS scheme behave like random oracles, an unauthorized coalition cannot obtain any information about the secret.*

Proof: Let A' be the adversarial coalition having $t_i - 1$ participants from L_i and higher compartments. Let $M_{A'}$ be the product of the prime modulus values assigned to these $t_i - 1$ participants and $y_i' = y_i \mod M_{A'}$. Since ${p_0}^2 \prod_{j=1}^{t_i-1} p_{n-j+1} < \prod_{j=1}^{t_i} p_j < \prod_{j=1}^{t_i} p_j = M_i$, we have $M_i/M_{A'} > {p_0}^2$. Hence $y_i' + \beta M_{A'}$ is a valid candidate for $y_i < M$ for all $\beta < {p_0}^2$. Since $gcd(p_0, M_{A'}) = 1$, all $(y' + \beta M_{A'}) \bmod p_0$ are distinct for $\ell p_0 \leq \beta < (\ell + 1)p_0$, for each $0 \leq \ell < p_0$. Thus s can be any integer from $\mathbb{Z}_{p_0}$ and the secret space is not restricted from the adversary's point of view.

For each value s' in the secret space, from the adversary's point of view, there are either $\lfloor M_i/(M_{A'}p_0) \rfloor$ or $\lfloor M_i/(M_{A'}p_0) \rfloor + 1$ possible consistent y_i candidates consistent with s'. Considering $M_i/M_{A'} > {p_0}^2$, for two different integers s' and s'' in $\mathbb{Z}_{p_0}$, the probabilities of $s = s'$ or $s = s''$ are almost equal and the difference between these two values reduces when p_0 increases. More formally, thanks to the modified Asmuth-Bloom SSS we employed [14], the proposed MTSS scheme is *statistical*, i.e., the statistical distance between the probability distribution of the secret candidates being a secret and an uniform distribution is smaller than a given ϵ with a carefully chosen p_0. □

4.2. A CRT-based multilevel threshold (conjunctive) SSS

The ideas presented above for the disjunctive scheme can also be employed to have a conjuctive SSS. Here, we present the first CRT-based conjunctive MTSS scheme which adopts Iftene's CRT-based compartmented SSS [10].

The setting is the same as that of the disjunctive MTSS scheme; compartment L_i with threshold t_i has n_i participants for $1 \leq i \leq m$. Hence, the total number of participants is $n = \sum_{i=1}^{m} n_i$. There is a hierarchy between the compartments; a member of L_j can act as a member of a lower compartment L_i if $i > j$. The proposed conjunctive scheme shares a given secret $s \in \mathbb{Z}_{p_0}$ as follows:

- *Initialization:* The anchor prime sequence generation is the same. Let $\sigma_1, \sigma_2, \ldots, \sigma_{m-1}$ be random integers from $\mathbb{Z}_{p_0}$ and $\sigma_m \in \mathbb{Z}_{p_0}$ is chosen such that

$$s = (\sigma_1 + \sigma_2 + \cdots + \sigma_m) \bmod p_0.$$

- *Share generation:* For all $1 \leq i \leq m$, a random α_i is chosen such that $0 \leq y_i = \sigma_i + \alpha_i p_0 < M_i = p_1 p_2 \ldots p_{t_i}$. The shares and public information are generated similar to the disjunctive case. Let u_k be a participant in L_i; the original share s_k^i for u_k is generated as $s_k^i = y_i \mod p_k$. For all u_k who is from a higher level L_j to enable the use of s_k^j in L_i, $\Delta s_k^i = (y_i - h_k(s_k^j, i)) \mod p_k$ is computed and broadcasted.
- *Secret reconstruction:* The secret s can be recovered if and only if all of the σ_i values for $1 \leq i \leq m$ are recovered. A partial secret σ_i can be recovered if the number of shares from level L_i or from higher levels is greater than or equal to t_i. Let u_k be a coalition member participating in this task; if $u_k \in L_i$, her original share s_k^i can be used. Otherwise, if $u_k \in L_j$ for $j < i$, $h(s_k^j, i) + \Delta s_k^i$ is computed and used as s_k^i. After computing all σ_i values for $1 \leq i \leq m$, the secret s is constructed by $s = (\sigma_1 + \sigma_2 + \cdots + \sigma_m) \bmod p_0$.

4.2..1 Security analysis of the conjunctive MTSS

The security analysis of conjunctive scheme similar to the disjunctive one given in Section 4.1.1. The only difference between the proposed disjunctive and conjunctive schemes is that all the threshold conditions of the compartments need to be satisfied in the conjunctive setting. For that reason, in our conjunctive MTSS, the individual shares (s_k^i) are not directly generated from the secret (s) itself, but an additive share of the secret (σ_i). Other than that, they have a similar structure.

The public information of user u_k for lower level L_i is computed in the same way as in disjunctive case, $\Delta s_k^i = (y_i - h_k(s_k^j, i)) \mod p_k$. Since the scheme uses exactly the same set of public information, we can use the same claim: assuming the hash function h_k behaves like a random oracle, Δs_k^i will be random. Therefore, under the random oracle model, the adversary cannot learn any additional information on the shares of u_k for lower levels.

Theorem 9. *Given that the hash functions used in the conjunctive MTSS scheme behave like random oracles, an unauthorized coalition cannot obtain any information about the secret.*

Proof Sketch: In the initialization phase of the scheme, the secret s is shared using additive secret sharing into σ_i values. In order to recover s, each of the individual σ_i values needs to be obtained. In addition, we showed that an adversary A' cannot use public information to learn share of a participant at

a lower level. Therefore, the adversary is restricted to the case where s/he tries to obtain each secret of compartments σ_i separately. Each σ_i value is shared using the modified Asmuth-Bloom SSS presented in [14], which is shown to be statistical. In other words, an unauthorized coalition cannot obtain any information about the σ_i, thereby they cannot obtain any information about the secret s. □

5. Conclusion

The CRT-based multilevel threshold SSS of Harn-Fuyou in the literature cannot be used for all threshold settings. Furthermore, the scheme is not secure and an adversary can extract the secret by using the private shares of the participants she corrupted and information revealed to the public during the secret sharing phase. We proposed novel, compact, and elegant disjunctive and conjunctive multilevel SSSs based on a special prime sequence called anchor sequence and showed that the proposed schemes can be adopted for FSSs which have numerous applications in applied cryptography.

References

[1] Charles Asmuth and John Bloom. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 30(2):208–210, 1983.

[2] Amos Beimel. Secret-sharing schemes: A survey. volume 6639 of *Coding and Cryptology*, pages 11–46. 2011.

[3] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

[4] George Robert Blakley. Safeguarding cryptographic keys. volume 48 of *Proceedings of the National Computer Conference*, pages 313–317, 1979.

[5] Ilker Nadi Bozkurt, Kamer Kaya, and Ali Aydın Selçuk. Secret sharing for general access structures. 4th International Conference on Information Security and Cryptology, Ankara, Turkey, 2010.

[6] Oğuzhan Ersoy, Thomas Brochmann Pedersen, Kamer Kaya, Ali Aydin Selçuk, and Emin Anarim. A crt-based verifiable secret sharing scheme secure against unbounded adversaries. *Security and Communication Networks*, 9(17):4416–4427, 2016.

[7] Hossein Ghodosi, Josef Pieprzyk, and Rei Safavi-Naini. Secret sharing in multilevel and compartmented groups. Information Security and Privacy, pages 367–378, 1998.

[8] Cheng Guo and Chin-Chen Chang. An authenticated group key distribution protocol based on the generalized chinese remainder theorem. *International Journal of Communication Systems*, 27(1):126–134, 2014.

[9] Lein Harn and Miao Fuyou. Multilevel threshold secret sharing based on the chinese remainder theorem. *Information Processing Letters*, 114(9):504–509, 2014.

[10] Sorin Iftene. Compartmented secret sharing based on the chinese remainder theorem. *IACR Cryptology ePrint Archive*, 2005:408, 2005.

[11] Sorin Iftene. General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science*, 186:67–84, 2007.

[12] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Proc. of the IEEE Global Telecom. Conf., Globecom 87*, pages 99–102, 1987.

[13] Kamer Kaya and Ali Aydın Selçuk. A verifiable secret sharing scheme based on the Chinese Remainder Theorem. volume 5365 of *Progress in Cryptology - INDOCRYPT 2008*, pages 414–425. 2008.

[14] Kamer Kaya and Ali Aydın Selçuk. Threshold cryptography based on Asmuth-Bloom secret sharing. *Information Sciences*, 177(19):4148–4160, 2007.

[15] Kamer Kaya and Ali Aydin Selçuk. Sharing DSS by the chinese remainder theorem. *J. Computational Applied Mathematics*, 259:495–502, 2014.

[16] Yanjun Liu, Lein Harn, and Chin-Chen Chang. An authenticated group key distribution mechanism using theory of numbers. *International Journal of Communication Systems*, 27(11):3502–3512, 2014.

[17] Yanjun Liu, Lein Harn, and Chin-Chen Chang. A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets. *International Journal of Communication Systems*, 28(7):1282–1292, 2015. IJCS-13-0526.R3.

[18] Maurice Mignotte. How to share a secret. Cryptography, pages 371–375. 1983.

[19] Michaël Quisquater, Bart Preneel, and Joos Vandewalle. On the security of the threshold scheme based on the Chinese Remainder Theorem. Public Key Cryptography, pages 199–210, 2002.

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

[21] Gustavus J Simmons. How to (really) share a secret. Proceedings on Advances in Cryptology, pages 390–448, 1990.

[22] Tamir Tassa. Hierarchical threshold secret sharing. Theory of cryptography, pages 473–490. Springer, 2004.

Appendix

Example 10. *The Harn-Fuyou scheme is not well-defined for a very basic setting with two compartments L_1 and L_2, where $n_1 = 3$, $n_2 = 3$, $t_1 = 2$ and $t_2 = 4$ since there are only 3 users in the second compartment. The threshold is 4 and a (t, n)-Asmuth-Bloom sequence with $n = 3$ and $t = 4$ does not exist.*

Example 11. *Let there be two levels L_1 and L_2 in the Harn-Fuyou scheme involving $n_1 = |L_1| = 2$ and $n_2 = |L_2| = 3$ participants and let the thresholds be $t_1 = 2$ and $t_2 = 3$. The dealer selects the primes $p_0 < p_1^1 < p_2^1$ and $p_0 < p_1^2 < p_2^2 < p_3^2$ which need to satisfy*

$$p_0 p_2^1 < p_1^1 p_2^1 \quad \text{and} \quad p_0 p_2^2 p_3^2 < p_1^2 p_2^2 p_3^2$$

to be secure. Recall that $p_{k,j}^i$ is the prime distributed to kth user in ith level to be used for participation in a lower compartment j. Since $p_{k,j}^i$ must be chosen such that $p_{t_j}^j < p_{k,j}^i < p_{n_j - t_j + 2}^j$, we have $p_3^2 < p_{1,2}^1 < p_2^2$ and $p_3^2 < p_2^2$ contradicts with the initial choice of primes $p_2^2 < p_3^2$.

Example 12. *Consider the following setting emerging from the scheme with modified Harn-Fuyou scheme. Let $p_0 = 5$ and $s = 1 \in \mathbb{Z}_5$. Suppose that we have two compartments L_1 and L_2 with $n_1 = 4$, $n_2 = 2$, $t_1 = 2$ and $t_2 = 3$. Let*

$$p_1^1 < p_2^1 < p_3^1 < p_4^1 \stackrel{\triangle}{=} 11 < 13 < 17 < 23$$

$$p_1^2 < p_2^2 < p_3^2 < p_4^2 < p_5^2 < p_6^2$$
$$\stackrel{\triangle}{=} \quad 29 < 31 < 37 < 61 < 67 < 71$$

be the primes which satisfies Equation (3) and t-threshold range. $p_{1,2}^1 = p_6^2 = 71$, $p_{2,2}^1 = p_5^2 = 67$, $p_{3,2}^1 = p_4^2 = 61$, $p_{4,2}^1 = p_3^2 = 37$ be the additional primes that will be used to enable the share of the participants in L_1 for L_2. Let $\alpha_1 = 5$ and $\alpha_2 = 952$, then

$$y_1 = s + \alpha_1 p_0 = 1 + 5 \times 5 = 26,$$

$$y_2 = s + \alpha_2 p_0 = 1 + 952 \times 5 = 4761.$$

With these parameters, the shares and the public information are computed as

$$s_1^1 = 4, s_2^1 = 0, s_3^1 = 9, s_4^1 = 3, \quad s_1^2 = 5, s_2^2 = 18$$

$$s_{1,2}^1 = 4, s_{2,2}^1 = 4, s_{3,2}^1 = 3, s_{4,2}^1 = 25$$

$$\Delta s_{1,1}^1 = 0, \Delta s_{2,1}^1 = 4, \Delta s_{3,1}^1 = 55, \Delta s_{4,1}^1 = 22.$$

Suppose that the adversary corrupted u_1^2 and u_2^2 hence obtained their shares. She knows that y_2 is bounded by $4757 < y_2 < 33263$ and she also can compute $y_2 \mod p_1^2 p_2^2 = y_2 \mod 899 = 266$ by using these shares. There are $\lceil (33263 - 4757)/899 \rceil = 32$ candidates for y_2 all in form $266 + 899 \times K$ where $5 \leq K \leq 36$. Since, 899 is relatively prime with 5, each secret candidate in $\mathbb{Z}_{p_0}$ must be valid for around 7 of these values, i.e., for $266 + 899 \times 6$ the valid secret candidate is 0.

The participant u_1^1 has a public information pair $(\Delta s_{1,2}^1, p_{1,2}^1) = (0, 71)$ and her prime is $p_1^1 = 11$. Hence, the adversary knows that the value $s_{1,2}^1$ is bounded by $s_{1,2}^1 = s_1^1 + \Delta s_{1,2}^1 \in [0, 10]$ since $s_1^1 \in \mathbb{Z}_{11}$. Similarly, for u_2^1, u_3^1, and u_4^1, the adversary knows that $s_{2,2}^1 \in [4, 16], s_{3,2}^1 \in [55, 60] \cup [0, 10], s_{4,2}^1 \in [22, 36] \cup [0, 7]$.

As the Table 2 shows, there is only one y_2 candidate in the form $51 + 899K$, which yields $s_{\{1,2,3,4\},2}^1$ values within these ranges. Thus the adversary knows that $y_2 = 4761$ and the secret $s = 1$ is recovered in an unauthorized manner by corrupting only two participants from L_2.

TABLE 2

Secrets for each y_2 candidate from adversary's point of view for Example 2. The values consistent with the ranges obtained by public information are shown in boldface.

candidate	$s^1_{1,2}$	$s^1_{2,2}$	$s^1_{3,2}$	$s^1_{4,2}$	candidate	$s^1_{1,2}$	$s^1_{2,2}$	$s^1_{3,2}$	$s^1_{4,2}$
4761	**4**	**4**	**3**	**25**	19145	46	50	52	16
5660	51	32	48	**36**	20044	22	**11**	36	**27**
6559	27	60	32	10	20943	69	39	20	**1**
7458	**3**	21	16	21	21842	45	0	**4**	12
8357	50	49	**0**	**32**	22741	21	28	49	**23**
9256	26	**10**	45	**6**	23640	68	56	33	**34**
10155	**2**	38	29	17	24539	44	17	17	8
11054	49	66	13	**28**	25438	20	45	**1**	19
11953	25	27	**58**	**2**	26337	67	**6**	46	**30**
12852	**1**	55	42	13	27236	43	34	30	**4**
13751	48	16	26	**24**	28135	19	62	14	15
14650	24	44	**10**	**35**	29034	66	23	**59**	**26**
15549	**0**	**5**	**55**	9	29933	42	51	43	**0**
16448	47	33	39	20	30832	18	**12**	27	11
17347	23	61	23	**31**	31731	65	40	11	**22**
18246	70	22	**7**	**5**	32630	41	1	**56**	**33**