Information Processing Letters 114 (2014) 504–509

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Multilevel threshold secret sharing based on the Chinese Remainder Theorem

Lein Harn [a,*], Miao Fuyou [b]

[a] Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, United States
[b] School of Computer Science and Technology, University of Science & Technology of China, China

ARTICLE INFO

Article history:
Received 30 July 2013
Received in revised form 1 December 2013
Accepted 5 April 2014
Available online 16 April 2014
Communicated by S.M. Yiu

Keywords:
Multilevel secret sharing
Chinese Remainder Theorem
Asmuth–Bloom's secret sharing scheme
Threshold value
Multilevel secret sharing scheme
Cryptography

ABSTRACT

The (t, n) threshold secret sharing schemes (SSs) were introduced by Shamir and Blakley separately in 1979. Multilevel threshold secret sharing (MTSS) is a generalization of classical threshold SS, and it has been studied extensively in the literature. In an MTSS, shareholders are classified into different security subsets. The threshold value of a higher-level subset is smaller than the threshold value of a lower-level subset. Shareholders in each subset can recover the secret if the number of shares available is equal to or more than a threshold value. Furthermore, the share of a shareholder in a higher-level subset can be used as a share in the lower-level subset to recover the secret. Chinese Remainder Theorem (CRT) is one of popular tools used for designing SSs. For example, the Mignotte's scheme and Asmuth–Bloom's scheme are two classical (t, n) threshold SSs based on the CRT. So far, there was no CRT-based MTSS in the literature. In this paper, we propose the first MTSS based on the CRT. In our proposed scheme, one unique feature is that each shareholder needs to keep only one private share. Our proposed scheme is based on the Asmuth–Bloom's SS which is unconditionally secure.

1. Introduction

In a secret sharing scheme (SS), a dealer divides a secret s into n shares and shared among a set of n *shareholders*, $U = \{U_1, U_2, ..., U_n\}$, in such a way that any authorized subset can reconstruct the secret s; whereas any un-authorized subset cannot recover the secret s. The (t, n) threshold secret sharing schemes were introduced by Shamir [1] and Blakley [2] separately in 1979. A (t, n) threshold secret sharing scheme allows any t or more than t shareholders to reconstruct the secret s; while any fewer than t shareholders cannot reconstruct the secret s. In Shamir's (t, n) threshold SS, a dealer generates n shares based on a $t-1$ degree polynomial. Secret reconstruction is based on the Lagrange interpolating polynomial of any t private shares. Shamir's (t, n) SS is unconditionally secure. There are other types of SSs. For example, Blakley's scheme [1] is based on the geometry, Mignotte's scheme [3] and Asmuth–Bloom's scheme [4] are based on the Chinese Remainder Theorem (CRT).

Multilevel threshold secret sharing (MTSS) is a generalization of classical threshold SS, and it has been studied extensively in the literature [5–10]. In an MTSS, all shareholders play different roles; while in a classical threshold SS, all shareholders play the same role. Simmons [9] considered a setting where all shareholders are partitioned into different levels, $L_1, L_2, ..., L_m$, and each level, L_i, is assigned with a threshold value t_i, for $i = 1, 2, ..., m$. Note that throughout this paper, the notations, L_i and L_j, where $i < j$, indicate that the level L_i is higher than the level L_j. In an MTSS scheme, when there are at least t_i shareholders belonging to levels higher than or equal to the level L_i, this subset of shareholders can reconstruct the secret. For example, we assume that thresholds are $t_1 = 2$ in level

* Corresponding author.

http://dx.doi.org/10.1016/j.ipl.2014.04.006
0020-0190/

L_1 and $t_2 = 3$ in level L_2. Then, two shareholders in L_1, or three shareholders in L_2 can reconstruct the secret. In addition, when there are one shareholder in L_1 and two shareholders in L_2, this combination of shareholders can also reconstruct the secret.

Brickell [6] proposed an ideal MTSS. However, his scheme is inefficient since the dealer is required to compute exponentially to ensure non-singular matrices. Ghodosi et al. [7] proposed an ideal MTSS scheme based on Shamir's threshold SS; but their schemes only work for small number of shareholders. Lin et al. [10] proposed an ideal MTSS based on the polynomial in 2009.

The CRT has been a popular tool used for designing SSs. For example, the Mignotte's scheme [3] and Asmuth–Bloom's scheme [4] are two classical (t, n) threshold SSs. Kaya et al. [11] pointed out that both schemes cannot prevent a corrupted dealer to distribute inconsistent shares to shareholders. They have proposed a CRT-based VSS which uses a range proof technique proposed by Boudot [12]. The security of their VSS is based on the RSA assumption [13]. In addition, in 2009, Sarkar et al. [14] have proposed a CRT-based RSA-threshold cryptography for a mobile ad hoc network (MANET) and in 2011, Lu et al. have proposed a secret key distributed storage scheme [15] based on CRT-VSS and trusted computing technology. Quisquater et al. [16] have shown that Asmuth–Bloom's SS [4] is asymptotically optimal both from an information theoretic and complexity theoretic viewpoint when the parameters satisfy a simplified relationship.

So far, there was no CRT-based MTSS in the literature. In this paper, we propose the first MTSS based on Asmuth–Bloom's scheme [4] which is unconditionally secure. One unique feature of our proposed scheme is that each shareholder needs to keep only one private share. This private share can also be used in the lower-level subsets to recover the secret.

The rest of this paper is organized as follows. In the next section, we introduce some preliminaries that include the definition of MTSS, the CRT, Mignotte's and Asmuth–Bloom schemes based on the CRT. In Section 3, we propose an MTSS based on a simple modification of Asmuth–Bloom scheme. In Section 4, we include the security analysis of our proposed scheme. Conclusion is given in Section 5.

2. Preliminaries

In this section, we introduce some preliminaries that are the fundamentals in our design including a definition of MTSS, the CRT, Mignotte's and Asmuth–Bloom schemes based on the CRT.

2.1. Definition of MTSS

Definition 1 *(Authorized set in a multilevel threshold secret sharing scheme).* Let $L_1, L_2, ..., L_m$, denote a partition of shareholders, $(U_1, U_2, ..., U_n)$, into multiple security levels, i.e., $U = (U_1, U_2, ..., U_n) = \bigcup_{j=1}^{m} L_j$. Let $T = (t_1, t_2, ..., t_m)$ denote a sequence of threshold values, where $1 \le t_j \le |L_1| + |L_2| + ... + |L_j|$ for $j = 1, 2, ..., m$, and $t_1 < t_2 < ... < t_m$. The authorized set (MA) of n shareholders in an (L, T) multilevel threshold secret sharing (MTSS) scheme is defined as

$$MA = \left\{ A \subseteq (U_1, U_2, ..., U_n) \;\middle|\; \exists i \in \{1, 2, ..., m\} \text{ and } \left| A \cap \bigcup_{j=1}^{i} L_j \right| \ge t_i \right\},$$

where $A = (U_{i_1}, U_{i_2}, ..., U_{i_t})$ and $U_{ik} \ne U_{ij}$ if $k \ne j$ for any subset $\{i_1, i_2, ..., i_t\}$ of $\{1, 2, ..., n\}$.

2.2. The Chinese Remainder Theorem (CRT) [17]

Given following system of equations as

$$x = s_1 \bmod p_1;$$
$$x = s_2 \bmod p_2;$$
$$\vdots$$
$$x = s_t \bmod p_t,$$

there is one unique solution as $x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \cdot s_i \bmod N$, where $\frac{N}{p_i} \cdot y_i \bmod p_i = 1$, and $N = p_1 \cdot p \cdot ... \cdot p_t$, if all moduli are pairwise coprime (i.e., $\gcd(p_i, p_j) = 1$, for every $i \ne j$).

The CRT has been used in the RSA decryption to speed-up the decryption process. With the knowledge of prime decomposition of the RSA composite integer and using the CRT, the complexity of RSA decryption is reduced by a factor of $\frac{1}{4}$. The CRT can also be used in the SS. Each of the shares is represented in a congruence, and the solution of the system of congruences using the CRT is the secret to be recovered. SS based on the CRT uses, along with the CRT, a special sequence of integers that guarantee the impossibility of recovering the secret from a set of shares with less than a certain cardinality. In the next subsections, we will review two most well-known SSs based on the CRT.

2.3. Review of Mignotte's (t, n) SS

Share generation: A sequence consists of pairwise coprime positive integers, $p_1 < p_2 < ... < p_n$, with $p_{n-t+2} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$, where p_i is the public information associated with each shareholder, U_i. For this given sequence, the dealer chooses the secret s as an integer in the set $Z_{p_{n-t+2} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t}$ (i.e., $Z_{p_{n-t+2} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t}$ is referred to the range $(p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t)$). We call the range, $Z_{p_{n-t+2} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t}$, the t-**threshold range**.

Share for the shareholder, U_i, is generated as $s_i = s \bmod p_i$, $i = 1, 2, ..., n$. s_i is sent to shareholder, U_i, secretly.

Remark 1. The numbers in the t-threshold range, $Z_{p_{n-t+2} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t}$, are integers upper bounded by $p_1 \cdot p_2 \cdot ... \cdot p_t$, which is the smallest product of any t moduli, and lower bounded by $p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n$, which is the largest product of any $t - 1$ moduli. The secret, s, selected in this range can ensure that (a) the secret can be recovered with any t or more than t shares (i.e., the product