A Multi-secret Sharing Scheme Based on the CRT and RSA

Xuedong Dong
College of Information Engineering, Dalian University
10th Street, Dalian Economic Technological Development Zone, Dalian, Liaoning 116622, China
(Email: dongxuedong@sina.com)
(Received Sept. 10, 2013; revised and accepted July 23, 2014)

Abstract

In this paper, we propose to enhance threshold secret sharing schemes based on the Chinese remainder theorem (CRT) by incorporating the well-known RSA Cryptosystem.In the proposed scheme, participants select their secret shadows by themselves. Also, a secure channel among the dealer and participants is no longer needed. In addition,each participant can check whether another participant provides the true secret shadow or not.Furthermore, it allows to reconstruct several secrets parallelly. The scheme is based on the RSA cryptosystem and intractability of the Discrete Logarithm.

Keywords: Chinese remainder theorem; Discrete logarithm; RSA; Threshold secret sharing.

1 Introduction

In a (t, n)-threshold secret sharing scheme, a secret is shared among n participants in such a way that any t (or more) of them can reconstruct the secret while a group of $t-1$ or fewer can not obtain any information. The idea of a secret sharing scheme was first introduced independently by Shamir [16] and Blakley [3], both in 1979. A threshold secret sharing scheme has many practical applications, such as opening a bank vault, launching a nuclear, or authenticating an electronic funds transfer. There are several threshold secret sharing schemes based on the Chinese remainder theorem(CRT) [1, 2, 6, 7, 9, 11, 12, 13, 14, 17]. In these secret sharing schemes there are several common drawbacks as follows [18]:

1) Only one secret can be shared during one secret sharing process;
2) Once the secret has been reconstructed, it is required that the dealer redistributes a fresh shadow over a security channel to every participant;
3) A dishonest dealer may distribute a fake shadow to a certain participant, and then that participant would subsequently never obtain the true secret;
4) A malicious participant may provide a fake share to other participants, which may make the malicious participant the only one who gets to reconstruct the true secret.

In this paper, we propose to enhance threshold secret sharing schemes based on the CRT by incorporating the well-known RSA Cryptosystem invented by Rivest, Shamir, and Adleman [15]. The proposed threshold secret sharing scheme has the following features.

1) Participants select their secret shadows by themselves;
2) A secure channel among the dealer and participants is no longer needed;
3) Each participant can check whether another participant provides the true secret shadow or not;
4) It allows to reconstruct several secrets parallelly.

The scheme is based on the RSA cryptosystem and intractability of the Discrete Logarithm.

The rest of this paper is organized as follows. In Section 2, we give some preliminaries about the CRT. A brief review is given in Section 3, about threshold secret sharing schemes based on the CRT. In Section 4, we propose a new threshold secret sharing scheme based on the CRT by incorporating the well-known RSA Cryptosystem. Section 5 gives the analysis of the proposed scheme. Finally, concluding remarks are given in Section 6.

2 Preliminaries

Several versions of the CRT have been proposed. The next one is called the general CRT [4, 10].

Theorem 1. *Let $k \geq 2, p_1 \geq 2, \cdots, p_k \geq 2$, and $b_1, \cdots, b_k \in Z$. The system of equations*

$$\begin{cases} x \equiv b_1 (\text{mod } p_1) \\ x \equiv b_2 (\text{mod } p_2) \\ \quad \vdots \\ x \equiv b_k (\text{mod } p_k) \end{cases}$$

has solutions in Z if and only if $b_i \equiv b_j (\text{mod } (p_i, p_j))$, for all $1 \leq i, j \leq k$. Moreover, if the above system of equations has solutions in Z, then it has a unique solution in $Z_{[}p_1, \cdots, p_k]$, where $[p_1, \cdots, p_k]$ is the least common multiple of $p_1, \cdots, p_k$.

When $(p_i, p_j) = 1$, for all $1 \leq i, j \leq k$, one gets the standard version of the CRT. Garner [5] has found an efficient algorithm for this case and Fraenkel [4] has extended it to the general case.

3 Brief Reviews

3.1 Review of Mignotte's Threshold Secret Sharing Scheme

Mignotte's threshold secret sharing scheme [9] uses some special sequences of integers, referred to as the Mignotte sequences. Let n be a positive integer, $n \geq 2$, and $2 \leq t \leq n$. An (t, n)-Mignotte sequence is a sequence of pairwise co-prime positive integers $p_1 < p_2 < \cdots < p_n$ such that $\prod_{i=0}^{t-2} p_{n-i} < \prod_{i=1}^{t} p_i$.

Given a publicly known (t, n)-Mignotte sequence, the scheme works as follows:

1) The secret S is chosen as a random integer such that $\prod_{i=0}^{t-2} p_{n-i} < S < \prod_{i=1}^{t} p_i$,

2) The shares I_i are chosen as $I_i \equiv S (\text{mod} p_i)$, for all $1 \leq i \leq n$;

3) Given t distinct shares $I_{i_1}, \cdots, I_{i_t}$, the secret S is recovered, using the CRT, as the unique solution modulo $p_{i_1} \cdots p_{i_t}$ of the system.

$$\begin{cases} x \equiv I_{i_1} (\text{mod } p_{i_1}) \\ x \equiv I_{i_2} (\text{mod } p_{i_2}) \\ \quad \vdots \\ x \equiv I_{i_t} (\text{mod } p_{i_t}). \end{cases}$$

3.2 Review of Asmuth-Bloom's Threshold Secret Sharing Scheme

This scheme, proposed by Asmuth and Bloom in [1], also uses some special sequences of integers. More exactly, a sequence of pairwise co-prime positive integers $p_0, p_1 < p_2 < \cdots < p_n$ is chosen such that $p_0 \prod_{i=0}^{t-2} p_{n-i} < \prod_{i=1}^{t} p_i$.

Given a publicly known Asmuth-Bloom sequence, the scheme works as follows:

1) The secret S is chosen as a random element of the set Z_{p_0};

2) The shares I_i are chosen as $I_i = (S + \gamma p_0) (\text{mod } p_i)$, for all $1 \leq i \leq n$, where γ is an arbitrary integer such that $(S + \gamma p_0) \in Z_{p_1 \cdots p_t}$;

3) Given t distinct shares $I_{i_1}, \cdots, I_{i_t}$, the secret S is recovered as $S = x_0 (\text{mod } p_0)$, where x_0 is obtained,using the CRT, as the unique solution modulo $p_{i_1} \cdots p_{i_t}$ of the system

$$\begin{cases} x \equiv I_{i_1} (\text{mod } p_{i_1}) \\ x \equiv I_{i_2} (\text{mod } p_{i_2}) \\ \quad \vdots \\ x \equiv I_{i_t} (\text{mod } p_{i_t}). \end{cases}$$

4 Proposed Scheme

Let $\{P_1, P_2, \cdots, P_n\}$ be a set of participants and D the dealer of the scheme.The scheme needs a bulletin board.Only the dealer D can change and update the information on the bulletin board and other persons can read and download the information from the bulletin board.

4.1 Initialization phase

1) The dealer D chooses two strong primes $p = 2p^{'} + 1$ and $q = 2q^{'} + 1$, where $p^{'}$ and $q^{'}$ are also primes. Both p and q should be so safe that anybody can't factor $N = pq$ efficiently. Then the dealer chooses an integer g such that $1 < g < N, (g, N) = 1$ and $(g \pm 1, N) = 1$. Then the order of g is equal to $p^{'}q^{'}$ or $2p^{'}q^{'}$ [2]. D publishes system information $[g, N]$ on the bulletin board and keeps p and q in secret.Each participant P_j randomly chooses a secret integer s_j from $[2, N]$ as her/his own secret shadow, and computes $R_j = g^{s_j}(\mathrm{mod}\, N)$, and then sends R_j to D. D must make sure that R_i and R_k are different when $i \neq k$. If $R_i = R_k$, D asks these participants to choose secret shadows again until $R_1, \cdots, R_n$ are different.

2) D chooses the secret integer e, $1 < e < \phi(N) = (p-1)(q-1)$, such that $(e, \phi(N)) = 1$, computes $R_0 = g^e(\mathrm{mod}N)$ and then uses extended Euclidean algorithm to compute a unique integer h, $1 < h < \phi(N)$, such that $eh \equiv 1(\mathrm{mod}\phi(N))$. D publishes R_0, h on the bulletin board.

3) D chooses positive integers $p_1, \cdots, p_n$ such that $\max_{1 \leq i_1 < \cdots < i_{t-1} \leq n}([p_{i_1}, \cdots, p_{i_{t-1}}]) < \min_{1 \leq i_1 < \cdots < i_t \leq n}([p_{i_1}, \cdots, p_{i_t}])$, i.e., the sequence $p_1, \cdots, p_n$ is a generalized Mignotte sequence. Then D publishes the sequence $p_1, \cdots, p_n$ on the bulletin board.

4.2 Divide Secret Phase

Suppose that $S_1, \cdots, S_k$ are k secrets to be shared such that $\max_{1 \leq i_1 < \cdots < i_{t-1} \leq n}([p_{i_1}, \cdots, p_{i_{t-1}}]) < S_w < \min_{1 \leq i_1 < \cdots < i_t \leq n}([p_{i_1}, \cdots, p$ where $w = 1, \cdots, k$. The dealer D computes $y_{ij} = S_j(\mathrm{mod}p_i) \oplus {R_i}^e(\mathrm{mod}N)$, where $\oplus$ denotes the XOR operation, i.e., componentwise addition modulo 2. D publishes triples (p_i, R_i, y_{ij}), where $i = 1, \cdots n, j = 1, \cdots k$ on the bulletin board.

4.3 Recover Secret Phase

Without loss of generality, assume that participants $P_1, P_2, \cdots, P_t$ cooperate to reconstruct the secret data S_j.

1) Each participant $P_v, v = 1, 2, \cdots, t$ downloads public information R_0, h, and uses her/his secret shadow s_v to compute ${R_0}^{s_v}(\mathrm{mod}N)$ and then sends it and $R_v = g^{s_v}(\mathrm{mod}N)$ to the designated combiner.

2) After receiving ${R_0}^{s_v}(\mathrm{mod}N)$ and $R_v = g^{s_v}(\mathrm{mod}N)$, the designated combiner computes $({R_0}^{s_v})^h(\mathrm{mod}N)$,and checks whether ${R_0}^{hs_v} \equiv R_v(\mathrm{\ mod\ }N)$ is true or not.If ${R_0}^{hs_v} \not\equiv R_v(\mathrm{\ mod\ }N)$, the designated combiner knows that P_v does not provide her/his true secret shadow s_v.

3) The designated combiner downloads public information (p_i, R_i, y_{ij}) on the bulletin board, where $i = 1, \cdots, t$, and computes $y_{ij} \oplus {R_0}^{s_i}(\mathrm{\ mod\ }N) = S_j(\mathrm{\ mod\ }p_i) \oplus {R_i}^e(\mathrm{\ mod\ }N) \oplus {R_0}^{s_i}(\mathrm{\ mod\ }N) = S_j(\mathrm{\ mod\ }p_i)$,where $i = 1, \cdots, t$.

4) The designated combiner uses the general CRT to solve the system of equations

$$\begin{cases} x \equiv y_{1j} \oplus {R_0}^{s_1}(\mathrm{mod}N)(\mathrm{mod}\ p_1) \\ x \equiv y_{2j} \oplus {R_0}^{s_2}(\mathrm{mod}N)(\mathrm{mod}\ p_2) \\ \qquad\qquad \vdots \\ x \equiv y_{tj} \oplus {R_0}^{s_t}(\mathrm{mod}N)(\mathrm{mod}\ p_t) \end{cases}$$

and gets the general solutions $S_j + [p_1, \cdots, p_t]u$, where $u \in Z$. The unique nonnegative solution less than $[p_1, \cdots, p_t]$ is the secret data S_j.

5 Analysis of the Scheme

5.1 Verification Analysis

From the Euler Theorem it follows that $g^{\phi(N)} \equiv 1(\mathrm{mod}N)$. If P_v is not a cheater, then ${R_0}^{hs_v} \equiv g^{ehs_v} \equiv g^{s_v} = R_v(\mathrm{mod}N)$ since $eh \equiv 1(\mathrm{mod}\phi(N))$. Otherwise, P_v does not provide her/his true secret shadow.

Remark: If a malicious participant randomly chooses an integer s from the range of 2 to N, then performs the subsequent procedures based on s instead of s_v, she/he can pass the above verification successfully. However, $R_s = g^s(\mathrm{mod}N)$ is not equal to any one of R_i in the public information (p_i, R_i, y_{ij}) on the bulletin board, where $i = 1, \cdots, t$. So, the combiner can identify the cheater.

5.2 Security Analysis

1) Having only $t-1$ distinct shares $y_{i_1 j}, \cdots, y_{i_{t-1} j}$, one can only get that $S_j \equiv x_0(\ \mathrm{mod}\ [p_{i_1}, \cdots, p_{i_{t-1}}])$, where x_0 is the unique solution modulo $[p_{i_1}, \cdots, p_{i_{t-1}}]$ of the resulted system(in this case, $S_j > \max_{1 \le i_1 < \cdots < i_{t-1} \le n}([p_{i_1}, \cdots, p_{i_{t-1}}]) > x_0$).

2) If system attacker personates the dealer to publish a pseudo secret data, she/he has to get the secret number e. Since $R_0 = g^e(\mathrm{mod}N)$, she/he is faced with the difficulty in solving the discrete logarithm problem. Another method of getting e is to solve the equation $eh \equiv 1(\mathrm{mod}\phi(N))$. This needs factorization N into a product of primes which is also difficult.

3) In the secret reconstruction phase, each participant only provides a public value and does not have to disclose her/his secret shadow.Anyone who wants to get the participant's secret shadow will be faced with the difficulty in solving the discrete logarithm problem. The reuse of the secret shadow is secure.

4) Kima *et al.* [8] proposed new modular exponentiation and CRT recombination algorithms which are secure against all known power and fault attacks.

5.3 Performance Analysis

There are efficient algorithms for modular exponentiation and CRT recombination [4, 5, 8]. The XOR operation is of negligible complexity. What's more, each participant chooses her/his secret shadow by her/himself in the proposed scheme, P_j computes $R_j = g^{s_j}(\mathrm{mod}N)$, this also cuts the computation quantity of D.In addition, the system doesn't need a security channel, which also cuts the cost of the system.Therefore the proposed scheme is efficient and practical.

6 Concluding Remarks

This paper proposes to enhance threshold secret sharing schemes based on the CRT by incorporating the well-known RSA Cryptosystem. In the proposed scheme, participants select their secret shadows by themselves. In addition, each participant can check whether another participant provides the true secret shadow or not. Furthermore, it allows to reconstruct several secrets parallelly. Moreover, a security channel is no needed for the proposed scheme. The property is very practical in the system which is unlikely to have a security channel. The scheme is based on the RSA cryptosystem and intractability of the Discrete Logarithm.

Acknowledgments

This study was supported by the National Nature Science Foundation of China under grant 10171042. The author gratefully acknowledges the three anonymous reviewers for their valuable comments.

References

[1] C. A. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, pp. 208-210, 1983.
[2] G. Ateniese, J. Camenisch, M. Joye and G. Tsudik, "A practical and provably secure coalition resistant group signature scheme," in *Proceedings of CRYPTO'00*, pp. 255-270, Santa Barbara, USA, 2000.
[3] G. Blakley, "Safeguarding Cryptographic Keys," *Proceedings of the National Computer Conference*, AFIPS, vol. 48, pp.313-317, 1979.
[4] A. S. Fraenkel, "New proof of the generalized CRT," *Proceedings of American Mathematical Society*, vol. 14, pp. 790-791, 1963.
[5] H. Garner, "The residue number system," *IRE Transactions on Electronic Computers*, vol.8, pp. 140-147, 1959.
[6] K. Kaya and A. A. Selcuk, "Robust threshold schemes based on the chinese remainder theorem," in *Africacrypt'08*, pp. 94-108, 2008.

[7] K. Kaya and A. A. Selcuk, "A verifiable secret sharing scheme based on the chinese remainder theorem," in *Indocrypt'08*, LNCS 5365, pp. 414-425, Dalian, China, 2008.
[8] S. K. Kima, T. H. Kima, D. G. Hanb, S. Honga, "An efficient CRT-RSA algorithm secure against power and fault attacks, " *Journal of Systems and Software*, vol. 84, no. 10, pp. 1660-1669, 2011.
[9] M. Mignotte, "How to share a secret," in *Proceedings of the Workshop on Cryptography*, Burg Feuerstein, 1982, Lecture Notes in Computer Science, vol. 149, pp. 371-375, 1983.
[10] O. Ore, "The general CRT," *American Mathematical Monthly*, vol. 59, pp. 365-370, 1952.
[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 *1st International Conference on Recent Advances in Information Technology (RAIT'12)*, pp. 11-13, Dhanbad, 2012.
[13] S. Y. V. Rao and C. Bhagvati, "Multi-secret com- munication scheme," in *ICIET'12*, pp. 201-203, Mumbai, 2012.
[14] S. Y. V. Rao and C. Bhagvati,"CRT based threshold multi secret sharing scheme," *International Journal of Network Security*, vol. 16, no. 3, PP. 194-200, May 2014.
[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commununications of the ACM*, vol. 21, pp. 120-126, 1978.
[16] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.
[17] Q. Shi and W. Du,"Multi-secret sharing scheme CRT based on RSA and remainder theorem," *Computer Engineering* (in Chinese), vol. 37, no. 2, PP. 141-142, Jan. 2011.
[18] J. Zhao, J. Zhang, R. Zhao, "A practical verifiable multi-secret sharing scheme," *Computer Standards & Interfaces*, vol. 29, pp. 138-141, 2007.

Xuedong Dong received his Ph.D degree from Nanyang Technological University in 1999. He is currently a Professor in College of Information Engineering, Dalian University. His research interest includes Cryptography, Coding Theory etc. He has published about 30 research papers in journals and conferences.