Multi-Secret Communication Scheme

Y. V. Subba Rao and Chakravarthy Bhagvati

***Abstract*—In this era of Information, exchange of digital data in various forms and formats is an important activity of human and computer networks. This digital communication pops up many security issues to keep the data and thus information reliable. This paper presents a secured scheme using Chinese remainder theorem to communicate multiple secrets in shared forms to disjoint groups of users and also presents a proof of security that this scheme can offer.**

***Index Terms*—*Multi*-secrets, Chinese Remainder Theorem, Secret shares.**

I. Introduction

Security of information is an important requirement of communication and there are many publications to address various aspects of this requirement. We look at couple of such aspects. One, bundling few messages together and sending a single cipher text to set of receiver, where each receiver can receive only the message intended for him or her. second is to share a secret to a group of receivers and they can only get the secret when all the shares are together. There are many papers on these two aspects with second one drawing attention of many with number of publications in past two decades. Shamir's algorithm in [1] is the one which created interest for many in this area. [1] uses a polynomial over finite field to share secret to *n* people and any *t* of the shares together can help one to reconstruct the secret. Later another important paper by Naor and Shamir [2] introduced a new secret sharing scheme called visual cryptography that can be used to share secret images to its users where only qualified subset(s) of them together can visually reconstruct the secret image from their shares. This paper combines the above two aspects, that is, it proposes a scheme to communicate multiple secrets in shared forms to disjoint groups of users, such that users of each group all together can and only can receive the secret message intended for them. To do this, we use a mathematical primitive called as Chinese Remainder Theorem (CRT). CRT is used in cryptography in various algorithms at various levels. One simple application of CRT in cryptography is to reduce the high exponentiation cost in RSA decryption process [3]. Later CRT was used by many for implementing/improving efficiency of various algorithms mainly by splitting or sharing encrypted information into smaller units and thus increase the security of those algorithms. [4] gives details about usage of CRT in computing, coding and cryptography. [5] explains about the security of the threshold scheme based on the Chinese Remainder Theorem. But, later many new results were presented using CRT. For instance [6] proposed a verifiable secret sharing scheme and later [7] proposed a verifiable threshold secret sharing scheme to decrease the size of shares without compromising on the security. But then [8] demonstrated that schemes in [6] and [7] can be attacked to have inconsistent shares and proposed a scheme to deal with consistent shares. [9] first gives robust threshold function sharing scheme for the RSA cryptosystem and then applies the ideas to the ElGamal and Paillier decryption functions. [10] proposes an algorithm to use CRT for embedding a secret in a gray scale picture to suggest a robust watermarking.

In all these and many other applications, CRT plays a good supporting role to provide/enhance security/efficiency. In this paper we made an attempt to use it as an encryption tool. Section 2 here presents a brief explanation of CRT, section 3 explains the encryption scheme of [11] and presents the proposed scheme and section 4 gives security analysis of the proposed scheme along with some possible lines of improvement as future work.

Manuscript received April 13, 2012; revised May 22, 2012.

Y. V. Subba Rao is with Department of CIS, University of Hyderabad, Hyderabad 500046 India (e-mail: yvsrcs@ uohyd.ernet.in).

Chakravarthy Bhagvati is with Department of CIS, University of Hyderabad, Hyderabad 500046 India (e-mail: chakcs@ uohyd.ernet.in).

II. Chinese Remainder Theorem

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

$x = a_1 Mod(m_1)$

$x = a_2 Mod(m_2)$

...

$x = a_k Mod(m_k).$

for some positive integer k, with only condition that this m_i's are pair wise co-prime.. Then from the proof of CRT, as given in many Number theory/Cryptography books such as [3], we define variables as

$M = m_1 * m_2 * ... * m_k.$
$M_i = M/m_i.$
$y_i = (M_i)^{-1} Mod(m_i).$

Now the unique solution mod (M) is

$$x=(a_1 * M_1 * y_1 + a_2 * M_2 * y_2 + ... + a_k * M_k * y_k) Mod(M). \quad (1)$$

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

Example

Consider the System of congruencies as x = 1Mod(95), x = 2Mod(99) and x = 1Mod(101). Here we have $a_1 = 1$, $a_2 = 2$, $a_3 = 1$ and $m_1 = 95$, $m_2 = 99$, $m_3 = 101$. Now from the above

sketch of CRT proof, we can see the following values $M = m_1 * m_2 * m_3 = 95*99*101 = 949905$. $M_1 = M/m_1 = 9999$, similarly $M_2=M/m_2= 9595$ and $M_3=M/m_3 = 9405$. Now we can compute inverses of M_i's as $y_1 = 9999^{-1} = 4\text{Mod}(95)$, $y_2= 9595^{-1} = 37\text{Mod}(99)$ and $y_3 = 9405^{-1} = 59\text{Mod}(101)$. From the expression (1), we have

$$x = (a_1 *M_1*y_1+a_2 *M_2*y_2+a_3 *M_3*y_3)\text{Mod}(949905)$$
$$= (39996 + 710030+ 554895)\ \text{Mod}(949905)$$
$$= 1304921\ \text{Mod}(949905) = 355016.$$

For this value of x, we can easily see that $x = 1\text{Mod}(95) = 2\text{Mod}(99) = 1\text{Mod}(101)$.

III. CRT-Communication Schemes

In this section we present two variants of CRT based communication schemes. First of these variants deals with a scenario, where a dealer *D* communicates with *n* users, where each user will be receiving secret intended for him only, more details of this are in [11]. In second variant dealer *D* communicates with *n* groups of user, where in each group, all users together can get their secret.

A. Scheme-I

Phase I: This is set-up phase. Consider the environment with a single dealer *D* and a set of *n* users $U_1,U_2,\ldots U_n$. Let *D* choose *n* pair wise co-prime numbers (positive integers) $m_1,m_2,\ldots m_n$. Each m_i is privately communicated to user U_i (this can be done with help of public key systems such as RSA or ElGammel or ECC etc). 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*.

Phase II: This is encryption phase, where the dealer *D*, posses data $a_1, a_2, \ldots, a_n$, with each a_i is from the ring Z_{mi} . Here, for $i = 1, 2, \ldots n$, each a_i is intended to be sent only for user U_i, but not for others. Dealer shall first compute *x* using CRT, such that *x* satisfies set of congruencies $x = a_i\text{Mod}(m_i)$, for *i* ranging from 1 to *n*. From CRT we know that, this *x* is unique upto Mod(*M*), where *M* is the product of all m_is. Then this *x* is communicated to all users.

Phase III: This is decryption phase, where each user U_i after receiving x, using his key m_i, shall compute a_i as $x\text{Mod}(m_i)$. For others who have no knowledge of m_i will not be able to know, what the a_i is, as it shown in next section.

B. Scheme-II

Phase I: Set-up phase for this proposed scheme assumes a single dealer *D* and a set of *n* groups $G_1, G_2, \ldots, G_n$, where each group G_i has *t* users $U_{1i},U_{2i},\ldots U_{ti}$ (for the sake of simplicity we assumed *t* users for each group, this number can different for different groups). Let *D* choose *n*t* pair wise co-prime numbers (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 with help of public key systems such as RSA or ElGammel or ECC etc). 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 $m_i = m_{1i}*m_{2i}*\ldots*m_{ti}$.

Phase II: This is encryption phase, where the dealer *D*, posses data $a_1, a_2, \ldots, a_n$, with each a_i is from the ring Z_{mi} . Here, for $i = 1, 2, \ldots n$, 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 congruencies $x = a_i\text{Mod}(m_i)$, for *i* ranging from 1 to *n*. From CRT we know that, this *x* is unique upto Mod(*M*), where *M* is the product of all m_is. Then this *x* is communicated to all users.

Phase III: This is decryption phase, where each user U_{ij} after receiving *x*, using his key m_{ij}, shall compute a_{ij} as $x\text{Mod}(m_{ij})$. For others who have no knowledge of m_{ij}, they will not be able to do this. Together all user of j^{th} group have *t* a_{ij}'s, so they have *t* congruencies as $x=a_{ij}\text{Mod}(m_{ij})$ 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 that unique value.

IV. Analysis of the Scheme

Security of the schemes can be proved by considering the following result. This proof is line with that of [11].

A. Lemma

In scheme I, even with the knowledge of *n*-1 pairs of (a_i , m_i), for $i = 1, 2, \ldots n$-1 and the cipher *x*, it is not possible to guess what the a_n is, without the knowledge of m_n.

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

$y = x - \alpha$

$d = \gcd(y, M_n)$ (this M_n is the product of all n-1 M_is known)

$\beta = y/d$

From this computation, if $\beta > \alpha$, we can consider β as m_n and this will serve our requirement, as $x=y+q$ and β divides *y*, we have $x=(y+q)\text{Mod}(\beta)=\alpha\ \text{Mod}(\beta)$. If $\beta > \alpha$ fails, we can start again with a new choice of a_n. This proves the randomness of a_n, and thus the lemma.

This lemma proves the security of our scheme1, by showing that even *n*-1 users with their key information are not in a state to know the n^{th} secret or key. If any smaller sub set of users are together, it is a weaker attack and only allows more randomness, this proves the security of scheme1. Scheme2 deals with groups instead of individuals. Same security proof can show that some of these groups cannot guess the secrets or keys of other groups. Within a group also, any number of users lesser then *t* will have no method to guess the keys or secrets of others of the same group.

B. Limitations

In spite of all these positive aspects there are few limitations to these schemes. First and important one is, if the values of m_i's are very small (say 8 bits to handle ASCII) and if such 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 overcome this

limitation we recommend use of mi's of at least 100 bits in size, so that brute force type of attack becomes infeasible.

The second limitation is, if the same secret is to be transmitted to all, this encryption scheme will not mask the secret, since the secret itself becomes the unique x to be communicated. Few simple tricks can save us in such nasty situation. First alternate is to send 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.

V. Conclusion

The above given schemes are simple but secured and efficient schemes as proved in analysis section. These schemes can be effectively used in areas such as session key establishment protocols that deal with one control point and many users and/or groups of users. Future work can look on lines of obtaining some compression of data to make them more practical and useful schemes.

References

[1] A. Shamir, "How to share a secret," in *Communications of the ACM* vol. 22, issue 11, Nov. 1979

[2] M. Naor and A. Shamir, "Visual Cryptography. Advances in Cryptology," *EUROCRYPT'94, LNCS 950*, *Springer-Verlag*, 1994, 287-298.

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

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

[5] M. Quisquater, B. Preneel, and J. Vandewalle, "On the security of the threshold scheme based on the Chinese Remainder Theorem," *PKC 2002, LNCS*, vol. 2274, Springer, Heidelberg , pp.199-210.

[6] Q. Li, Z. Wang, X. Niu, and S. Sun, "A noninteractive modular verifiable secret sharing scheme," *ICCCAS 2005: International Conference on Communications, Circuits and Systems*, IEEE, Los Alamitos, 2005, pp. 84-87.

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

[8] K. Kaya and A. A. Selcuk, "A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem," *INDOCRYPT 2008*, LNCS 5365, 2008, 414-425.

[9] K. Kaya and A. A. Selcuk, "Robust Threshold Schemes Based on the Chinese Remainder Theorem," *AFRICACRYPT 2008*, LNCS, 2008, 94-108.

[10] J. C. Patra, A. Karthik, and P. K. Meher, "Robust CRT-Based Watermarking Technique for Authentication of Image and Document," *IEEE International Conference on Systems, Man and Cybernetics (SMC 2008)*, 3250-3255.

[11] Y. V. S. Rao and C. Bhagvati, "CRT Based Encryption scheme," *RAIT* 2012, IEEE Xplore.