CRT Based Threshold Multi Secret Sharing Scheme

Subba Rao Y V and Chakravarthy Bhagvati
(Corresponding author: Subba Rao Y V)

Department of CIS, University of Hyderabad, Hyderabad, India Pin 500046.
(Email: yvsrcs@uohyd.ernet.in)

(Received Apr. 19, 2012; revised and accepted Dec. 19, 2012)

Abstract

This paper presents a novel secret sharing system that is based on Chinese remainder theorem. This scheme deals with a concept of multiple secrets to be shared to different groups, such that each group receives shares of secret intended for it. The sharing is a threshold scheme, that is more than a fixed number of members from any particular group, will be able to reconstruct the secret and any smaller set will not be able to know what it is. Resource requirements here are not very high as in other cryptography schemes and is suitable for resource constrained environment for establishing session key or any such random secrets which they can use for short time.

Keywords: Chinese remainder theorem, multiple secrets, threshold Secret sharing

1 Introduction

Cryptography is an ancient art/science that deals with information security. From classical systems such as shift cipher system, hill cipher system etc., to modern crypto systems such as RSA, AES, ElGamal, ECC etc., and also in, various useful techniques such as secret sharing schemes, zero knowledge proofs, digital signature schemes etc., many mathematical topics play very crucial role. Among these topics, Chinese remainder theorem (CRT) is an important topic. Applications of CRT are mainly seen in cryptography literature in reducing the high exponentiation cost of RSA decryption process [17] and many papers such as [5, 6, 7, 9, 11], etc., use CRT for implementing/improving efficiency of various algorithms by splitting or sharing encrypted information into smaller units and thus increase the security of those algorithms. [4] is a book that discusses the role of CRT in computing, coding and cryptography in detailed manner. In [12], it was demonstrated that CRT can also be used as an encryption function where the decryption function is a simple division operation to get the remainder, which happens to be the hidden secret. Then [13], extended the scheme of [12] to a scheme that can send shared secrets to members of groups, such that all of them together can reconstruct the secret, using a different layer of CRT. This paper discusses an unobserved limitation of this encryption scheme in [13] and improves it to overcome the limitation and also extends it to a more general threshold scheme to encrypt multiple secrets to different groups, such that members of the group more than a specified threshold number can reconstruct the secret. Secret sharing schemes in [1, 2, 3, 8, 10, 16, 18, 21] may provide some lines on which the schemes presented in this paper can be further improved.

In this paper, Section 2 presents a brief explanation of CRT, schemes of [12] and [13] and then explains the limitation of [12] and [13]. Section 3 explains the proposed scheme and Section 4 gives some applications of these schemes along with possible lines of improvement as future work.

2 CRT and Communication Schemes

2.1 Chinese Remainder Theorem

Chinese remainder theorem assures existence of solution for system of congruence relations (unique modulo some M). For a given system of congruences as

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\vdots \\ x &= a_k \pmod{m_k}. \end{aligned}$$

For some positive integer k, with only condition that, these m_i's are pairwise co-prime. The detailed proof of CRT can be seen in any Number theory/Cryptography books such as [17], but the brief outline is presented here.

Define some variables as

$$M = m_1 * m_2 * \ldots * m_k = \prod_{i=1}^{k} m_i. \quad (1)$$

$$M_i = M/m_i. \quad (2)$$

$$y_i = M_i^{-1} \pmod{m_i}. \quad (3)$$

Now the unique solution $\pmod{M}$ is

$$x = (\sum_{i=1}^{k} a_i * M_i * y_i) \pmod{M}. \quad (4)$$

This construction gives a unique x (modulo M) that can satisfy the given system of congruences.

2.2 CRT Communication Scheme-I

This is a brief summary of scheme in [12]. The environment for this scheme has a single dealer D and a set of n users $U_1, U_2, \ldots U_n$, see Figure 1. This scheme can be dealt in two phases, set-up phase and communication phase. In set-up phase, D chooses n pairwise co-prime (positive) integers $m_1, m_2, \ldots m_n$. Each m_i is privately communicated by D to user U_i (this can be done with the help of any public key system or using any non cryptographic means). At the end of this, each user U_i will be having m_i, which the user can use as a key for decrypting the cipher received from dealer D. In second phase, that is, communication phase, for encryption, dealer D with data a_1, a_2, ..., a_n, where each a_i is intended for user U_i and only for U_i. These a_i's are chosen from the ranges 0 to $m_i - 1$. Dealer shall first compute x using CRT, such that x satisfies set of congruences $x = a_i \pmod{m_i}$, for $i = 1, 2, \ldots, n$. From CRT we know that, this x is unique upto $\pmod{M}$, where M is the product of all m_is. Then this x is communicated to all users. For decryption, each user U_i after receiving x, using his key m_i, shall compute a_i as $x \pmod{m_i}$. For others who have no knowledge of m_i, will not be able to know, what the a_i is, as shown in Section 4.1.

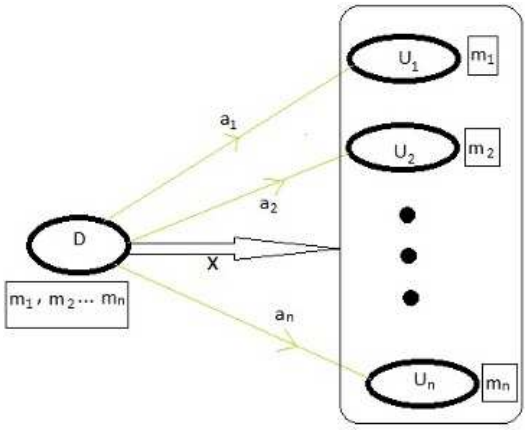

Figure 1: CRT Scheme-I

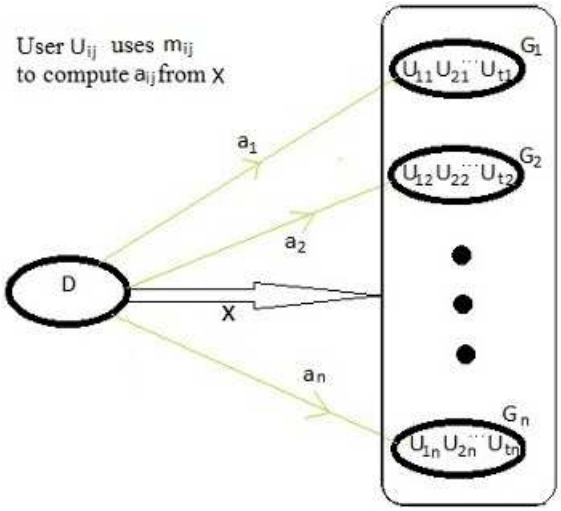

Figure 2: CRT Scheme-II

2.3 CRT Communication Scheme-II

This is a breif summary of scheme in [13], and this deals with Dealer D communicating n secrets to n different groups $G_1, G_2, \ldots, G_n$, see Figure 2. Here it is assumed that each group G_i has t members in it. For the sake of simplicity we assumed t users for each group, this number can be different for different groups. In Set-up phase of this scheme, let D choose $n * t$ pair wise co-prime (positive) integers, $m_{11}, m_{21}, \ldots m_{t1}$, $m_{12}, m_{22}, \ldots m_{t2}, \ldots, m_{1n}, m_{2n}, \ldots m_{tn}$. Each m_{ij} is privately communicated to user U_{ij}, i^{th} member of j^{th} group (this can be done as in Scheme 2.2). At the end of this, each user U_{ij} will be having m_{ij}, which the user can use as a key for decrypting the cipher received from dealer D. After this, dealer also computes group key m_i for each group G_i as $m_i = \prod_{k=1}^{t} m_{ki}$.

In communication phase, the dealer D, chooses secret data $a_1, a_2, \ldots, a_n$, with each a_i is from the ring Z_{m_i}. Here, each a_i is intended to be sent only for users of group G_i, but not for others. Dealer shall first compute x using CRT, such that x satisfies set of congruences $x = a_i \pmod{m_i}$, for i ranging from 1 to n. From CRT we know that, this x is unique upto $\pmod{M}$, where M is the product of all m_is. Then this x is communicated to all users. For decryption, where each user U_{ij} after receiving x, using his key m_{ij}, shall compute a_{ij} as $x \pmod{m_{ij}}$. For others who have no knowledge of m_{ij}, they will not be able to do this. Together all users of j^{th} group have t, a_{ij}'s, so they have t congruences as $x = a_{ij} \pmod{m_{ij}}$ for i ranging from 1 to t. Now they can solve for this x using CRT again. As the solution of x in CRT is unique modulo m_j, the group can get back their secret a_j, which happens to be the unique value.

2.4 Limitations of Schemes

Few limitations to the above schemes are discussed in [12] and [13]. First is, if the values of m_i's are very small (say 8 bits to handle ASCII) and if the same m_i's are used to encrypt a sequence of characters, this can lead to a attack where one can try with all possible m_i's, until one sees a meaningful decryption of characters. This can be avoided by using m_i's of at least 100 bits in size, so that this above brute force type of attack becomes infeasible. The second limitation is, if the same secret is to be transmitted to all, then this encryption scheme will not mask the secret. Few alternates to deal with such situation are, first is to send $M + X$, second is to add some kind of padding for at least one user, etc..

An important, unobserved problem/limitation in Scheme-II is, once the decryption process is over to reconstruct a_j of group G_j, every member of the group will have the secret keys of all other members of the group. This essentially means, that this system is only suitable as a one time use system. In the next section we suggest modification of Scheme II, such that, keys of members are not directly used in decryption process.

3 Proposed CRT Schemes

3.1 Reusable CRT Multi Secret Scheme

This scheme also has two phases. First one is set up phase to establish reusable keys m_{ij}'s. Second phase is communication phase and has two sub phases where first is to establish session keys and second is to actually communicate secret data.

In Set-up phase, let D choose $n * t$ pair wise co-prime (positive) integers, $m_{11}, m_{21}, \ldots m_{t1}$, $m_{12}, m_{22}, \ldots m_{t2}, \ldots$, $m_{1n}, m_{2n}, \ldots m_{tn}$. Each m_{ij} is privately communicated to user U_{ij}, i^{th} member of j^{th} group in a secured way. At the end of this, each user U_{ij} will be having m_{ij}, which the user can use as a key for decrypting the cipher received from dealer D. After this, dealer also computes group key m_i for each group G_i as $m_i = \prod_{k=1}^{t} m_{ki}$.

Communication phase in each session, has a sub phase to set up temporary keys for that session. For this, the dealer D first chooses temporary keys $q_{11}, q_{21}, \ldots q_{t1}$, $q_{12}, q_{22}, \ldots q_{t2}, \ldots$, $q_{1n}, q_{2n}, \ldots q_{tn}$, one for each user, such that, these keys can be used for reconstruction/Decryption Phase. These keys are also chosen to be pairwise co-prime(within each group) positive integers and also for each i, j in the ranges of reference they satisfy the requirement $m_{ij} \geq q_{ij}$. These temporary keys can be communicated to users, using Scheme in Section 2.2. Dealer also stores these products as $q_i = \prod_{k=1}^{t} q_{ki}$, for each i and will be using these q_is to determine the range of secrets.

Now to communicate secret data $a_1, a_2, \ldots, a_n$, for n groups where, each a_i is from the ring Z_{q_i}, i.e in range from 1 to $q_i - 1$. Here, each a_i is intended to be sent only for users of group G_i, but not for others. Dealer shall first compute a_{ij}'s, such that $a_{ij} = a_j \pmod{q_{ij}}$. Now calculate x, using CRT, such that x satisfies set of congruences $x = a_{ij} \pmod{m_{ij}}$, for i ranging from 1 to t and j ranging from 1 to n. From CRT we know that, this x is unique upto $\pmod{M}$, where M is the product of all m_{ij}s. Then this x is communicated to all users. For decryption again using Scheme I above, where each user U_{ij} after receiving x, using his key m_{ij}, shall compute a_{ij} as $x \pmod{m_{ij}}$. For others who have no knowledge of m_{ij}, they will not be able to do this. Together all users of j^{th} group have t, a_{ij}'s, so they have t congruences as $x = a_{ij} \pmod{q_{ij}}$ for i ranging from 1 to t. Now they can solve for this x using CRT again. As the solution of x in CRT is unique modulo q_j, the group can get back their secret a_j, which happens to be that unique value.

This can be written in the form of an algorithm as

1) Set-up phase:
   (a) Dealer D chooses $n * t$ pair wise co-prime (positive) integers, $m_{11}, m_{21}, \ldots m_{t1}$, $m_{12}, m_{22}, \ldots m_{t2}, \ldots$, $m_{1n}, m_{2n}, \ldots m_{tn}$.
   (b) Each m_{ij} is privately communicated to user U_{ij}.
   (c) Computes group key m_i for each group G_i as $m_i = \prod_{k=1}^{t} m_{ki}$.
2) Session key phase:
   (a) Dealer D chooses temporary keys $q_{11}, q_{21}, \ldots q_{t1}$, $q_{12}, q_{22}, \ldots q_{t2}, \ldots$, $q_{1n}, q_{2n}, \ldots q_{tn}$, one for each user. These keys are chosen to be pairwise co-prime(within each group) positive integers and also for each i, j in the ranges of reference they satisfy $m_{ij} \geq q_{ij}$.
   (b) These temporary keys can be communicated to users, using Scheme of Section 2.2.
   (c) Computes group key q_i for each i as $q_i = \prod_{k=1}^{t} q_{ki}$ as range of secret for group G_i.
3) Secret Data communication:
   (a) D chooses secret data to communicate as $a_1, a_2, \ldots, a_n$, for n groups where, each a_i is in the range from 1 to $q_i - 1$. Here, each a_i is intended to be sent only for users of group G_i, but not for others.
   (b) Compute a_{ij}'s, such that $a_{ij} = a_j \pmod{q_{ij}}$.
   (c) Calculate x, using CRT, such that x satisfies set of congruences $x = a_{ij} \pmod{m_{ij}}$, for i ranging from 1 to t and j ranging from 1 to n.
   (d) This x is communicated to all users.

From this x, users of groups can reconstruct secrets as

1) User U_{ij} shall compute $a_{ij} = x \pmod{m_{ij}}$.
2) All users of j^{th} group can compute their secret by solving for y in $y = a_{ij} \pmod{q_{ij}}$ for i ranging from 1 to t.

3.2 Threshold Scheme

Here we suggest threshold scheme, where a secret is sent in encrypted form to n users and if t is the threshold such that $1 \leq t \leq n$, then any t or more users together can reconstruct/decrypt the secret. Lesser number of users will not be able to know the secret. For this we use a binary matrix S of order $n \times r$, where n represents number of users and r represents parts of key. Entries of S are s_{ij} such that s_{ij} is 1 if j^{th} part of key is to be given to user i and 0 otherwise. We construct this matrix S to satisfy the following property - that is, consider the rows of S as set of vectors and let $v_1, v_2, \ldots v_k$ be any sub set of this vectors set and lastly let v be the vector obtained by the XORing the vectors in the above subset. The property we want S to satisfy is the Hamming weight of the v obtained as above is r if and only if $k \geq t$. We call, any binary matrix that satisfies this property as sharing matrix of size (n, t) and use them for the scheme to be proposed here. An example of $(3, 2)$ sharing matrix A is

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Now the actual scheme can be explained by looking at both set-up and communication phases. In set-up phase, to deal with n users, with threshold t, dealer D chooses a (n, t) sharing matrix A of order $n \times r$, for some positive integer r. Then, D also chooses r pairwise coprime positive integers $m_1, m_2, \ldots m_r$. These m_is are distributed to n users, such that each user U_j is given some m_is based on j^{th} row of A. The simple rule used here is, if matrix entry A_{ji} is 1, then m_i is given to U_j and if matrix entry A_{ji} is 0, then m_i is not given to U_j. The product of all m_is given to U_j is denoted as M_j. Lastly, D also computes $M = \prod_{k=1}^{r} m_k$, so that the possible range for secret can be from 1 to $M - 1$. Now, let S be the secret to be communicated to all users, such that any t of them can reconstruct it and smaller number cannot. To send this S, D just computes S_j for j from 1 to n, such that $S_j = S \pmod{M_j}$ and then sends them to respective users, using basic CRT based communication scheme that is scheme in Section 2.2. If we use a_i as representation for $S \pmod{m_i}$, for i from 1 to r. After receiving S_j, user U_j can compute some a_i's for those m_i's which are given to him. If any t users are together, since XORed weight of those t rows of A is r, they know all m_i's and hence the corresponding a_i's are known to at least one user. So t of them together can construct the unique value S that satisfies $S = a_i \pmod{m_i}$ for i from 1 to r, using CRT and thus they know what the secret is.

This can be written in the form of an algorithm as

1) Set-up phase:
   (a) Dealer D Chooses a (n, t) secret sharing matrix A of order $n \times r$.
   (b) D also chooses r pairwise coprime positive integers $m_1, m_2, \ldots m_r$.
   (c) These m_i's are distributed to n users, such that each user U_j is given m_i's corresponding to 1's in j^{th} row of A.
   (d) D computes M_j for $1 \leq j \leq n$ as product m_i's given to user U_j and also computes M as product of all m_i's.
2) Secret Sharing:
   (a) D Chooses a secret S in the range $1 \leq S \leq M - 1$ and compute S_j for $1 \leq j \leq n$ as $S_j = S \pmod{M_j}$.
   (b) Each S_j is communicated to user U_j secretly using scheme such as basic communication scheme discussed in Section 2.2.
3) Secret Reconstruction:
   (a) Each user U_j from S_j can compute a_i's for those m_is which are given to him as $a_i = S_j \pmod{m_i}$.
   (b) Any t of the user together can construct the unique value S that satisfies $S = a_i \pmod{m_i}$ for i from 1 to r, using CRT.

3.3 Multi Secret Threshold Scheme

In this dealer D deals with more than one group, we shall call these groups as $G_1, G_2, \ldots G_z$. Let us use n_i and t_i to represent number of users and threshold number in group G_i. Dealer first chooses z sharing matrices A_i for i ranging from 1 to z, each of size (n_i, t_i) and of order $n_i \times r_i$ for some positive integers r_i. Then D chooses set of pairwise coprime keys for users as $K = \{m_{ij} : 1 \geq i \geq z \text{ and } 1 \geq j \geq r_i\}$, such that for any fixed i in the specified range $K_i = \{m_{ij} : 1 \geq j \geq r_i\}$ is the key set intended for group G_i. These keys of K_i are distributed to members of G_i using the sharing matrix A_i as explained in the previous scheme. Secret S_i for each group G_i is chosen from the range from 1 to M_i, where $M_i = \prod_{k=1}^{r_i} m_k$. Then D can use CRT to compute X that satisfies congruences $X = S_i \pmod{M_i}$. This X is sent to all by broadcasting it. For decrypting any t_i members of group G_i with all elements of key set K_i can again use CRT to reconstruct their secret S_i.

1) Set-up phase:
   (a) Dealer first chooses z sharing matrices A_i for i ranging from 1 to z, each of size (n_i, t_i) and of order $n_i \times r_i$ for some positive integers r_i.
   (b) Then D chooses set of pairwise coprime keys for users as $K = \{m_{ij} : 1 \geq i \geq z \text{ and } 1 \geq j \geq r_i\}$, such that for any fixed i in the specified range $K_i = \{m_{ij} : 1 \geq j \geq r_i\}$ is the key set intended for group G_i.
   (c) These keys of K_i are distributed to members of G_i using the sharing matrix A_i as explained in the previous scheme.

2) Secret Sharing:

   (a) Secret S_i for each group G_i is chosen from the range from 1 to M_i, where $M_i = \prod_{k=1}^{r_i} m_k$.

   (b) Then D can use CRT to compute X that satisfies congruences $X = S_i \pmod{M_i}$.

   (c) This X is sent to all by broadcasting it.

3) Secret Reconstruction:

   (a) Any t_i members of group G_i with all elements of key set K_i can again use CRT to reconstruct their secret S_i.

4 Analysis of CRT schemes

4.1 Security Analysis

Security of CRT schemes can be proved as a consequence of the following theorem.

Theorem 1. *Even with the knowledge of $n-1$ pairs of (a_i, m_i), for $i = 1, 2, \ldots n-1$ and the cipher x in CRT communication scheme discussed in Section 2.2, it is not possible to guess what the a_n is, without the knowledge of m_n.*

Proof. To prove this, we shall show that for many choices of a_n and m_n can be computed to satisfy the requirement $x = a_n Mod(m_n)$. Let us start with some arbitrary value for a_n say α, then consider the variables defined as,

$$\begin{aligned} y &= x - \alpha. \\ M_n &= \prod_{i=1}^{n-1} m_i. \\ d &= gcd(y, M_n). \\ \beta &= y/d. \end{aligned}$$

From this computation, if $\beta > \alpha$, we can consider β as m_n and this will serve our requirement, since β divides $(x-\alpha)$, we have $x = \alpha \pmod{\beta}$. If $\beta \leq \alpha$ we can start again with a new choice of a_n. This proves the randomness of a_n, as desired. □

Lemma 1. *CRT Communication Scheme-II is secure scheme.*

Proof. As a consequence of Theorem 1, participants of any $n-1$ groups and also $t-1$ participants of the group in consideration will not be able to determine the share of one participant who is not involved and thus the secret of his group. □

Lemma 2. *Reusable CRT Multi Secret Scheme is secure.*

Proof. As a consequence of Theorem 1, all participants other than U_{ij} will not be able to determine what q_{ij} is. Thus the secret of group G_j is also secure. □

Lemma 3. *Threshold Scheme is secure scheme.*

Proof. From the definition of sharing matrix, we know that hamming weight of rows corresponding to lesser than t users is less than r. Thus there are some m_i's not known to these users and the shares associated with these m_i can take random values as shown in Theorem 1. □

Apart from security, we are also interested in economic use of space for efficient communication. In our scheme each a_i is from space Z_{m_i} and needs $log_2(m_i)$ bits of space and the encrypted message x is from space Z_M which is approximately sum of all $log_2(m_i)$s. Thus there is no real increase in size as in many other encryption systems.

Computation requirements are quite limited for our scheme and for decryption it just computes a mod operation.

In spite of all these positive aspects there are few limitations to this scheme. First and important one is, if the values of m_i's are very small (say 8 bits to handle ASCII) and if the same m_i's are used to encrypt a sequence of characters, then in the event of having knowledge of $n-1$ m_i's can lead to a attack where one can try with all possible m_i's, until one sees a meaningful decryption of characters. To over come this limitation we recommend use of m_i's of at least 100 bits in size, so that above brute force type of attack becomes infeasible.

The second limitation is, if the same secret is to be transmitted to all, then this encryption scheme will not mask the secret. This is demonstrated in the example bellow.

Example 1. *Here we continue with same m_i's, that is $97, 99, 101$ for U_1, U_2 and U_3 respectively.*
Assume that secrets for U_1, U_2 and U_3 is same and it is $a_1 = a_2 = a_3 = 2$, then dealer will have new system of congruences

$$\begin{aligned} x &= 2 Mod(97) \\ x &= 2 Mod(99) \\ x &= 2 Mod 101) \end{aligned}$$

From the expression
$x = a_1 * M_1 * y_1 + a_2 * M_2 * y_2 + a_3 * M_3 * y_3$,
we now have
$x = 1699830 + 1449956 + 729828 = 3879614$.

Considering $ModuloM$, we have $x = 2$, we need not be surprised of this, as this is the only unique value modulo 969903 to satisfy our system we started working with in this example. This is always true when ever the secret is same for all users.

Few simple tricks can save us in such situations. First alternate is to send 969905 that is $M+2$. Second alternate is to add some kind of padding for at least one user. Third alternate is to add a dummy user with a different secret and some new m_{n+1} as key parameter.

4.2 Comparision with Sharing Schemes

Here we compare our scheme with secret sharing schemes of [14, 15, 19, 20, 22]. Runhua et al'. in [15] presented a (t, n)- threshold multi-secret sharing scheme that

Table 1: Comparison of secret sharing schemes

Parameter	Ours	[11]	[12]	[13]	[14]
Parameters in Public	1	$n+1+p-t$	$t+1$	$n+p+1$	$n+1$
Parameters in Private	n	n	$n(2t+1)$	n	0
Operation Complexity	Low	High	High	High	High
Selective Revealing of Secrets	Yes	No	No	No	No
Verification	No	No	No	Yes	No

uses ECDLP to add verifiability of the shares given by dealer/user. Runhua et al'.s [14] improves Yang et al'.s scheme in [22] by reducing the complexity involved in secret reconstruction. Wang et al'. in [19] presented a multi-secret sharing scheme that deals with dynamic threshold using Elliptic Curves and Bilinear Maps.

The entries in the table given in Table 1 are worst case values for respective schemes. Our scheme allows reuse of keys (m_i's) as in other schemes except [14]. The number of parameters to be displayed in public for our approach is only one as we will be displaying only x, where as the no.of parameters in other approaches are ranging from $t+1$ to $N+p+1$. This is major achievement of our approach when compared to the other approaches. Above all, the complexity of reconstruction of secrets is low in our approach when compared to the other approaches, as they all involve computation of lagrange's interpolation for solving system of equations, which increases the computational complexity of these approaches to a large extent. Our approach deals with a simple division operation, which obviously has less computational complexity compared to lagrange's interpolation. In our approach the dealer can send different secrets to different groups, thus secrets are selectively revealed to the groups. Thus group G_i can only receive its secret a_i and not the secrets meant for other groups. [20] presented a scheme that deals with multiple secrets for genaralized threshold with weighted participants, which can give future direction for improving our scheme.

5 Conclusion and Future Work

The above given scheme is a simple but secured and efficient scheme as proved in analysis section. Future work can look on obtaining some compression of data to make a real and very useful scheme. Also these scheme can be modified to add verfication of dealer and other participants and also to deal with genaralized threshold scheme with weighted participants.

Acknowledgments

The authors would like to thank Ms Rukma Rekha, Ms Anupama and Dr, S Durga Bhavani for their support and help. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] T. Y. Chang, M. S. Hwang, and W. P. Yang, "An improvement on the lin-wu (t, n) threshold verifiable multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 163, no. 1, pp. 169–178, 2005.

[2] T. Y. Chang, M. S. Hwang, and W. P. Yang, "A new multi-stage secret sharing scheme using one-way function," *ACM Operating Systems Review*, vol. 39, no. 1, pp. 48–55, 2005.

[3] T. Y. Chang, M. S. Hwang, and W. P. Yang, "An improved multi-stage secret sharing scheme based on the factorization problem," *Information Technology and Control*, vol. 40, no. 3, pp. 246–251, 2011.

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

[5] S. Iftene. "Secret sharing schemes with applications in security protocols,". Tech. Rep. Technical report, University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science, University Alexandru Ioan Cuza of Iasi, 2007.

[6] K. Kaya and A. A. Selcuk, "Robust threshold schemes based on the chinese remainder theorem," in *Africacrypt*, pp. 94–108, 2008.

[7] K. Kaya and A. A. Selcuk, "A verifiable secret sharing scheme based on the chinese remainder theorem," in *Indocrypt*, LNCS 5365, pp. 414–425, Dalian, China, 2008.

[8] C. T. Li and M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181–2188, 2010.

[9] Q. Li, Z. Wang, X. Niu, and S. Sun, "A non-interactive modular verifiable secret sharing scheme," in *IEEE International Conference on Communications, Circuits and Systems (ICCCAS)*, pp. 84–87, Los Alamitos, 2005.

[10] J. Pieprzyk and X. M. Zhang, "Ideal secret sharing schemes from permutations," *International Journal of Network Security*, vol. 2, no. 3, pp. 238–244, 2006.

[11] M. Quisquater, B. Preneel, and J. Vandewalle, "On the security of the threshold scheme based on the

chinese remainder theorem," in *PKC 2002*, LNCS 2274, pp. 199–210, Heidelberg, 2002.

[12] S. Y. V. Rao and C. Bhagvati, "Crt based secured encryption scheme," in *2012 1st International Conference on Recent Advances in Information Technology (RAIT),*, pp. 11–13, Dhanbad, 2012.

[13] S. Y. V. Rao and C. Bhagvati, "Multi-secret communication scheme," in *ICIET 2012*, pp. 201–203, Mumbai, 2012.

[14] R. Shi, L. Huang, and H. Zhong, "An efficient (t, n)-threshold multi-secret sharing scheme," in *(IEEE) Workshop on Knowledge Discovery and Data Mining*, pp. 580–583, 2008.

[15] R. Shi, H. Zhong, and L. Huang, "A $(a(t, n)$-threshold verified multi-secret sharing scheme based on ecdlp," in *(IEEE) Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, pp. 9–13, 2007.

[16] R. Steinfeld, J. Pieprzyk, and H. Wang, "Lattice-based threshold changeability for standard shamir secret-sharing schemes," *IEEE Transactions on Information Theory*, vol. 53, no. 7, pp. 2542–2559, 2007.

[17] D. R. Stinson, *Cryptography Theory and Practice (3rd ed)*. Chapman and Hall/CRC, 2006.

[18] Y. Tian, C. Peng, and J. Ma, "Publicly verifiable secret sharing schemes using bilinear pairings," *International Journal of Network Security*, vol. 14, no. 3, pp. 142–148, 2012.

[19] S. J. Wang, Y. R. Tsai, and J. J. Shen, "Dynamic threshold multi-secret sharing scheme using elliptic curve and bilinear maps," in *(IEEE) Second International Conference on Future Generation Communication and Networking*, pp. 405–410, 2008.

[20] Y. Wu, X. Zhou, W. Du, and Y. Gao, "Threshold multi-secret sharing scheme for cheat-proof among weighted participants," in *(IEEE) Second International Symposium on Electronic Commerce and Security*, pp. 252–255, 2009.

[21] C. C. Yang, T. Y. Chang, and M. S. Hwang, "A (t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.

[22] C. C. Yang, T. Y. Chang, and M. S. Hwang, "A (t, n) multisecret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.

Subba Rao Y V is an Assistant Professor in the Department of Computer and Information Sciences, University of Hyderabad. His area of interests include Cryptography, Theory of Computation etc.

Chakravarthy Bhagvati is a Professor in the Department of Computer and Information Sciences, University of Hyderabad. His area of interests in- clude Cryptography, Image Processing, Indian Language OCR, Computer Networks, Traffic Modeling.