An Access Control Mechanism Based on the Generalized Aryabhata Remainder Theorem

Yanjun Liu [1, 2], Chin-Chen Chang[2, 3], and Shih-Chang Chang[4]
(Corresponding author: Chin-Chen Chang)

School of Computer Science and Technology, Anhui University[1]
No. 3, Feixi Rd., Hefei, 230039, China
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Rd., Wufeng, Taichung, 41354, Taiwan, R.O.C.
Department of Information Engineering and Computer Science, Feng Chia University[3]
No. 100 Wenhwa Rd., Seatwen, Taichung, 40724, Taiwan, R.O.C.
Department of Computer Science and Information Engineering, National Chung Cheng University[4]
No.168, Sec. 1, University Rd., Min-Hsiung Township, Chiayi, 62102, Taiwan, R.O.C.
(Email: alan3c@gmail.com)

(Received Jan. 10, 2013; revised and accepted May 16, 2013)

Abstract

An access control mechanism is a technology to protect the confidential files stored in a database by restricting the access rights of different approved users of these files. In this paper, we propose a novel access control mechanism using the single-key-lock system and the generalized Aryabhata remainder theorem (GART), in which each user is associated with a key and each digital file with a lock. Our mechanism possesses three unique features, 1) a high efficiency of constructing the keys for the users and the locks for the files; 2) a simple operation on the user's key and on the file's lock allows the user access to the file; and 3) the keys for adding or deleting a user can be updated easily without affecting the existing keys for other users.

Keywords: Access control, generalized Aryabhata remainder theorem (GART), single-key-lock system

1 Introduction

With the advent of distribution systems and multimedia technology, different users in a specific system or organization must share extensive digital information, such as digital books, personnel data, commercial specifications, and digital audio or video duplicates, which is stored in a common database. Due to the fact that such shared digital files are extremely important and must be kept confidential, protecting the files from unauthorized access is a topic of great interest in the field of information security. In order to ensure that the files are secure, an access control mechanism [2, 3, 4, 6, 12, 15, 17, 19, 21, 22, 23, 24, 26] must be used to grant or limit the access rights of different approved users, i.e., to determine the level of access that each user has to the confidential digital files. Thus, the fundamental objective of the access control mechanism is to prevent any unauthorized user from viewing, changing, or destroying any digital files.

Considering the significant impact that the access control mechanism has on resource sharing and information confidentiality, many different access control mechanisms have been proposed in the previous literature [1, 7, 8, 10, 11, 14, 25, 29]. Among them, the access control matrix model has a comparatively simple design and has been used extensively in information protection systems. An abstract concept of the access control matrix model, known as the abstract protection model, was developed by Graham and Denning [13]. Specifically, they used three variables, i.e., S, O, and A (defined below), in the abstract protection model to represent the status of the information protection system, where 1) S stands for a set of subjects (or users) who can access the digital files in the database, 2) O stands for a set of objects (or digital files) that must be protected according to specified access rights, and 3) A stands for an access control matrix in which the rows represent the subjects (S), the columns represents the objects (O), and the entry a_{ij} represents the access right of the i^{th} subject to the j^{th} object.

In general, there are five kinds of access rights in an information protection system, i.e., no access, executing, reading, writing, and owning, which are denoted as "0," "1," "2," "3," and "4," respectively, in access control matrix A. Access rights of larger numbers include the access rights of smaller numbers, e.g., if a user has the right of reading (denoted as "2") a file, he or she also has the right of executing (denoted as "1") the same file; similarly, if a user is granted the right of owning (denoted as "4") a file, he or she definitely has all the rights to access the same file. Figure 1 shows an access control matrix of an information protection system consisting of four users,

a_{ij}	F_1	F_2	F_3
U_1	3	2	0
U_2	1	4	3
U_3	4	2	1
U_4	2	3	4

0: No access
1: Execute
2: Read
3: Write
4: Own

Figure 1: An access control matrix

$U_1 - U_4$, three digital files, $F_1 - F_3$, and the corresponding access rights of U_i to F_j, where $1 \le i \le 4$ and $1 \le j \le 3$.

Although the principle of the abstract protection model mentioned above is simple, the model is unable to store the access control matrix directly. The access control matrix is sparse, which can lead to the inefficient use of space. The single-key-lock pair scheme, proposed by Wu and Hwang [26], provides a solution to this problem. In their scheme, each user is associated with a key vector, and each digital file is associated with a lock vector. Each access right a_{ij} in the access control matrix can be computed by the corresponding key vector and lock vector. Thus, only keys and locks have to be stored in the information protection system to derive the access control matrix. However, this scheme has three drawbacks, i.e., 1) the method used to generate the keys and locks is complex; 2) the approach used to obtain the access control matrix is time-consuming due to the complicated representation of keys and locks; and 3) the complexity of the required storage is high, e.g., $O(mn)$, where *m* and *n* are the number of keys and locks, respectively.

To overcome these drawbacks, Chang [2] proposed a novel access control mechanism based on the concepts of the single-key-lock system and the Chinese remainder theorem (CRT) [5, 16, 18, 27]. His mechanism can be used to construct the keys and locks easily, expediting the procedure of computing the access control matrix. In addition, when there are *m* keys and *n* locks, the complexity of the required storage can be decreased to $O(m+n)$. Later, in 1986, Chang and Chen [3] proposed another novel access control scheme based on the generalized Chinese remainder theorem (GCRT). Their scheme can obtain several keys for a user by using the grouped generation method while maintaining the advantages of Chang's mechanism. However, the efficiency of Chang and Chen's mechanism can still be increased, especially the complexity of constructing the keys for all users, which requires a lot of time. Inspired by Chang and Chen's mechanism, in this paper, we propose a new access control mechanism using the single-key-lock system and the generalized Aryabhata remainder theorem (GART), which is more efficient than Chang and Chen's mechanism. The main contributions of our proposed mechanism are listed below:

1) The keys for users in an information protection system can be constructed efficiently. According to the GART utilized in our mechanism, the key for a specific user can be generated by the locks for the digital files, the pre-determined access right of this user to each digital file, and a parameter *k* that is a crucial component in the computational process of the GART. This method of constructing the keys is more efficient than the mechanism that Chang and Chen used.
2) The access right of a user to a digital file can be obtained by the GART, in which only a simple operation on the key of this user and the lock of this file must be performed.
3) When a new user is added to the information protection system, a new key for her or him can be allocated by using the GART without modifying the other users' existing keys; when a user is deleted from the system, the only thing to do is to eliminate her or his key.
4) The approach of reconstructing the keys for all of the users in the system only involves updating parameter *k* in the GART, i.e., there is no need to modify any existing locks and access rights. This feature is indicative of the flexibility of our proposed mechanism.
5) The complexity of the required storage of our mechanism is the same as that of Chang and Chen's mechanism, i.e., $O(m+n)$ for *m* keys and *n* locks, thereby avoiding the overflow problem.

The rest of this paper is organized as follows. In Section 2, we briefly introduce Chang and Chen's scheme and the fundamental component of our mechanism, i.e., the GART. In Section 3, we propose our novel access control mechanism. Section 4 analyzes the proposed mechanism, and our conclusions are presented in Section 5.

2 Preliminaries

In this section, we briefly introduce Chang and Chen's scheme and the basic component that we used in designing our access control mechanism. First, we describe the single-key-lock system, and then, we review Chang and Chen's scheme that used the single-key-lock system. Finally, we describe the principle of the GART and the associated computational process.

2.1 The Single-Key-Lock System

The single-key-lock system [2] is a well-known, information-protection system that be used to realize the access control matrix successfully. Assume that a single-key-lock system consists of *m* users and *n* digital files. The single-key-lock system must be able to validate each user's request to access a digital file, thereby protecting all the files from unauthorized access. To achieve this goal, the single-key-lock system assigns each user U_i a key K_i and each digital file F_j a lock L_j, where $1 \le i \le m$ and $1 \le j \le n$. As illustrated in Figure 2, the procedure of access control by a typical single-key-lock system is conducted as follows. First, the system determines the access right of each registered user U_i to each digital file F_j. Then, the system constructs the key K_i for each U_i by using the locks and her or his pre-determined access rights. When U_i requests access to F_j, the system computes the true access right a_{ij} in the invisible access control matrix by the key K_i and the lock L_j. If the access right that is requested is smaller than or equal to the value of a_{ij}, U_i can access F_j successfully; otherwise, the system will reject the request.

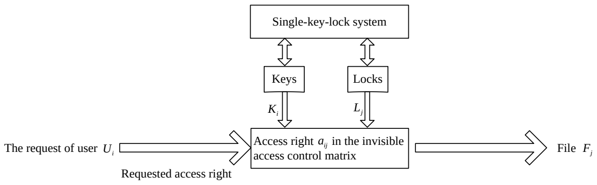
Single-key-lock system
Keys
Locks
K_i
L_j
The request of user U_i
Requested access right
Access right a_{ij} in the invisible access control matrix
File F_j

Figure 2: Architecture of a single-key-lock system

From the above description of the single-key-lock system, it is evident that an efficient and practical access control mechanism must be used in the implementation of this system. Also, the following issues must be considered in designing this access control mechanism, i.e., (1) the effective construction and representation of the keys and locks rather than storing the access control matrix directly; (2) the efficient use of the key K_i and the lock L_j to calculate the access right a_{ij}; (3) the development of an effective solution for the dynamic access control problem when the keys and locks must be updated as the result of adding or deleting a user or when an access right is altered; and (4) approaches for reducing the storage requirement for the keys and locks.

2.2 Chang and Chen's Key-lock-pair Scheme

Chang and Chen's key-lock-pair scheme [3] used the concepts of the single-key-lock system described in Figure 2 and the generalized Chinese remainder theorem (GCRT). In their scheme, the system selects n positive integers, $L_1, L_2, \ldots, L_n$, that are relatively prime in pairs as the locks for the files. Assuming that a_{ij}, where $1 \le i \le m$ and $1 \le j \le n$, denotes the access right of each user U_i to each digital file F_j in the invisible access control matrix, we can create the system of equations shown below:

$$\lfloor K_i / L_1 \rfloor \equiv a_{i1} (\bmod k),$$
$$\lfloor K_i / L_2 \rfloor \equiv a_{i2} (\bmod k),$$
$$\vdots$$
$$\lfloor K_i / L_n \rfloor \equiv a_{in} (\bmod k),$$

where k is a positive integer subject to $\text{Max}\{a_{ij}\}_{1 \le j \le n} < k < \text{Min}\{L_j\}_{1 \le j \le n}$. According to the GCRT, K_i can be calculated by the following equation:

$$K_i = \sum_{j=1}^{n} L'_j \cdot L''_j \cdot b_{ij} (\bmod kM), \quad (1)$$

where $M = \prod_{j=1}^{n} L_j$, $L'_j = k \cdot M / L_j$, $L'_j \cdot L''_j \equiv k (\bmod k \cdot L_j)$, and $b_{ij} = \lceil a_{ij} \cdot L_j / k \rceil$.

Therefore, in this access control scheme, it is easy to determine the locks by selecting n pairwise relatively prime numbers and to construct all the keys by the GCRT. However, the efficiency of generating the keys can be improved. This is the aim of our new mechanism.

2.3 Generalized Aryabhata Remainder Theorem

Since our proposed access control mechanism is based on the generalized Aryabhata remainder theorem (GART), this subsection will introduce the GART and demonstrate how it performs to compute a unique solution in a certain range.

The GART, proposed by Chang et al. [9], is a considerable variation of the Aryabhata remainder theorem (ART) [20, 28]. The GART uses a positive integer k as an additional parameter to compute an integer X. Given n pairwise, co-prime integers, $q_1, q_2, \ldots, q_n$, and n positive integers, $x_1, x_2, \ldots, x_n$, where $\text{Max}\{x_i\}_{1 \le i \le n} < k < \text{Min}\{q_i\}_{1 \le i \le n}$, a system of equations can be established as follows:

$$\lfloor X / q_1 \rfloor \equiv x_1 (\bmod k),$$
$$\lfloor X / q_2 \rfloor \equiv x_2 (\bmod k),$$
$$\vdots$$
$$\lfloor X / q_n \rfloor \equiv x_n (\bmod k).$$

Then, the integer X, which is the unique solution in $Z_{k\prod_{i=1}^{n} q_i}$, can be calculated by the iterative algorithm of GART shown below.

```
Input: ($\{x_1, x_2, \ldots, x_n\}$, $\{q_1, q_2, \ldots, q_n\}$, $k$)
Output: $X$
1. $Q_1 \leftarrow q_1$, $X_1 = x_1 \cdot q_1$
2. for $i$ = 2 to $n$ do
3.     $Q_i \leftarrow Q_{i-1} \cdot q_i$
4.     $X_i \leftarrow k \cdot Q_{i-1} \cdot ((\lceil (x_i \cdot q_i - X_{i-1}) / k \rceil \cdot (Q_{i-1})^{-1}) \bmod q_i) + X_{i-1}$,
       where $(Q_{i-1})^{-1} \bmod q_i$ is the multiplicative inverse of $Q_{i-1}$ modulo $q_i$.
5. end for
6. return $X_n$
```

Next, an example is given to illustrate how to use the GART to compute an integer.

Example 1. *Assume that* $\{x_1, x_2, x_3\}$ *= {1, 2, 3},* $\{q_1, q_2, q_3\}$ *= {7, 13, 17}, and k = 5. Find the integer X that satisfies* $\lfloor X / q_i \rfloor \equiv x_i (\bmod k)$ *using the GART, where* $1 \le i \le 3$.

The computational process is comprised of the following three steps:

Step 1:

$Q_1 = q_1 = 7,\ X_1 = x_1 \cdot q_1 = 1 \cdot 7 = 7.$

Step 2:

$$Q_2 = Q_1 \cdot q_2 = 7 \cdot 13 = 91,$$

$$\begin{aligned} X_2 &= k \cdot Q_1 \cdot ((\lceil (x_2 \cdot q_2 - X_1)/k \rceil \cdot (Q_1)^{-1}) \bmod q_2) + X_1 \\ &= 5 \cdot 7 \cdot ((\lceil (2 \cdot 13 - 7)/5 \rceil \cdot 7^{-1}) \bmod 13) + 7 \\ &= 5 \cdot 7 \cdot 8 + 7 \\ &= 287. \end{aligned}$$

Step 3:

$$Q_3 = Q_2 \cdot q_3 = 91 \cdot 17 = 1547,$$

$$\begin{aligned} X_3 &= k \cdot Q_2 \cdot ((\lceil (x_3 \cdot q_3 - X_2)/k \rceil \cdot (Q_2)^{-1}) \bmod q_3) + X_2 \\ &= 5 \cdot 91 \cdot ((\lceil (3 \cdot 17 - 287)/5 \rceil \cdot 91^{-1}) \bmod 17) + 287 \\ &= 5 \cdot 91 \cdot 12 + 287 \\ &= 5747. \end{aligned}$$

We can verify the unique solution X_3 *in* Z_{7735} *as follows:*

$$\lfloor X_3/q_1 \rfloor \bmod k = \lfloor 5747/7 \rfloor \bmod 5 = 1 = x_1,$$

$$\lfloor X_3/q_2 \rfloor \bmod k = \lfloor 5747/13 \rfloor \bmod 5 = 2 = x_2,$$

and $\lfloor X_3/q_3 \rfloor \bmod k = \lfloor 5747/17 \rfloor \bmod 5 = 3 = x_3$.

3 Our Proposed Mechanism

From the description of the single-key-lock system and the GART in Section 2, it is feasible to combine these two concepts to yield a novel access control mechanism. Now, we provide details concerning the proposed mechanism in the four steps that follow:

Step 1. Initialization of the system.

Assume that the single-key-lock system consists of *m* users and *n* digital files and that each user U_i is associated with a key K_i and that each digital file F_j is associated with a lock L_j. The initialization of the system contains two tasks, i.e., (1) selecting *n* pairwise co-prime integers L_j for $1 \le j \le n$ as the locks of the *n* files and (2) determining the access right a_{ij} for $1 \le i \le m$ and $1 \le j \le n$ of each user U_i to each digital file F_j in the invisible access control matrix, where $\mathrm{Max}\{a_{ij}\}_{1 \le j \le n} < \mathrm{Min}\{L_j\}_{1 \le j \le n}$ according to user U_i.

Step 2. Construction of the keys.

First, choose a positive integer *k* subject to $\mathrm{Max}\{a_{ij}\}_{1 \le j \le n} < k < \mathrm{Min}\{L_j\}_{1 \le j \le n}$. Then, establish the following system of equations:

$$\lfloor K_i / L_1 \rfloor \equiv a_{i1} (\bmod k),$$

$$\lfloor K_i / L_2 \rfloor \equiv a_{i2} (\bmod k),$$

$$\vdots$$

$$\lfloor K_i / L_n \rfloor \equiv a_{in} (\bmod k).$$

Therefore, the key K_i for each user U_i can be generated by the locks $L_1, L_2, \ldots, L_n$, U_i 's access rights $a_{i1}, a_{i2}, \ldots, a_{in}$ to all *n* files, and the integer *k* according to the GART described in Subsection 2.2, in which we only replace $q_1, q_2, \ldots, q_n$ and $x_1, x_2, \ldots, x_n$ with $L_1, L_2, \ldots, L_n$ and $a_{i1}, a_{i2}, \ldots, a_{in}$, respectively. Now let us describe how K_i is calculated by using the GART. Since K_i must be computed by (*n*-1) rounds according to the GART, we use the symbol K_{i_d} to represent the value of K_i in the *d*th round, where $d = 2$ to n. In each round,

$$K_{i_d} = k \cdot M_{d-1} \cdot ((\lceil (a_{id} \cdot L_d - K_{i_{d-1}})/k \rceil \cdot (M_{d-1})^{-1}) \bmod L_d) + K_{i_{d-1}}, \quad (2)$$

where $M_1 = L_1$, $K_{i_1} = a_{i1} \cdot L_1$, and $M_d = M_{d-1} \cdot L_d$. Then, all the *m* keys can be constructed easily by repeating the computational process of the key K_i for the user U_i *m* times.

Step 3. Computation of access right.

When user U_i requests access to file F_j, the corresponding access right a'_{ij} must be computed by the equation $a'_{ij} = \lfloor K_i / L_j \rfloor \bmod k$. The value of a'_{ij} is identical to a_{ij} in the invisible access control matrix that was determined in Step 1.

Step 4. Verification of access right.

If U_i 's requested access right to F_j is smaller than or equal to the value of a'_{ij}, the request will be accepted; otherwise, it will be declined.

Next, we give an example to illustrate how our proposed access control mechanism performs.

Example 2. *Consider a single-key-lock system consisting of four users,* $U_1 - U_4$*, and three digital files,* $F_1 - F_3$*. During the initialization of the system, assume that* $L_1 = 7$*,* $L_2 = 11$*, and* $L_3 = 13$*; the access control matrix that was determined is shown in Figure 1.*

After choosing $k = 5$*, satisfying* $\mathrm{Max}\{a_{ij}\}_{1 \le j \le 3} < k < \mathrm{Min}\{L_j\}_{1 \le j \le 3}$*, the key* K_i *for each user* U_i *is generated by* L_1*,* L_2*,* L_3*,* U_i *'s access rights* a_{i1}*,* a_{i2}*,* a_{i3}*, and the integer k according* *to the GART, such that* $K_1 = 3381$, $K_2 = 1862$, $K_3 = 4368$, *and* $K_4 = 4214$. *Then, the access right* a'_{ij} *is computed by* $a'_{ij} = \lfloor K_i / L_j \rfloor \bmod k$, *which coincides with* a_{ij} *in the invisible access control matrix. For example,* $a'_{12} = \lfloor K_1 / L_2 \rfloor \bmod k = 2 = a_{12}$, $a'_{22} = \lfloor K_2 / L_2 \rfloor \bmod k = 4 = a_{22}$, *and* $a'_{43} = \lfloor K_4 / L_3 \rfloor \bmod k = 4 = a_{43}$.

Consider that U_1 *attempts to write* F_2. *Because the number representing the access right of writing is "3," which is larger than the value of* a'_{12}, *this access request will be rejected. However, if* U_1 *wants to access* F_2 *by executing (denoted as "1") or reading (denoted as "2"), her or his request will be accepted because the value of* a'_{12} *is equal to or greater than the requested access right.*

4 Discussion

In this section, we discuss some issues about our proposed access control mechanism, including the computational complexity associated with the construction of the keys, the effort required to modify the keys when adding or deleting a user or a file, the effort required to reestablish keys, and the storage requirement for the keys and locks.

4.1 Construction of Keys

Our access control mechanism uses the GART to construct keys for users. According to the GART, key K_i for a specific user U_i can be generated by the locks $\{L_j\}_{1 \le j \le n}$ for digital files, the pre-determined access rights $\{a_{ij}\}_{1 \le j \le n}$ of U_i to all digital files, and the important parameter *k*. Since Chang and Chen's mechanism utilizes the GCRT to generate keys, we present below an analysis of the comparative time complexity of the GCRT and the GART to determine which method has less time complexity.

Now, let us consider the time complexity of the GCRT according to Equation (1). Assume that both L_j and a_{ij} are assigned b digits, and the expressions $L'_j \cdot L''_j$ and $k \cdot M$ can be pre-computed. Therefore, in Equation (1), 2*n* multiplications, *n* divisions, (*n*-1) additions, and one modular operation exist. Notice that the multiplication/division of two integers, each of which has b digits, requires b^2 bit operations, and the addition of such two integers requires b bit operations. In addition, a modular operation with b bits requires b^2 bit operations, thus the operation of "$\bmod kM$" requires $((n+1) \cdot b)^2$ bit operations. By the above analysis, we can calculate that the computational cost of the GCRT is about $2n \cdot b^2 + n \cdot b^2 + (n-1) \cdot b + ((n+1) \cdot b)^2$ bit operations, which implies the time complexity of the GCRT is $O(n^2b^2)$.

Table 1: Comparison of the methods for key construction

Mechanism	Method	Time Complexity
Chang and Chen's mechanism	GCRT	$O(n^2b^2)$
Our mechanism	GART	$O(nb^2)$

Table 2: Operations for adding or deleting a user or a file

Case	Required Operation
Adding a user U_i	Only calculate K_i by using the GART
Deleting a user U_j	Only eliminate K_j
Adding a file F_i	Recalculate all keys
Deleting a file F_j	Recalculate all keys

Next, we analyze the time complexity of the GART used in our mechanism. In Equation (2), we assume that k, L_d , and a_{id} are assigned b digits, the expression $k \cdot M_{d-1} \cdot ((M_{d-1})^{-1} \bmod L_d)$ can be computed. Hence, in Equation (2), two multiplications, one subtraction, one division, one addition, and one modular operation exist. As a result, after (*n*-1) rounds are completed, the computation cost of the GART is about $(n-1) \cdot (2b^2 + b + b^2 + b + b^2)$ bit operations. Thus, the time complexity of the GART is $O(nb^2)$, which is less than that of the GCRT.

In the following, we perform an analysis to determine why the GART is more efficient than the GCRT. In the GCRT, a modular operation must be performed with a large number, $k \cdot M$, which is time-consuming. However, the computational process of the GART is divided into several iterations in which a modular operation with a smaller number is needed, making the GART have a higher efficiency than the GCRT. Hence, our access control mechanism is more efficient in the construction of the keys than Chang and Chen's mechanism. Table 1 compares the methods for key construction of both mechanisms.

In addition, after the keys are generated, access right a'_{ij} of each user U_i to each digital file F_j can be obtained by a simple operation on U_i 's key and F_j 's lock, i.e., $a'_{ij} = \lfloor K_i / q_j \rfloor \bmod k$, which coincides with a_{ij} in the invisible access control matrix.

4.2 Adding or Deleting a User or a File

In this subsection, we discuss how to modify the keys when adding or deleting a user or a file.

It is convenient to add or delete a user with our mechanism. When a new user joins the information protection system, her or his key can be constructed easily by the locks for digital files, her or his pre-determined access rights to each digital file, and the parameter *k* according to the GART. Fortunately, the construction of the new user's key does not affect the existing users' keys. When an existing user is deleted from the system, the only thing to do is to eliminate her or his key while there is no need to update other users' keys. However, when adding or deleting a file, the key for each user must be altered due to the characteristics of the GART. Table 2 summaries the required operations for adding or deleting a user or a file.

4.3 Reestablishment of Keys

Our mechanism can reestablish keys by modifying only parameter k according to the GART, which can avoid modifying any existing locks and access rights. Therefore, our mechanism is flexible.

4.4 Storage Requirement

The complexity of the required storage of our mechanism is the same as that of Chang and Chen's mechanism, i.e., $O(m+n)$ for m keys and n locks, thereby avoiding the overflow problem.

5 Conclusions

In this paper, we proposed an efficient access control mechanism based on the concepts of the single-key-lock system and the generalized Aryabhata remainder theorem (GART). Our mechanism used an efficient approach to generate keys for users. First, selecting n pairwise co-prime integers L_j for $1 \leq j \leq n$ as the keys of the n files and determining the access right a_{ij} of each user U_i to each digital file F_j in the invisible access control matrix. Then, the key K_i for each user U_i can be generated easily by the locks $L_1, L_2, \ldots, L_n$, U_i's rights $a_{i1}, a_{i2}, \ldots, a_{in}$ to all of the n files, and the parameter k according to the GART. We analyzed the time complexity of the GART and concluded that our mechanism is more efficient than Chang and Chen's mechanism in the method used to construct the keys. Also, in our proposed mechanism, keys can be updated when users are added to or deleted from the system without modifying other users' keys.

Acknowledgments

This study was supported in part by the National Nature Science Foundation of China (grant number: 61202228) and the College Natural Science Key Project of Anhui Province of China (grant number: KJ2012A008). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," *ACM Transactions on Information and System Security*, vol. 13, no. 1, pp. 1-38, 2009.

[2] C. C. Chang, "On the design of a key-lock-pair mechanism in information protection systems," *Bit*, vol. 26, no. 4, pp. 410-417, 1986.

[3] C. C. Chang and C. P. Chen, "A key-lock-pair mechanism based on generalized Chinese remainder theorem", *Journal of the Chinese Institute of Engineers*, vol. 9, no. 4, pp. 383-390, 1986.

[4] C. C. Chang, "An information protection scheme based upon number theory," *Computer Journal*, vol. 30, no. 3, pp. 249-253, 1987.

[5] C. C. Chang and H. C. Lee, "A new generalized group-oriented cryptoscheme without trusted centers," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 725-729, 1993.

[6] C. C. Chang and D. C. Lou, "A binary access control method using prime factorization," *Information Science*, vol. 96, no.1-2, pp. 15-26, 1997.

[7] C. C. Chang, I. C. Lin, and H. M. Tsai, "A dynamic mechanism for determining relationships in a partially ordered user hierarchy," *Proceedings of the 18th International Conference on Advanced Information Networking and Applications*, pp. 133-138, Fukuoka, Japan, 2004.

[8] C. C. Chang, I. C. Lin, and C. T. Liao, "An access control system with time-constraint using support vector machines," *International Journal of Network Security*, vol. 2, no. 2, pp. 150-159, 2006.

[9] C. C. Chang, J. S. Yeh, and J. H. Yang, "Generalized Aryabhata remainder theorem," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 4, pp. 1865-1871, 2010.

[10] H. K. C. Chang, J. J. Hwang, and H. H. Liu, "A novel access control method using morton number and prime factorization," *Information Sciences*, vol. 130, no. 1, pp. 23-40, 2000.

[11] Y. Cheng, J. Park, and R. Sandhu, "A user-to-user relationship-based access control model for online social networks," *Data and Applications Security and Privacy*, vol. 7371, pp. 8-24, 2012.

[12] D. Ferraiolo, J. Barkley, and R. Kuhn, "A role based access control model and reference implementation within a corporate," *ACM Transactions on Information and System Security*, vol. 2, no.1, pp. 34-64, 1999.

[13] G. S. Graham and P. J. Denning, "Protection-principles and practice," *Proceedings of the Spring Joint Computer Conference*, pp. 417-429, AFIPS, Montrale, N. J., 1972.

[14] J. T. Hamill, R. F. Deckro, and J. M. Kloeber, "Evaluating information assurance strategies," *Decision Support Systems*, vol. 39, no. 3, pp. 463-484, 2005.

[15] M. Hitchens and V. Varadharajan, "Design and specification of role based access control policies," *IEEE Proceedings of Software*, vol. 147, no. 4, pp. 117-129, 2000.

[16] Y. P. Lai and C. C. Chang, "Parallel computational algorithms for generalized Chinese remainder theorem," *Computers and Electrical Engineering*, vol. 29, no. 8, pp. 801-811, 2003.

[17] C. S. Laih, L. Harn, and J. Y. Lee, "On the design of a single-key-lock mechanism based on Newton's interpolating polynomial," *IEEE Transactions on Software Engineering*, vol. 15, no. 9, pp. 1135-1137, 1989.

[18] H. Liao and X. G. Xia, "A sharpened dynamic range of a generalized Chinese remainder theorem for multiple integers," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 428-433, 2007.

[19] J. D. Moffett and M. S. Sloman, "The source of authority for commercial access control," *IEEE Computer*, vol. 21, no. 2, pp. 59-69, 1988.

[20] T. R. N. Rao and C. H. Yang, "Aryabhata remainder theorem: relevance to public-key crypto-algorithms," *Circuits, Systems, and Signal Processing*, vol. 25, no. 1, pp. 1-15, 2006.

[21] R. Sandhu, E. J. Coyne, and H. L. Feinstein, "Role based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38-47, 1996.

[22] M. Singh and M. S. Patterh, "Formal specification of common criteria based access control policy model," *International Journal of Network Security*, vol. 11, no. 3, pp. 112-121, 2010.

[23] X. Tian, X. Wang, and A. Zhou, "DSP re-encryption based access control enforcement management mechanism in DaaS," *International Journal of Network Security*, vol. 15, no. 1, pp. 28-41, 2013.

[24] S. F. Tzeng, C. C. Lee, and T. C. Lin, "A novel key management scheme for dynamic access control in a hierarchy," *International Journal of Network Security*, vol. 12, no. 3, pp. 178-180, 2011.

[25] M. Vroblefski, A. Chen, B. Shao, and M. Swinarski, "Managing user relationship in hierarchies for information system security," *Decision Support Systems*, vol. 43, no. 2, pp. 408-419, 2007.

[26] M. L. Wu and T. Y. Hwang, "Access control with single-key-lock," *IEEE Transactions on Software Engineering*, vol. 10, no. 2, pp. 185-191, 1984.

[27] X. G. Xia and K. Liu, "A generalized Chinese remainder theorem for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates," *IEEE Signal Processing Letters*, vol.12, no.11, pp. 768-771, 2005.

[28] J. H. Yang and C. C. Chang, "Aryabhata remainder theorem for moduli with common factors and its application in information protection systems," *Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1379-1382, Harbin, China, 2008.

[29] J. H. Yeh, R. Chow, and R. Newman, "Key assignment for enforcing access control policy exceptions in distributed systems," *Information Sciences*, vol. 152, no. 1, pp. 63-88, 2003.

Yanjun Liu was born in Anhui Province, China, in 1982. She received the B.S. degree from Anhui University, Hefei, China, in 2005 and the Ph.D. degree from the University of Science and Technology of China (USTC), Hefei, China, in 2010, both in computer science. She is currently serving in Anhui University. Meanwhile, she is a post doc at Asia University, Taichung, Taiwan. Her current research interests include information security and computer cryptography.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. His current research interests include database design, computer cryptography, image compression and data structures.

Shih-Chang Chang received his B.S. degree in 2005 and his M.S. degree in 2007, both in Department of Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan. He is currently pursuing his Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, computer cryptography, and mobile communications.