Reusable Multi-Stage Multi-Secret Sharing Schemes Based on CRT

Anjaneyulu Endurthi, Oinam Bidyapati Chanu, Appala Naidu Tentu, and V. Ch. Venkaiah

***Abstract*—Three secret sharing schemes that use the Mignotte's sequence and two secret sharing schemes that use the Asmuth-Bloom sequence are proposed in this paper. All these five secret sharing schemes are based on Chinese Remainder Theorem (CRT) [8]. The first scheme that uses the Mignotte's sequence is a single secret scheme; the second one is an extension of the first one to Multi-secret sharing scheme. The third scheme is again for the case of multi-secrets but it is an improvement over the second scheme in the sense that it reduces the number of public values. The first scheme that uses the Asmuth-Bloom sequence is designed for the case of a single secret and the second one is an extension of the first scheme to the case of multi-secrets.**

Novelty of the proposed schemes is that the shares of the participants are reusable i.e. same shares are applicable even with a new secret. Also only one share needs to be kept by each participant even for the muslti-secret sharing scheme. Further, the schemes are capable of verifying the honesty of the participants including the dealer. Correctness of the proposed schemes is discussed and show that the proposed schemes are computationally secure.

***Index Terms*—Multi-Secret, Mignotte's sequence, Asmuth-Bloom sequence, CRT, Secret sharing scheme**

I. Introduction

The requirement of the key being secret brings several problems. Storing a secret key with only one person or server or database reduces the security of the system to the security and credibility of that agent. Besides, not having a backup of the key introduces the problem of losing the key if a mischief occurs. On the other hand, if the key is held by more than one agent an adversary with a desire for the key has more flexibility of choosing the target. Hence the security is reduced to the security of the least secure or least credible of these agents. Secret sharing schemes are introduced to solve these problems of key management. The main idea of these schemes is to share a secret among a set of agents such that only the predefined coalitions can come together and reveal the secret, while no other coalition can obtain any information about the secret. Thus, the keys used in areas requiring vital secrecy like large-scale finance applications and command control mechanisms of nuclear systems, can be stored by using secret sharing schemes.

Secret sharing was first proposed by Blakley[3] and Shamir[4]. The scheme by Shamir relies on the standard Lagrange polynomial interpolation, whereas the scheme by Blakley[3] is based on the geometric idea that uses the concept of intersecting hyperplanes.

The family of authorized subsets is known as the access structure. An access structure is said to be monotone if a set is qualified then its superset must also be qualified. Several access structures are proposed in the literature. They include the (t, n)-threshold access structure, the Generalized access structure and the Multipartite access structure. In the (t, n)-threshold access structure there are n shareholders. An authorized group consists of any t or more participants and any group of at most $t-1$ participants is an unauthorized group. Let $\mathbb{U}$ be a set of n participants and let $2^{\mathbb{U}}$ be its power set. Then the 'Generalized access structure' refers to situations where the collection of permissible subsets of $\mathbb{U}$ may be any collection $\Gamma \subseteq 2^{\mathbb{U}}$ having the monotonicity property.

In multipartite access structures, the set of players $\mathbb{U}$ is partitioned into m disjoint entities $\mathbb{U}_1, \mathbb{U}_2, \cdots, \mathbb{U}_m$ called levels and all players in each level play exactly the same role inside the access structure.

In multi-secret sharing schemes the problem of sharing many secrets is addressed. In these schemes, every participant needs to keep only one shadow and many secrets can be shared independently without refreshing the shadow. In order to reconstruct a secret, each involved participant only needs to submit a pseudo shadow computed from the real shadow instead of the real shadow itself. The reconstruction of a secret cannot compromise the secrecy of the remaining secrets that haven't been reconstructed. A typical scenario wherein the multi-secret sharing problem occurs is as follows.

Suppose that a company has l secrets which are important for business functionalities. Each secret contains a key information needed to perform a business operation. The company does not trust any single employee to access any one of the secrets. The company decides that each secret be shared among a set of employees/participants according to a specific threshold access structure. The company may use multiple secret sharing schemes to share these secrets. Howevereach employee needs to keep multiple shadows to participate in each game of secret sharing corresponding to each secret. So, there will be a shadow/share management problem in this method. Hence the need for multi-secret sharing schemes.

Manuscript received February 25, 2015; revised April 12, 2015.

A. Endurthi is with the Computer Science and Engineering Department, RGUKT - IIIT Basar, Telangana State, 504107, India (e-mail: anjaneyuluendurthi@gmail.com)

O. B. Chanu and V. Ch. Venkaiah are with the School of Computer and Information Sciences, University of Hyderabad, 500046, India (e-mail: obidyapatichanu@gmail.com, venkaiah@hotmail.com)

A. N. Tentu is with the CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science, Hyderabad, 500046, India (e-mail: naidunit@gmail.com)

1845-6421/03/8388

A. Detection of cheaters

A verifiable secret-sharing scheme [13] provides its shareholders with an ability to verify that (a) the secret shadows obtained from the dealer are derived consistently from the same secret and (b) the secret shadows obtained from the other shareholder in the secret reconstruction process are genuine shadows. This ability is important because a dishonest dealer can cheat share holders by giving them fake shadows. Also communication errors can result in fake shadows. A shareholder may also cheat others in the secret reconstruction process by presenting a fake shadow to prevent others from obtaining the real secret. Secret sharing schemes involving cheaters is discussed in [5] and Cheating detection and identification in CRT based schemes was presented by pasaila [7].

B. Related Work

Secret sharing scheme that uses Mignotte's sequence and is based on Chinese Remainder Theorem [8] is introduced in [1], and it is modified to result in another scheme by Asmuth-Bloom [2]. J. He, E. Dawson [9], proposed a multi-stage secret sharing scheme based on one way function in 1994 [10], [11], [12]. They used Lagrange interpolation polynomial in order to perform secret sharing. Later in 2000, Chien et al. [15] proposed a new type of (t, n) multi-secret sharing scheme based on the systematic block codes. Subba Rao Y V and Chakravarthy Bhagvati [14] came up with a multi-stage secret sharing scheme based on CRT. In the later scheme multiple secrets are shared to different groups, such that each group receives a share of the secret intended for it.

C. Motivation

Mignotte's and Asmuth-Bloom Secret Sharing Schemes are based on CRT. They are designed to handle single secret only and hence they are not capable of handling multiple secrets. So, to share multiple secrets, one needs to initiate multiple (one for each secret) secret sharing schemes. Also the shares distributed in connection with (corresponding to) one secret cannot be reused for a different secret. That is shares need to be distributed whenever a new secret is to be shared. This results in receiving a participant to keep multiple shares corresponding to each secret. So, there will be a share management problem. This paper addresses this aspect of the secret sharing schemes and proposes several schemes that overcome this issue.

The paper is organised as follows: The following subsections gives an overview of Mignotte and Asmuth-Bloom schemes. Section 2 gives an overview of the Mignotte's and Asmuth-Bloom Schemes. Section 3 and 4 propose Mignotte's sequence based reusable secret sharing schemes designed for single and multiple secrets respectively. Section 5 improves on the multi-secret Sharing Scheme given in Section 4 by reducing the number of public values required. Sections 6 and 7 propose Asmuth-Bloom sequence based reusable secret sharing schemes designed for single and multiple secrets respectively. Our results are shown in section 8 and Concluding remarks are in section 9.

II. Existing Schemes

A. Overview of Mignotte's SSS

Mignotte's sequence: Let t and n be two integers such that $n \geq 2$ and $2 \leq t \leq n$. A (t, n) *Mignotte's sequence* is a sequence of pairwise co-prime positive integers $p_1 < p_2 < \ldots < p_n$ such that

$$\prod_{i=0}^{t-2} p_{n-i} < \prod_{i=1}^{t} p_i$$

This can be seen to be equivalent to
$max_{1 \leq i_1 < \ldots < i_{t-1} \leq n}(p_{i_1} * p_{i_2} * \ldots * p_{i_{t-1}}) <$
$min_{1 \leq i_1 < \ldots < i_t \leq n}(p_{i_1} * p_{i_2} * \ldots * p_{i_t})$

To share a secret S among a group of n users, the dealer does the following:

1) Distribution:
   - The secret S is chosen as a random integer such that $\beta < S < \alpha$
     where $\alpha = \prod_{i=1}^{t} p_i$ and $\beta = \prod_{i=0}^{t-2} p_{n-i}$.
   - Compute shares $I_i = S \bmod p_i$ for all $1 \leq i \leq n$.
   - Distribute shares $I_i, 1 \leq i \leq n$, to n participants.

2) Reconstruction:
   - Given t distinct shares $I_{i_1} I_{i_2}, \ldots, I_{i_t}$ the secret S is reconstructed using the standard variant of Chinese Remainder Theorem, as the unique solution modulo $p_{i_1} \ldots p_{i_t}$ of the system,

$$S \equiv I_{i_j} \bmod p_{i_j}, 1 \leq j \leq t$$

B. Overview of Asmuth-Bloom SSS

A sequence of pairwise coprime positive integers (can also be called as Asmuth-Bloom sequence) $p_0, p_1 < \cdots < p_n$ is chosen such that

$$p_0 \prod_{i=0}^{t-2} P_{n-i} < \prod_{i=1}^{t} P_i$$

To share a secret S among a group of n users, the dealer does the following:

Distribution:

- The secret S is chosen as a random integer of the set Z_{p_0}.
- Compute shares $I_i = X = (S + \gamma p_0) \bmod p_i$ for all $1 \leq i \leq n$ where γ is an arbitary integer such that
  $$p_0 \prod_{i=0}^{t-2} P_{n-i} < (S + \gamma p_0) < \prod_{i=1}^{t} P_i$$
  .
- Distribute shares $I_i, 1 \leq i \leq n$, to participants.

Reconstruction:

- Given t distinct shares $I_{i_1} I_{i_2}, \ldots, I_{i_t}$ the modified secret X is reconstructed using the standard variant of Chinese Remainder Theorem, as the unique solution modulo $p_{i_1} \ldots p_{i_t}$ of the system

$$X \equiv I_{i_j} \bmod p_{i_j}, 1 \leq j \leq t$$

- The original secret can be reconstructed using $S = X \bmod p_0$

C. Two-variable one-way function

A two-variable one-way function $F(r, z)$ is a function that maps a random value r and a share z onto a bit string $F(r, z)$ of a fixed length. This function has the following properties.

- Given r and z, it is easy to compute $F(r, z)$;
- Given z and $F(r, z)$, it is hard to compute r;
- Having no knowledge of z, it is hard to compute $F(r, z)$ for any r;
- Given z, it is hard to find two different values r_1 and r_2 such that $F(r_1, z) = F(r_2, z)$;
- Given r and $F(r, z)$, it is hard to compute z;
- Given pairs of r_i and $F(r_i, z)$, it is hard to compute $F(r', z)$ for $r' \neq r_i$.

III. Reusable single secret scheme based on Mignotte's sequence

In the previous schemes i.e Mignotte [1], Asmuth-Bloom [2], the shares are directly related to the secret. That is a new set of shares needs to be distributed whenever a new secret is to be shared. So, we hereby propose a scheme [6] that overcomes this limitation; thereby allowing the shares to be reusable.

Overview of the scheme

Initially, the dealer comes up with the number of participants, (n), threshold value, (k), the secret (S) to be shared among the participants $P_1, P_2, \cdots, P_n$, one way function, (f) and the Mignotte's sequence $p_1, p_2, \cdots, p_n$ to be used. Also the delaer chooses random values $y_i, 1 \leq i \leq n$, and distributes them one each to the participants (i.e y_i to P_i) as the pseduo shares of the participants. The dealer then computes the (real) shares (Z_i) of the participants P_i, $1 \leq i \leq n$, from the secret. Now the dealer applies the chosen one-way function f to each of these random numbers (y_i), subtracts each of these resulting numbers $f(y_i)$ from the corresponding real shares $Z_i, 1 \leq i \leq n$, of the participants. These values are made public. While reconstructing the secret, the participants first apply one-way function to the pseudo share, which they possess, adds the resulting value $f(y_i)$ to the corresponding public share and recovers the actual share Z_i. These shares are then used to recover the secret using CRT.

A. Distribution

- Dealer chooses a publicly known (k, n) Mignotte's sequece $p_1, p_2, \ldots, p_n$
- Chooses randomly $y_1, y_2, \cdots, y_n$ such that $y_i \in Z_{p_i}$ as the pseudo share of the i^{th} participant.
- Chooses the secret S such that $\beta < S < \alpha$, where $\alpha = \prod_{i=1}^{k} p_i$ and $\beta = \prod_{i=0}^{k-2} p_{n-i}$.
- Computes $Z_i = S \bmod p_i, 1 \leq i \leq n$.
- Computes $d_i = (Z_i - f(y_i)) \bmod p_i$, $1 \leq i \leq n$, as the shift values, where f is the chosen one way function.
- For every $i, 1 \leq i \leq n$, deliver y_i to the i^{th} participant through a secure channel and publish d_i

B. Reconstruction

- Each particiapnt calculates his actual share by computing $Z_i = (d_i + f(y_i)) \bmod p_i$.
- The secret is reconstructed from the shares Z_i of k or more participants using CRT.

C. Example:

1) Distribution:

- Consider a publicly known $(3, 5)$ Mignotte's sequece to be 5,7,11,13,17.
- Let the random values be $y_1 = 3, y_2 = 4, y_3 = 8, y_4 = 5, y_5 = 10$ and the chosen one-way function be the exponentiation of 2 modulo 17.
- Consider the secret as 297 which lies between β and α, where $\beta = 221$ and $\alpha = 385$.
- Compute $Z_i = S \bmod p_i$, $1 \leq i \leq 5$.
  $Z_1 = 297 \bmod 5 = 2$, $Z_2 = 297 \bmod 7 = 3$, $Z_3 = 297 \bmod 11 = 0$, $Z_4 = 297 \bmod 13 = 11$, $Z_5 = 297 \bmod 17 = 8$.
- Compute shift values $d_i = Z_i - f(y_i) \bmod p_i$,$1 \leq i \leq 5$.
  $d_1 = (2 - 8) \bmod 5 = 4$, $d_2 = (3 - 16) \bmod 7 = 1$, $d_3 = (0 - 1) \bmod 11 = 10$, $d_4 = (11 - 15) \bmod 13 = 9$, $d_5 = (8 - 4) \bmod 17 = 4$.
  These values are made public and y_i, $1 \leq i \leq 5$, are privately delivered to the participants.

2) Reconstruction:

- Three particiapnts, say Z_1, Z_2, Z_5, want to pool their shares and reconstruct the secret. So they calculate their actual shares by computing $Z_i = (d_i + f(y_i)) \bmod p_i$ for $i = 1, 2$ and 5. That is
  $Z_1 = (4 + 8) \bmod 5 = 2$, $Z_2 = (1 + 16) \bmod 7 = 3$, and $Z_5 = (4 + 4) \bmod 17 = 8$.

- The secret is reconstructed from the following equations using CRT.

$$S \equiv 2 \bmod 5$$
$$S \equiv 3 \bmod 7$$
$$S \equiv 8 \bmod 17$$

We have $M = 5 * 7 * 17 = 595$, $m_1 = \frac{M}{5} = 119, m_2 = \frac{M}{7} = 85, m_3 = \frac{M}{17} = 35$ and $N_1 = 4, N_2 = 1, N_3 = 1$ where N_i, $1 \leq i \leq 3$ are such $m_1 N_1 = 1 \bmod 5, m_2 N_2 = 1 \bmod 7, m_3 N_3 = 1 \bmod 17$
Therefore, $S = ((2*119*4)+(3*85*1)+(8*35*1)) \bmod 595 = 297$
Hence the secret.

IV. Proposed Multi-stage Multi-secret sharing scheme based on Mignotte's Sequence

Overview of the scheme

As in the previous single secret scheme, here also the dealer initializes all the required parameters. The only difference is

that the dealer chooses multiple, say l, secrets S_i, $1 \leq i \leq l$, instaead of a single secret. The chosen secrets $S_i, 1 \leq i \leq l$, are then modified to $S'_i = S_i + S_{i+1}$, $1 \leq i \leq l-1$, except the last secret S_l, which remains as it is. Successful reconstruction of the secrets is possible only when the secrets lie between the values of β and α. So as to bring the modified secrets (i.e $S'_i = S_i + S_{i+1}$) to this range , we divide each of the modified secret by 2. While doing so, we modify the secrets S'_i by subtracting 1 from the odd secrets and record this by setting a flag bit b_i. The resulting values are the final modified secrets (S''_i), from which the actual shares (Z_{ij}) of the participants are generated. From the actual shares $Z_{ij}, 1 \leq i \leq l, 1 \leq j \leq n$, and the pseudo shares $y_1, y_2, \cdots, y_n$ public values d_{ij} are computed. Verification values are also derived from the actual shares. Both the sets, i.e the set of the public (d_i values) and the the set of verification values are made public. The random values (i.e pseudo shares $y_1, y_2, \cdots, y_n$) which were chosen by the dealer are distributed privately to each participant. In the verification phase, any participant can compute the hash value by using verification function and check whether they are equal to the published verification values.

In the reconstruction phase, participants compute their actual shares by adding the images of the one-way function of their secret shadows to the public values. CRT is used to reconstruct the modified secrets, which are then multiplied by 2. S_{i-1} is then recovered by subtracting the previously recostructed secret S_i.

A. Initialization

In this phase, all the variables are intialized and the secrets are chosen.

Algorithm 1 Initialization

1: Let $\{P_1, P_2, \cdots, P_n\}$ be the n paricipants and k be the threshold value.
2: Consider a publicly known (k, n) Mignotte's sequece, say $p_1 < p_2 < \ldots < p_n$.
3: Randomly choose n secret shadows $y_1, y_2, \cdots, y_n$ such that $y_i \in Z_{p_i}$ as the pseudo shares.
4: Choose the secrets $S_1, S_2, \cdots, S_l$ such that $\beta < S_i < \alpha$, $1 \leq i \leq l$, where $\alpha = \prod_{i=1}^{k} P_i$ and $\beta = \prod_{i=0}^{k-2} P_{n-i}$.

B. Distribution

In the distribution phase, actual secret is modified except the l^{th} secret. Shares are computed from these modified secrets.

Algorithm 2 Distribution of Shares

1: Compute $S'_i = S_i + S_{i+1}$, for $i = 1, 2, \cdots, l-1$
2: For $i = 1, 2, \cdots, l-1$
Begin
3: If $(S'_i \bmod 2 == 1)$ then $S''_i = (S'_i - 1)/2$ and set $b_i = 1$
4: Else $S''_i = S'_i/2$ and set $b_i = 0$.
End.
5: $S''_l = S'_l = S_l$
For $i = 1, 2, \cdots, l$ and $j = 1, 2, \cdots, n$ do
Begin
6: Compute $Z_{ij} = S''_i \bmod p_j$
7: Compute $d_{ij} = (Z_{ij} - f^i(y_j)) \bmod p_j$, where f is a one way function and $f^i(x)$ denotes i successive applications of f to x. i.e $f^0(x) = x$ and $f^i(x) = f(f^{i-1}(x))$ for $i \geq 1$
8: Compute $F(r, Z_{ij})$, where r is a random value
End.
9: Distribute y_j to each participant through a secure channel and publish all d_{ij}, $F(r, Z_{ij})$ values, r and two-variable one-way function $F(r, z)$.

C. Verification

In this phase, each participant can verify the allocated share. Reconstructor also can verify the shares provided by the participants.

Algorithm 3 Verification of shares

1: Participants can verify their shares by calculating $F(r, Z_{ij})$, where Z_{ij} itself can be computed by using pseudo shares y_j and the corresponding public values d_{ij}.
2: Similarly, reconstructor also can verify honesty of the other participants by computing $F(r, Z_{ij})$.

D. Reconstruction

Secrets are reconstructed in seqiential order starting from the last, i.e, the l^{th}, secret. Any k or more participants can pool their shares and reconstruct these secrets.

Algorithm 4 Reconstruction of secrets

1: Each participant $j, 1 \leq j \leq n$, willing to take part in the reconstruction calculates $Z_{ij} = (d_{ij} + f^i(y_j)) \bmod p_j, 1 \leq i \leq l$
2: Any k participants can pool their shares and reconstruct the secrets $S_l, S_{l-1}, \cdots, S_1$ in a sequential order as follows
3: If $i = l$, then construct $S''_l = S'_l$ and hence the secret S_l using CRT from the shares Z_{lj}
For $i = l-1, l-2, \cdots, 1$ do the following:
4: Construct S''_i using CRT from the shares Z_{ij}
5: $S'_i = S''_i * 2$
6: If $b_i = 1$, $S'_i = S'_i + 1$
7: Compute the i^{th} secret as $S_i = S'_i - S_{i+1}$

E. Example

We hereby illustrate the proposed scheme with artificially small parameters.

1) Initialization:

- Consider a group of 5 participants $\{P_1, P_2, P_3, P_4, P_5\}$ wherein 3 participants are sufficient to reconstruct the secret. That is the number of participants, n, is 5 and the threshold, t, is 3.
- Consider the Mignotte's sequece as 5,7,11,13,17 in which $\beta = 221$ and $\alpha = 385$.
- Let the random values be: $y_1 = 3, y_2 = 4, y_3 = 8, y_4 = 5, y_5 = 10$.
- Consider the secrets to be $S_1 = 251, S_2 = 282, S_3 = 323, S_4 = 317$ which lie between β and α.

Let the chosen one way function be exponentiation of 2 modulo

2) Distribution:

- Compute $S'_i = S_i + S_{i+1}$ for $i = 1, 2, 3$. That is
  $S'_1 = S_1 + S_2 = 251 + 282 = 533$
  $S'_2 = S_2 + S_3 = 282 + 323 = 605$
  $S'_3 = S_3 + S_4 = 323 + 317 = 640$
  $S'_4 = S_4 = 317$.
- Check the condition $(S'_i \bmod 2 == 1)$ and correspondingly compute S''_i,
  $S''_1 = (533 - 1)/2 = 266$ and $b_1 = 1$
  $S''_2 = (605 - 1)/2 = 302$ and $b_2 = 1$
  $S''_3 = 640/2 = 320$ and $b_3 = 0$
  $S''_4 = S'_4 = 317$.
- Compute $Z_{ij} = S''_i \bmod p_j$,for $i = 1, 2, 3, 4$ and $j = 1, 2, 3, 4, 5$. This gives
  $Z_{11} = 1$, $Z_{12} = 0$, $Z_{13} = 2$, $Z_{14} = 6$, $Z_{15} = 11$
  $Z_{21} = 2$, $Z_{22} = 1$, $Z_{23} = 5$, $Z_{24} = 3$, $Z_{25} = 13$
  $Z_{31} = 0$, $Z_{32} = 5$, $Z_{33} = 1$, $Z_{34} = 8$, $Z_{35} = 14$
  $Z_{41} = 2$, $Z_{42} = 2$, $Z_{43} = 9$, $Z_{44} = 5$, $Z_{45} = 11$
- Compute public values $d_{ij} = (Z_{ij} - f^i(y_j)) \bmod p_j, 1 \leq i \leq 4, 1 \leq j \leq 5$
  $d_{11} = 3$, $d_{12} = 5$, $d_{13} = 1$, $d_{14} = 4$, $d_{15} = 7$
  $d_{21} = 1$, $d_{22} = 0$, $d_{23} = 3$, $d_{24} = 7$, $d_{25} = 14$
  $d_{31} = 3$, $d_{32} = 3$, $d_{33} = 8$, $d_{34} = 6$, $d_{35} = 13$
  $d_{41} = 3$, $d_{42} = 5$, $d_{43} = 4$, $d_{44} = 1$, $d_{45} = 9$
- $y_j, 1 \leq j \leq 5$ values are delivered to each participant through a secure channel and $d_{ij}, 1 \leq i \leq 4, 1 \leq j \leq 5$ values are published.

3) Reconstruction: Since the threshold is 3, let us assume that the participants P_1, P_2 and P_5 cooperate in the reconstruction procedure. So, they perform the following operations to reconstruct the secret.

- Each particiapnt calculates his actual share for secret S_i i.e., the j^{th} participant calculates $Z_{ij} = (d_{ij} + f^i(y_j)) \bmod p_j$. Also they know from the public values that b_1, b_2 and b_3 are 1,2, and 0 respectively.
- Construct the secret S_4 by pooling shares Z_{41}, Z_{42}, Z_{45} and using CRT as follows:
  We have $M = 5 * 7 * 17 = 595$, $m_1 = 119, m_2 = 85, m_3 = 35$ and $N_1 = 4, N_2 = 1, N_3 = 1$

  Therefore, $S_4 = ((2 * 119 * 4) + (2 * 85 * 1) + (11 * 35 * 1)) \bmod 595 = 317$.
- Computing S''_3, S''_2, S''_1 by pooling shares $(Z_{31}, Z_{32}, Z_{35}), (Z_{21}, Z_{22}, Z_{25}), (Z_{11}, Z_{12}, Z_{15})$ respctively, we have,
  $S''_3 = ((0*119*4)+(5*85*1)+(14*35*1)) \bmod 595 = 320$;
  $S''_2 = ((2*119*4)+(1*85*1)+(13*35*1)) \bmod 595 = 302$; and
  $S''_1 = ((1*119*4)+(0*85*1)+(11*35*1)) \bmod 595 = 266$
- Since $b_3 = 0$, we have $S'_3 = S''_3 * 2 = 640$.
  Similarly $b_2 = 1$ implies that $S'_2 = (S''_2 * 2) + 1 = 605$ and $b_1 = 1$ implies that $S'_1 = (S''_1 * 2) + 1 = 533$.
- Construct secrets S_3, S_2, S_1 sequentially by evaluating the expression $S_i = S'_i - S_{i+1}$ as follows:
  $S_3 = S'_3 - S_4 = 640 - 317 = 323$
  $S_2 = S'_2 - S_3 = 605 - 323 = 282$
  $S_1 = S'_1 - S_2 = 533 - 282 = 251$
  Hence the required secrets.

F. Correctness

In the following correctneess of the proposed multi-stage multi-secret scheme is discussed.

Theorem The secrets can be reconstructed if and only if the set of participants reconstructing the secrets is an authorized set.

Proof

- **Case 1: S_l reconstruction**
  As explained in the reconstruction, each participant P_j, $1 \leq j \leq n$ can compute the actual share Z_{lj} corresponding to the secret $S_l = S'_l = S''_l$ from d_{lj}. Note that S''_l is such that $\beta < S''_l < \alpha$. This is because $S''_l = S'_l = S_l$ and $\beta < S_l < \alpha$. Since $\alpha = \prod_{i=1}^{k} P_i$ and $\beta = \prod_{i=0}^{k-2} P_{n-i}$, from the principle of CRT, any k or more participants will be able to reconstruct $S''_l = S_l$ where as any set of atmost $(k-1)$ participants will not be able to reconstruct the same.
- **Case 2: Reconstruction of remaining secrets**
  Following the same procedure explained in case 1, one can reconstruct S''_{l-1} and hence $S'_{l-1} = 2S''_{l-1} + b_{l-1}$ from which $S_{l-1} = S'_{l-1} - S_l$ can be computed. Similarly the other secrets can be recovered. Note that all this is possible by an authorized set and not by an unauthorized set. This is because the product of any $k-1$ primes is less than or equal to β; whereas the secrets S_i, $1 \leq i \leq l-1$ and hence S''_i lie in the interval (β, α).

V. Improved Multi-Stage Multi-Secret Sharing Scheme based on Mignotte's Sequence

Note that the previous scheme uses flag bits, which are made public, to keep track of whether the modified secrets are even

or odd. This increases the number of public values by $l-1$, where l is the number of secrets. But the number of public values is one of the parameters that determine the goodness of a scheme; that is, lesser the number of public values of a scheme better it is. Motivated by this observation, we hereby propose an improved scheme for multi-secrets. Overview and correctness of this scheme is similar to the previous one.

A. Distribution Phase

Algorithm 5 Distribution of Shares

1: For $i = 1, 2, \cdots, l$ and $j = 1, 2, \cdots, n$ do the following:
(i) Calculate $Z_{ij} = S_i \mod p_j$.
2: For $i = l$ and $j = 1, 2, \cdots, n$ do the following:
(i) Compute $d_{lj} = (Z_{lj} - f^l(y_j)) \mod p_j$
3: For $i = 1, 2, \cdots, l-1$ and $j = 1, 2, \cdots, n$ do the following:
(i) Compute $d_{ij} = Z_{ij} \oplus f^i(y_j) \oplus (S_{i+1} \mod p_j)$. That is convert $Z_{ij}, f^i(y_j)$ and $(S_{i+1} \mod p_j)$ to binary, exor these binary values, and assign the resulting value to d_{ij}.
4: Compute $F(r, Z_{ij})$, where r is a random value
5: Distribute y_j to each participant through a secure channel and publish all d_{ij}, $F(r, Z_{ij})$ values, r and two-variable one-way function $F(r, z)$.

B. Reconstruction

Secrets are reconstructed in sequential order starting from the l^{th}, secret. Any k participants can pool their shares and reconstruct these secrets.

Algorithm 6 Reconstruction of secrets

1: For $i = l$ and $j = 1, 2, \cdots, n$ do the following
2: calculate $Z_{lj} = (d_{lj} + f^l(y_j)) \mod p_j$.
3: For $i = l-1, l-2, \cdots, 1$ and $j = 1, 2, \cdots, n$ do the following :
4: calculate $Z_{ij} = (d_{ij} \oplus f^i(y_j) \oplus (S_{i+1} \mod p_j))$.
5: Any k participants can pool their shares and reconstruct the secrets $S_l, S_{l-1}, \cdots, S_1$ in a sequential order using CRT from the shares Z_{ij}.

Note:Verification is same as in the previous schemes.

C. Example

Let the values of the parameters be as in the example of the previous section.

1) Distribution: Only those steps that differ from the previous one are given. The difference is only in the calculation of the true and public values of the secrets.

- Compute $Z_{ij} = S_i \mod P_j$ for $i = 1, 2, 3, 4$ and $j = 1, 2, \cdots, 5$. This gives
  $Z_{11} = 1$, $Z_{12} = 6$, $Z_{13} = 9$, $Z_{14} = 4$, $Z_{15} = 13$
  $Z_{21} = 2$, $Z_{22} = 2$, $Z_{23} = 7$, $Z_{24} = 9$, $Z_{25} = 10$
  $Z_{31} = 3$, $Z_{32} = 1$, $Z_{33} = 4$, $Z_{34} = 11$, $Z_{35} = 0$
  $Z_{41} = 2$, $Z_{42} = 2$, $Z_{43} = 9$, $Z_{44} = 5$, $Z_{45} = 11$
- Compute public values $d_{ij} = (Z_{ij} \oplus f^i(y_j) \oplus (S_{i+1} \mod P_j)), 1 \le i \le 3, 1 \le j \le 5$
  $d_{11} = 11$, $d_{12} = 20$, $d_{13} = 15$, $d_{14} = 2$, $d_{15} = 3$
  $d_{21} = 0$, $d_{22} = 2$, $d_{23} = 1$, $d_{24} = 11$, $d_{25} = 25$
  $d_{31} = 3$, $d_{32} = 1$, $d_{33} = 9$, $d_{34} = 12$, $d_{35} = 10$
- Calculate $d_{4j} = (Z_{4j} - f^4(y_j)) \mod p_j, 1 \le j \le 5$
  $d_{41} = 3$, $d_{42} = 5$, $d_{43} = 4$, $d_{44} = 1$, $d_{45} = 9$
- $y_j, 1 \le j \le 5$ are given to each participant through a secure channel and $d_{ij}, 1 \le i \le 4, 1 \le j \le 5$ values are published.

2) Reconstruction: Assume that the participants P_1, P_2 and P_5 cooperate to reconstruct the secrets.

- Compute $Z_{4j} = (d_{4j} + f^4(y_j)) \mod p_j$ for $j = 1, 2,$ and 5
- Construct the secret S_4 as 317 by pooling shares $Z_{41} = 2, Z_{42} = 2, Z_{45} = 11$ and using CRT
  Compute $Z_{ij} = (d_{ij} \oplus f^i(y_j) \oplus (S_{i+1} mod p_j))$ for $i = 3, 2, 1$ and $j = 1, 2, \cdots, 5$
  Compute S_3 as 323, S_2 as 282, S_1 as 251 by pooling shares $(Z_{31}, Z_{32}, Z_{35}), (Z_{21}, Z_{22}, Z_{25}), (Z_{11}, Z_{12}, Z_{15})$ respectively.

D. Comparison

The comparison between the previous Multi-Stage Secret sharing scheme and Improved Scheme is shown below.

VI. Proposed single secret sharing scheme based on Asmuth-Bloom sequence

Overview of the scheme

Initially, the dealer comes up with the number of participants (n), threshold value (k), the secret (S) to be shared among the participants $P_1, P_2, \cdots, P_n$, one way function (f), value γ and Asmuth-Bloom sequence $p_0, p_1, p_2, \cdots, p_n$ to be used. Also the delaer chooses random values $y_i, 1 \le i \le n$, and distributes them one each to the participants (i.e y_i to P_i) as the pseduo shares of the participants. The dealer modifies the secret to $X = S + \gamma p_0$ and then computes the (real) shares of the participants P_i, $1 \le i \le n$, from X. Now the dealer applies the chosen one-way function f to each of these random numbers (y_i), subtracts each of these resulting numbers $f(y_i)$ from the corresponding real shares $Z_i, 1 \le i \le n$ of the participants and distribute the chosen random numbers y_i to the participants P_i. While reconstructing the secret, the participants first apply one-way function to the pseudo share, which they possess, adds the resulting value $f(y_i)$ to the corresponding public share and recovers the actual shares, Z_i. These shares are then used to recover X using CRT, from which the actual secret S is reconstructed.

A. Distribution

- Let the chosen (k, n) Asmuth-Bloom sequence be $p_0, p_1, p_2, \ldots, p_n$.

TABLE I
COMPARISON

S.No	Property	Previous Scheme	Improved Scheme
1	No. of Public values	$ln + (l-1)$	(ln)
2	Information Leak	Leak information to intruders	No information is leaked
3	Computionally Security	Less secure	More secure

- Choose $y_1, y_2, \cdots, y_n$ such that $y_i \in Z_{p_i}$ as the pseudo shares.
- Choose the secret S such that $S \in Z_{p_0}$
- Modify secret S to $X = (S + \gamma p_0)$, where γ is an arbitary integer such that $\beta < (S + \gamma p_0) < \alpha$ where $\beta = p_0 \prod_{i=0}^{k-2} P_{n-i}$ and $\alpha = \prod_{i=1}^{k} P_i$.
- Compute shares $Z_i = X \bmod p_i, 1 \leq i \leq n$.
- Compute $d_i = (Z_i - f(y_i)) \bmod p_i$ as the shift values, where f is the chosen one way function.
- For every $i, 1 \leq i \leq n$, deliver y_i to the i^{th} participant through a secure channel and publish d_i

B. Reconstruction

- Each participant calculates his actual share by computing $Z_i = (d_i + f(y_i)) \bmod p_i$.
- The modified secret X is reconstructed from the shares Z_i of k participants using CRT.
- The original secret S is then reconstructed using $S = X \bmod p_0$

C. Example:

The proposed scheme is hereby illustrated with artificially small parameters.

1) Distribution:

- Consider a publicly known $(3, 4)$ Asmuth-Bloom sequence. Let it be 3,11,13,17,19.
- Let the random values be: $y_1 = 3, y_2 = 4, y_3 = 8, y_4 = 5$ and the chosen one-way function be the exponentiation of 2 modulo 17.
- Consider the secret as 2, as $2 \in Z_{p_0}$
- We need to consider γ such that $\beta < (S + \gamma p_0) < \alpha$ where $\beta = p_0 \prod_{i=0}^{k-2} P_{n-i}$ and $\alpha = \prod_{i=1}^{k} P_i$. So choose $\gamma = 431$ which gives $X = (2 + 431 * 3) = 1295$
- Computing $Z_i = X \bmod p_i$.
  $Z_{i_1} = 1295 \bmod 11 = 8$, $Z_{i_2} = 1295 \bmod 13 = 8$, $Z_{i_3} = 1295 \bmod 17 = 3$, $Z_{i_4} = 1295 \bmod 19 = 3$
- Computing shift values by $d_i = [Z_i - f(y_i)] \bmod p_i$.
  $d_1 = (8 - 8) \bmod 11 = 0$, $d_2 = (8 - 16) \bmod 13 = 5$, $d_3 = (3 - 1) \bmod 17 = 2$, $d_4 = (3 - 15) \bmod 19 = 7$.

  These values are made public and y_i,$i = 1, 2, \cdots, n$ are privately delivered to the participants.

2) Reconstruction:

- Any participant, say Z_1, Z_2, Z_3 wants to pool their shares and reconstruct the secret.
  Hence they calculate their actual shares by $Z_i = (d_i + f(y_i)) \bmod p_i$.
  $Z_1 = (0 + 8) \bmod 11 = 8$,
  $Z_2 = (5 + 16) \bmod 13 = 8$, and
  $Z_3 = (2 + 1) \bmod 17 = 3$.
- The secret is reconstructed from the following equations using CRT.

$$S \equiv 1 \bmod 11,$$
$$S \equiv 12 \bmod 13,$$
$$S \equiv 2 \bmod 17$$

  We have $M = 11*13*17 = 2431$, $M_1 = 2431/11 = 221$, $M_2 = 187$, $M_3 = 143$
  and $N_1 = 1$,$N_2 = 8$,$N_3 = 5$
  Therefore, $X = [(8 * 221 * 1) + (8 * 187 * 8) + (3 * 143 * 5)] \bmod 2431 = 1295$
  and the secret $S = 1295 \bmod 3 = 2$,
  Hence the secret.

VII. PROPOSED MULTI-STAGE MULTI-SECRET SHARING SCHEME BASED ON ASMUTH-BLOOM SEQUENCE

Overview of the scheme

The dealer initializes all the parameters and chooses the required multiple secrets S_i, $1 \leq i \leq l$, as against the single secret of the previous scheme. In the distribution phase, the chosen secrets except the last are modified to S_i' by adding two consecutive secrets, i.e. $S_i' = S_i + S_{i+1}$. Successful reconstruction of the secrets is possible only when $(S_i + \gamma p_0)$ lies between $p_0 \prod_{i=0}^{t-2} P_{n-i}$ and $\prod_{i=1}^{t} P_i$. So as to bring the modified secrets (i.e $S_i' = S_i + S_{i+1}$) to this range, we divide the modified secrets by 2. The resulting values are the new modified secrets (S_i''). Again from these modified secrets X values are computed, from which the actual shares (Z_{ij}) of the participants are generated. From the actual shares $Z_{ij}, 1 \leq i \leq l, 1 \leq j \leq n$, and the pseudo shares $y_1, y_2, \cdots, y_n$ public values are computed. Verification values are also derived from the actual shares. Both the sets, i.e the set of the public and the the set of the verification values are made public. The random values (i.e. pseudo shares $y_1, y_2, \cdots, y_n$) which were chosen by the dealer are distributed privately to each participant. In the verification phase, any participant can compute the hash value by using the verification function and check whether they are equal to the published verification values or not.

In the reconstruction phase, participants can compute their actual shares by adding the images of the one-way function

of their secret shadows to the public values. CRT is used to reconstruct the X values, from which modified secrets are computed and if the flag bit corresponding to the modified secret is 1, then the modified secret is multiplied by 2 and 1 is added to it. Otherwise the modified secret is just multiplied by 2. The actual secrets are then computed from these modified secrets.

A. Initialization

In this phase, all the variables are intialized and the secrets are chosen.

Algorithm 7 Initialization

1: Let $\{P_1, P_2, \cdots, P_n\}$ be the n participants and k be the threshold value.
2: Consider a publicly known (k, n) Asmuth-Bloom sequence, say $p_0, p_1, p_2, \ldots, p_n$.
3: Randomly choose n secret shadows $y_1, y_2, \cdots, y_n$ such that $y_i \in Z_{p_i}$ as the pseudo shares.
4: Choose the secrets $S_1, S_2, \cdots, S_l$ such that $S_i \in Z_{p_0}$, $1 \leq i \leq l$.

B. Distribution

In the distribution phase, actual secrets are modified except the last. Shares are computed from these modified secrets.

Algorithm 8 Distribution of Shares

1: Compute $S_i' = S_i + S_{i+1}$, for $i = 1, 2, \cdots, l-1$
2: If $(S_i' \bmod 2 == 1)$ then, $S_i'' = (S_i' - 1)/2$ and $b_i = 1$, for $1 \leq i \leq l-1$
Otherwise, $S_i'' = S_i'/2$ and $b_i = 0$, for $1 \leq i \leq l-1$
3: $S_l'' = S_l' = S_l$
4: $X_i = (S_i'' + \gamma p_0)$, where γ is an arbitary integer such that $(S_i + \gamma p_0)$ lies between $p_0 \prod_{i=0}^{t-2} P_{n-i}$ and $\prod_{i=1}^{t} P_i$.
5: For $i = 1, 2, \cdots, l$ and $j = 1, 2, \cdots, n$ do
Begin
6: Compute $Z_{ij} = X_i \bmod p_j$
7: Compute $d_{ij} = (Z_{ij} - f^i(y_j)) \bmod p_j$, where f is a one way function and $f^i(x)$ denotes i successive applications of f to x.
8: Compute $F(r, Z_{ij})$, where r is a random value
End
9: Distribute y_j to each participant through a secure channel and publish all d_{ij}, $F(r, Z_{ij})$ values, r and two-variable one-way function $F(r, z)$.

C. Verification

In this phase, each participant can verify the allocated shares. Reconstructor also can verify the shares provided by the participants.

Algorithm 9 Verification of shares

1: Participants can verify their shares by calculating $F(r, Z_{ij})$, where Z_{ij} itself can be computed by using pseudo shares and the corresponding public values.
2: Similarly, reconstructor also can verify honesty of the other participants by computing $F(r, Z_{ij})$.

D. Reconstruction

Secrets are reconstructed in sequential order starting from the last, i.e the l^{th} secret. Any k participants can pool their shares and reconstruct these secrets.

Algorithm 10 Reconstruction of secrets

1: Each participant $j, 1 \leq j \leq n$, willing to take part in the reconstruction, calculates $Z_{ij} = (d_{ij} + f^i(y_j)) \bmod p_j$, $1 \leq i \leq l$
Case 1: If $i = l$
2: Construct X_l value from corresponding shares Z_{lj} using CRT.
3: Compute $S_l = S_l' = S_l'' = (X_l \bmod p_0)$
Case 2: For $i = l-1, l-2, \cdots, 1$ **do the following:**
4: Construct X_i using CRT from the shares Z_{ij}
5: Construct $S_i'' = X_i \bmod p_0$
6: $S_i' = S_i'' * 2$
7: If $b_i = 1$, $S_i' = S_i' + 1$
8: Compute the i^{th} secret as $S_i = S_i' - S_{i+1}$

E. Example

We hereby illustrate the proposed scheme with artificially small parameters.

1) Initialization:

- Consider a group of 5 participants $\{P_1, P_2, P_3, P_4, P_5\}$ wherein 3 participants are sufficient to reconstruct the secret. That is the number of participants, n, is 5 and the threshold, k, is 3.
- Consider the Asmuth-Bloom sequence as 8,17,23,29,31,37 (where $p_0 = 8$)
- Let the random values be: $y_1 = 6, y_2 = 13, y_3 = 24, y_4 = 29, y_5 = 35$ and one-way function $f(x) = 2^x \bmod 43$
- Consider the secrets to be $S_1 = 2, S_2 = 3, S_3 = 5, S_4 = 7$ which lie in Z_{p_0}.

2) Distribution:

- Compute $S_i' = S_i + S_{i+1}$ for $i = 1, 2, 3$ so that we have $S_1', S_2', S_3' and S_4'$ as $5, 8, 12 and 7$ respectively.
- Check the condition $(S_i' \bmod 2 == 1)$ and correspondingly compute S_i'',
$S_1'' = (5-1)/2 = 2$ and $b_1 = 1$
$S_2'' = 8/2 = 4$ and $b_2 = 0$
$S_3'' = 12/2 = 6$ and $b_3 = 0$
$S_4'' = S_4' = 7$
- Compute $X_i = (S_i'' + \gamma p_0)$, consider $\gamma = 1200$ as $(S_i'' + \gamma p_0)$ should lie between $p_0 \prod_{i=0}^{t-2} P_{n-i}$ and $\prod_{i=1}^{t} P_i$. Therefore, $X_1 = 9602, X_2 = 9604, X_3 = 9606, X_4 = 9607$

TABLE II
COMPARISON OF EXISTING AND PROPOSED SCHEMES

S.No	Scheme	Multi-Secret	Reusable	No.of public values	Sequence used
1	Mignotte Scheme(existing)	Single	No	No pulic values	Mignotte Sequence
2	Asmuth-Bloom Scheme(existing)	Single	No	No pulic values	Asmuth-Bloom Sequence
3	Reusable Single Secret Sharing Scheme I	Single	No	No pulic values	Mignotte Sequence
4	Proposed Multi-Stage Multi-Secret Sharing Scheme I	Multi	Yes	ln+(l-1)	Mignotte Sequence
5	Improved Multi-Stage Multi-Secret Sharing Scheme	Multi	Yes	ln	Mignotte Sequence
6	Reusable Single Secret Sharing Scheme II	Single	Yes	No public values	Asmuth-Bloom Sequence
7	Proposed Multi-Stage Multi-Secret Sharing Scheme II	Multi	Yes	ln+(l-1)	Asmuth-Bloom Sequence

- Compute $Z_{ij} = X_i \bmod p_j$, for $i = 1,2,3,4$ and $j = 1,2,3,4,5$. This gives
  $Z_{11} = 14$, $Z_{12} = 11$, $Z_{13} = 3$, $Z_{14} = 23$, $Z_{15} = 19$
  $Z_{21} = 16$, $Z_{22} = 13$, $Z_{23} = 5$, $Z_{24} = 25$, $Z_{25} = 21$
  $Z_{31} = 1$, $Z_{32} = 15$, $Z_{33} = 7$, $Z_{34} = 27$, $Z_{35} = 23$
  $Z_{41} = 2$, $Z_{42} = 16$, $Z_{43} = 8$, $Z_{44} = 28$, $Z_{45} = 24$

- Compute public values $d_{ij} = (Z_{ij} - F^i(y_j)) \bmod p_j, 1 \leq i \leq 4, 1 \leq j \leq 5$
  $d_{11} = 10$, $d_{12} = 12$, $d_{13} = 26$, $d_{14} = 21$, $d_{15} = 14$
  $d_{21} = 8$, $d_{22} = 18$, $d_{23} = 21$, $d_{24} = 21$, $d_{25} = 20$
  $d_{31} = 0$, $d_{32} = 16$, $d_{33} = 6$, $d_{34} = 11$, $d_{35} = 21$
  $d_{41} = 0$, $d_{42} = 21$, $d_{43} = 6$, $d_{44} = 4$, $d_{45} = 20$

- $y_j, 1 \leq j \leq 5$ values are delivered to each participant through a secure channel and $d_{ij}, 1 \leq i \leq 4, 1 \leq j \leq 5$ values are published.

3) Reconstruction: Since the threshold is 3, let us assume that the participants P_1, P_2 and P_5 cooperate in the reconstruction procedure. So, they perform the following operations to reconstruct the secret.

- Each participant calculates his actual share for secret S_i i.e. the j^{th} participant calculates $Z_{ij} = (d_{ij} + f^i(y_j)) \bmod p_j$. Also they know public values b_1, b_2 and b_3 i.e. 1,0 and 0 respectively.

- Construct the value X_4 by pooling shares Z_{41}, Z_{42}, Z_{45} and using CRT as follows:
  We have $M = 17 * 23 * 37 = 14467$, $m_1 = \frac{M}{17} = 851, m_2 = \frac{M}{23} = 629, m_3 = \frac{M}{37} = 391$
  and $N_1 = 1, N_2 = 3, N_3 = 30$

  Therefore, $S_4 = ((2 * 851 * 1) + (16 * 629 * 3) + (24 * 391 * 30)) \bmod 14467 = 9607$.

- Now calculate secret S_4 as $S_4 = X_4 \bmod p_0$ so that $S_4 = 9607 \bmod 8 = 7$, Hence the secret S_4
- Compute X_3, X_2, X_1 by pooling shares $(Z_{31}, Z_{32}, Z_{35}), (Z_{21}, Z_{22}, Z_{25}), (Z_{11}, Z_{12}, Z_{15})$ respectively. Therefore,
  $X_3 = ((1*851*1)+(15*629*3)+(29*391*30)) \bmod 14467 = 9606$
  $X_2 = ((16*851*1)+(13*629*3)+(21*391*30)) \bmod 14467 = 9604$
  $X_1 = ((14*851*1)+(11*629*3)+(19*391*30)) \bmod 14467 = 9602$

- Compute S_3'', S_2'', S_1'' Therefore,
  $S_3'' = X_3 \bmod p_0 = 9606 \bmod 8 = 6$
  $S_2'' = X_2 \bmod p_0 = 9604 \bmod 8 = 4$
  $S_1'' = X_1 \bmod p_0 = 9602 \bmod 8 = 2$

- Since $b_3 = 0$, we have $S_3' = S_3'' * 2 = 12$
  and $b_2 = 0$, we have $S_2' = (S_2'' * 2) = 8$
  also since $b_1 = 1$, we have $S_1' = (S_1'' * 2) + 1 = 5$

- Construct secrets S_3, S_2, S_1 sequentially using the expression $S_i = S_i' - S_{i+1}$ and arrive at
  $S_3 = S_3' - S_4 = 12 - 7 = 5$
  $S_2 = S_2' - S_3 = 8 - 5 = 3$
  $S_1 = S_1' - S_2 = 5 - 3 = 2$
  Hence the required secrets.

F. Correctness

Correctness of the scheme is same as the one given in section 4 except that X values replace S'' values and that $S_i = X_i \bmod p_0$ for $1 \leq i \leq l$.

VIII. OUR RESULTS

Three Schemes that use the Mignotte's Sequence and then two Schemes that use the Asmuth-Bloom Sequence proposed by this paper. The first and the fourth Schemes are designed for single secret; whereas the remaining three Schemes are designed for multiple secrets. Among the proposed Schemes, third Scheme is an improvement over the Second one in the sense that it reduces the number of required public values. Also discussed in the paper is the correctness of the schemes. Novelty of our schemes, in contrast to the existing schemes is that the shares are reusable. Table II represents the comparative analysis of existing schemes (Mignotte and Asmuth-Bloom) and proposed schemes.

IX. CONCLUSIONS

In this paper, we have proposed three secret sharing schemes that use the Mignotte's sequence and two secret sharing schemes that use the Asmuth-Bloom sequence. All these five secret sharing schemes are based on Chinese Remainder Theorem (CRT). The first scheme that uses the Mignotte's sequence is a single secret scheme. It is extended to the multi-stage multi-secrets in the second scheme, which is later improved to result in a third scheme. The first scheme that uses the Asmuth-Bloom sequence is designed for the case of

a single secret and the second one is an extension of the first scheme to the case of multi-secrets. A novel feature of our schemes is that the shares of the participants are reusable, i.e, same shares can be used even with a new set of secrets. It also checks the dealer participant's honesty. This feature finds its use if the dealer distributes fake shares to the participants or a participant may provide a fake share to other participants in reconstruction. Correctness of the scheme is also discussed.

REFERENCES

[1] M. Mignotte. *How to share a secret*. In T. Beth, editor,Cryptography-Proceedings of the Work-shop on Cryptography, Burg Feuerstein, 1982, volume 149 of Lecture Notes in Computer Science,pp. 371-375. Springer-Verlag, 1983

[2] Asmuth, C., Bloom, J.: *A modular approach to key safeguarding*. IEEE Transactions on Information Theory IT-29(2),pp. 208-210 (1983)

[3] G. R. Blakley, *Safeguarding cryptographic keys*, AFIPS, Vol. 48 (1979), pp. 313-317.

[4] Shamir, A. 1979. How to share a secret. Comm. ACM 22, 612-613.

[5] Tompa, M., Woll, H. *How to share a secret with cheaters*, J. Cryptology 1(2), pp. 133-138 (1988)

[6] "Anjaneyulu Endurthi.,Appala Naidu Tentu.,V.Ch.Venkaiah. *Reusable Multi-stage Multi-secret Sharing Scheme Based on Asmuth-Bloom Sequence*. Proceedings of International Conference on Communication Computing and Information Technology, Department of Computer Science, M.O.P. Vaishnav College for Women (Autonomous), Chennai, Tamil Nadu, India. 12 th and 13 th December 2014."

[7] D. Pasaila, V. Alexa, and S. Iftene, *Cheating detection and cheater identification in crt-based secret sharing schemes*.IACR Cryptology ePrint Archive, vol. 2009, p. 426, 2009.

[8] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem*. Applications in Computing,Coding, Cryptography. Singapore: World Scientific, 1996.

[9] J. He, E. Dawson, *Multistage secret sharing based on one-way function*, Electronics Letters 30 (19) (1994) 1591-1592.

[10] J. He, E. Dawson, *Multisecret-sharing scheme based on one-way function*, Electronics Letters 31 (2) (1995) 93-95.

[11] L. Harn, *Comment: Multistage secret sharing based on one-way function*, Electronics Letters 31 (4) (1995) 262.

[12] L. Harn, *Efficient sharing (broadcasting) of multiple secrets*, IEEE Proceedings-Computers and Digital Techniques 142 (3) (1995) 237-240.

[13] M. Stadler, *Publicly verifiable secret sharing*, Advances in Cryptology, EUROCRYPT-96, Lecture Notes in Computer Science, vol.1070, Springer-Verlag, 1996, pp.190-199.

[14] Subba Rao Y V and C. Bhagvati, *CRT based threshold multi secret sharing scheme*,International Journal of Network Security, vol. 16, no. 3, pp. 194-200, 2014.

[15] H.Y. Chien, J.K. Jan, Y.M. Tseng, *A practical (t, n) multi-secret sharing scheme*, IEICE Transactions on Fundamentals E83-A (12) (2000) 2762-2765.

Anjaneyulu Endurthi Currently serving as Lecturer in Rajiv Gandhi University of Knowledge Technologies (IIIT), Basar, India. He obtained his Master of Technology (MTech) in Computer Science from University of Hyderabad, in 2014 and Bachelor of Technology (BTech) in Computer Science & Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2008. His research interests includes Cryptography and Cyber Security.

Oinam Bidyapati Chanu Currently persuing her Master of Technology in Computer Science from University of Hyderabad, India. She has obtained her Bachelor of Technology from National Institute Of Technology, Durgapur(NIT D), India in 2011.

Appala Naidu Tentu is a Research Scientist at CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science (AIMSCS), University of Hyderabad Campus. He obtained his Master of Technology (MTech) in Computer Science from National Institute of Technology, Suratkal (NITK) in 2010 and Master of Science (M.Sc) from Andhra University, in 2007. Currently, he is pursuing his PhD in Computer Science from JNTU Hyderabad. His research interests are in the areas of cryptography, cryptanalysis and design of security protocols.

V. Ch. Venkaiah obtained his Ph.D. in 1988 from the Indian Institute of Science (IISc), Bangalore, India, in the area of Scientific Computing. He worked for several organizations including the Central Research Laboratory of Bharat Electronics, Tata Elxsi India Pvt. Ltd., Motorola India Electronics Limited, all in Bangalore. He then moved onto academics and served IIT Delhi, IIIT Hyderabad, and C R Rao Advanced Institute of Mathematics, Statistics, and Computer Science. He is currently serving the University of Hyderabad, India.