International Journal of Computer Applications (0975 - 8887)
International Conference on Communication, Computing and Information Technology (ICCCMIT-2014)

Reusable Multi-Stage Multi-Secret Sharing Scheme Based on Asmuth-Bloom Sequence

Anjaneyulu Endurthi
School of Computer and Information Sciences, University of Hyderabad Hyderabad-500046, India

Appala Naidu Tentu
CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science, Hyderabad-500046, India

V. Ch. Venkaiah
School of Computer and Information Sciences, University of Hyderabad Hyderabad-500046, India

ABSTRACT

Two secret sharing schemes that use Asmuth-Bloom sequence and are based on Chinese Reminder Theorem (CRT) are proposed in this paper. The first scheme 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 multi-secret sharing scheme. Further, the schemes are capable of verifying the honesty of the participants including the dealer. Correctness of the schemes is also discussed.

Keywords:

Multi-Secret, Mignotte's sequence, Asmuth-Bloom sequence, CRT, Secret sharing scheme.

1. 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[5]. 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. A typical scenario wherein the multi-secret sharing problem occurs is as follows. In these schemes, every participant only needs to keep 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.
Suppose that a company has K 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 employees/-participants according to a specific threshold access structure.The company may use multiple secret sharing schemes to share these secrets. However each 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. In a threshold multi-secret sharing scheme multiple secrets can be packed into one major secret such that each component secret is still controlled by a single shadow; whereas in CRT based threshold secret sharing schemes, each participant will have a separate shadow for each secret and reconstruction is done sequentially.
Dectection of cheaters:
A verifiable secret-sharing scheme [18] 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. These abilities are very important. For example, a dishonest dealer can cheat some

shareholders by giving them fake shadows. Communication errors (i.e., noise) can also 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.
The following subsections defines Mignotte's and Asmuth-Bloom's schemes.

1.1 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,

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

1.2 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 $I_i = (S + \gamma p_0) \bmod p_i$ for all $1 \leq i \leq n$
Where γ is an arbitary integer such that $(S + \gamma p_0) \in Z_{p_1 \cdots p_t}$
—Distribute share $I_i, 1 \leq i \leq n$ to n 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

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

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

1.3 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 $r' \neq r_i$.

2. RELATED WORK

Secret sharing scheme that uses Mignotte's sequence and is based on CRT is introduced in [1], and it is modified to result in another scheme by Asmuth-Bloom [2]. J. He, E. Dawson [14], proposed a multi-stage secret sharing scheme based on one way function in 1994 [16], [17] and [15]. They used Lagrange interpolation polynomial in order to perform secret sharing. Later in 2000, Chien et al. [20] proposed a new type of (t, n) multi-secret sharing scheme based on the systematic block codes. Subba Rao Y V and Chakravarthy Bhagvati [19] came up with a multi-stage secret sharing schemes based on CRT. In the later scheme multiple secrets are shared to different groups, such that each group receives share of the secret intended for it.

2.1 Motivation

Mignotte's and Asmuth-Bloom Schemes can be used whenever we have a single secret. They are not capable of handling multiple secrets. The proposed scheme can be extended to handle multiple secrets.

2.2 Our Results

Proposed a secret sharing scheme that uses Asmuth-Bloom sequence. It can be seen to be a variant of Asmuth-Bloom scheme. The proposed scheme is then extended to a multi-stage multi-secret sharing scheme. Correctness of both the schemes is discussed. A novel feature of our scheme, apart from being extendable to multi-satge multi-secret sharing scheme, is that the shares are reusable. That is the same set of shares can be used even with a different set of secrets.

3. PROPOSED SCHEME

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 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 partici-

pants $P_1, P_2, \cdots, P_n$, 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 $y_i, 1 \leq i \leq n$ and distributes them one each to the participants (i.e y_i to P_i) as the pseduo shares of the participants. The dealer modifies the secret to X and then computes the (real) shares of the participants Z_i of P_i, $1 \leq i \leq n$ 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 $(Z_i, 1 \leq i \leq n)$ 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 i.e Z_i. These shares are then used to recover X using CRT, from which actual secret S is reconstructed.

3.1 Distribution

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

—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 by computing $X = (S + \gamma p_0)$, Where γ is an arbitary integer such that $(S + \gamma p_0) \in Z_{p_1 \cdots p_k}$

—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

3.2 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 can be reconstructed using $S = X \bmod p_0$

3.3 Example:

We hereby illustrate the proposed scheme with artificially small parameters.

3.3.1 Distribution

—Consider a publicly known $(3, 4)$ Asmuth-Bloom sequence. Let it be 3,11,13,17,19.

—Let the random values be: $y_1 = 3, y_2 = 4, y_3 = 8, y_4 = 5, y_5 = 10$ and the chosen one-way function be the modulo exponentiation of 2 ($2^x \bmod 17$).

—Consider the secret as 2, as $2 \in Z_{p_3}$

—We need to consider γ such that $(S + \gamma p_0) \in Z_{p_1 \cdots p_k}$. So choose $\gamma = 51$ which gives $X = (2 + 51 * 3) = 155 \in Z_{p_1 \cdots p_k}$

—Computing $Z_i = X \bmod p_i$.
$Z_{i_1} = 155 \bmod 11 = 1$, $Z_{i_2} = 155 \bmod 13 = 12$, $Z_{i_3} = 155 \bmod 17 = 2$, $Z_{i_4} = 155 \bmod 19 = 3$

—Computing shift values by $d_i = Z_i - f(y_i) \bmod p_i$.
$d_1 = (1 - 8) \bmod 11 = 4$, $d_2 = (12 - 16) \bmod 13 = 9$, $d_3 = (2 - 1) \bmod 17 = 1$, $d_4 = (3 - 15) \bmod 19 = 7$.
These values are made public and y_i,$i = 1, 2, \cdots, n$ are privately delivered to the participants.

3.3.2 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 $Z_i = (d_i + f(y_i)) \bmod p_i$.
$Z_1 = (4 + 8) \bmod 11 = 1$, $Z_2 = (9 + 16) \bmod 13 = 12$ and $Z_3 = (1 + 1) \bmod 17 = 2$.

—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, $X = [(1 * 221 * 1) + (12 * 187 * 8) + (2 * 143 * 5)] \bmod 2431 = 1586$
and the secret $S = 1586 \bmod 3 = 2$, Hence the secret.

4. PROPOSED MULTI-STAGE MULTI-SECRET SHARING SCHEME

Overview of the scheme

In the initialization phase, dealer initializes Asmuth-Bloom sequence i.e $p_0, p_1, p_2, \cdots, p_n$, number of participants n, threshold value k, and choses the secrets $S_i, 1 \leq i \leq l$. The dealer also choses secret shadows $y_1, y_2, \cdots, y_n$, value γ , a one-way function f and a verification function F. In the distribution phase, the chosen secrets are modified by adding two consecutive secrets. Successful reconstruction of the secrets is possible only when the secrets lie between 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 the modified secrets by 2. The resulting values are the new modified secrets (S''). 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 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 or not. In the reconstruction phase, participants can compute their actual shares by adding the images of 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 multiplied by 2. The actual secrets are then computed from these modified secrets.

4.1 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 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 $S_i \in Z_{p_0}$, $1 \leq i \leq l$.

4.2 Distribution

In the distribution phase, actual secrets are 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: 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 $(S + \gamma p_0) \in Z_{p_1 \cdots p_k}$
For $i = 1, 2, \cdots, l$ and $j = 1, 2, \cdots, n$ do the following:
5: Compute $Z_{ij} = X_i \bmod p_j$
6: 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 $i \geq 1$
7: Compute $F(r, Z_{ij})$, where r is a random value
8: 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 $F(r, z)$.

4.3 Verification

In this phase, each participant can verify the allocated shares. 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 and the corresponding public values.
2: Similarly, reconstructor also can verify honesty of the other participants by computing $F(r, Z_{ij})$.

4.4 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 4 Reconstruction of secrets

1: Each participant $j, 1 \leq j \leq n$, willing to take part in the reconstruction, calculates $Z_{ij} = (d_{ij} + f^i(y_j)) \bmod p_j$, $1 \leq i \leq l$
Case 1: If $i = l$
2: Construct X_l value from corresponding shares Z_{lj} using CRT.
3: From X_l value, $S_l = S'_l = S''_l = (X_l \bmod p_0)$ is costructed and hence the secret S_l
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 $S_i = S'_i - S_{i+1}$

4.5 Example

We hereby illustrate the proposed scheme with artificially small parameters.

4.5.1 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_8}.

4.5.2 Distribution

—Computes $S'_i = S_i + S_{i+1}$ for $i = 1, 2, 3$.
$S'_1 = S_1 + S_2 = 2 + 3 = 5$
$S'_2 = S_2 + S_3 = 3 + 5 = 8$
$S'_3 = S_3 + S_4 = 5 + 7 = 12$
$S'_4 = S_4 = 7$

—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 $\gamma = 89$ as $(S''_i + \gamma p_0)$ should lie in $Z_{p_1, p_2, \ldots, p_k}$. Therefore, $X_1 = 714, X_2 = 716, X_3 = 718, X_4 = 719$

—Compute $Z_{ij} = X_i \bmod p_j$, for $i = 1, 2, 3, 4$ and $j = 1, 2, 3, 4, 5$. This gives
$Z_{11} = 0, Z_{12} = 1, Z_{13} = 18, Z_{14} = 1, Z_{15} = 11$
$Z_{21} = 2, Z_{22} = 3, Z_{23} = 20, Z_{24} = 3, Z_{25} = 13$
$Z_{31} = 4, Z_{32} = 5, Z_{33} = 22, Z_{34} = 5, Z_{35} = 15$
$Z_{41} = 5, Z_{42} = 6, Z_{43} = 23, Z_{44} = 6, Z_{45} = 16$

—Compute public values $d_{ij} = (Z_{ij} - F^i(y_j)) \bmod p_j, 1 \leq i \leq 4, 1 \leq j \leq 5$
$d_{11} = 13, d_{12} = 2, d_{13} = 12, d_{14} = 30, d_{15} = 6$
$d_{21} = 11, d_{22} = 8, d_{23} = 7, d_{24} = 30, d_{25} = 12$
$d_{31} = 3, d_{32} = 6, d_{33} = 21, d_{34} = 20, d_{35} = 13$
$d_{41} = 3, d_{42} = 11, d_{43} = 21, d_{44} = 2, d_{45} = 12$

—$y_j, 1 \leq j \leq 5$ 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.

4.5.3 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 $M = 17 * 23 * 37 = 14467$, $m_1 = 851, m_2 = 629, m_3 = 391$
and $N_1 = 1, N_2 = 3, N_3 = 30$

Therefore, $S_4 = ((5 * 851 * 1) + (6 * 629 * 3) + (16 * 391 * 30)) \bmod 14467 = 719$.

—Now calculate secret S_4 by $S_4 = X_4 \bmod p_0$ implies $S_4 = 719 \bmod 89 = 7$, 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,
$X_3 = ((4*851*1)+(5*629*3)+(15*391*30)) \bmod 14467 = 718$
$X_2 = ((2*851*1)+(3*629*3)+(13*391*30)) \bmod 14467 = 716$
$X_1 = ((0*851*1)+(1*629*3)+(11*391*30)) \bmod 14467 = 714$

—Compute S_3'', S_2'', S_1'' Therefore,
$S_3'' = X_3 \bmod p_0 = 718 \bmod 8 = 6$
$S_2'' = X_2 \bmod p_0 = 716 \bmod 8 = 4$
$S_1'' = X_1 \bmod p_0 = 714 \bmod 8 = 2$

—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 by evaluating the expression $S_i = S_i' - S_{i+1}$ as follows:
$S_3 = S_3' - S_4 = 12 - 7 = 5$
$S_2 = S_2' - S_3 = 8 - 5 = 3$
$S_1 = S_1' - S_2 = 5 - 3 = 2$
Hence the required secrets.

5. SECURITY ANALYSIS

In this section, correctneess of the proposed multi-stage multi-secret scheme is discussed.

5.1 Correctness

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 value X_l. Note that X_l is such that $X_l \in Z_{p_1,p_2,\ldots,p_k}$. From the principle of CRT, any k or more participants will be able to reconstruct X_l where as any set of atmost $(k-1)$ participants will not be able to reconstruct the same. Further, from the obtained X_l, the required secret $S_l = S_l' = S_l''$ is reconstructed.

—**Case 2: Reconstruction of remaining secrets**
Following the same procedure explained in case 1, one can reconstruct X_{l-1} and hence S_{l-1}'' and $S_{l-1}' = 2S_l'' + b_{l-1}$ from which $S_{l-1} = S_{l-1}' - S_{l+1}$ 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 modified secrets X_i lies in $Z_{p_1,p_2,\ldots,p_k}$

6. CONCLUSIONS

In this paper, we have proposed a secret sharing scheme that uses Asmuth-Bloom sequence and it is based on the Chinese Remainder Theorem. This scheme is then extended to multi-stage multi-secret sharing scheme. 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.

7. 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] Blakley, G. R., Kabatianski, A., Ideal perfect threshold schemes and MDS codes, ISIT95, p. 488, 1995.

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

[6] G.J.Simmons., How to (Really) Share a secret, Advances in Cryptology-CRYPTO'88,LNCS,403(1990),pp.390-448.

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

[8] Cabello, S., Padro, C., Saez, G. Secret sharing schemes with detection of cheaters for a general access structure. In: Ciobanu, G., P un, G. (eds.) FCT 1999. LNCS, vol. 1684, pp. 185-194. Springer, Heidelberg (1999)

[9] Carpentieri, M., De Santis, A., Vaccaro, U. Size of shares and probability of cheating in threshold schemes. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 118-125. Springer, Heidelberg (1994)

[10] Ogata, W., Kurosawa, K., Stinson, D.R. Optimum secret sharing scheme secure against cheating. SIAM J. Discrete Math. 20(1),pp. 79-95 (2006)

[11] Goldreich, O., Ron, D., Sudan, M. Chinese remainder with errors. IEEE Trans. Inform. Theory, 2000, IT-46, pp. 1330-1338.

[12] 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.

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

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

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

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

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

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

[19] 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.

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