Lightweight Encryption of Hierarchical Access Control Mechanism Key Using Tribes of Farey Fractions and its Analysis

Rajendra Hegadi
Pragati College of Engineering & Management,
Sejbahar, Raipur, Chhattisgarh, India

Ramesh Shahabadkar
Research Scholar, Anna University, Coimbatore,
Tamil Nadu, India

Shamshekhar Patil
Dr. Ambedkar Institute of Technology
Bangalore, India.

ABSTRACT

In this paper we propose a mechanism to develop a lightweight encryption technique. We encrypt hierarchical single key-lock access control mechanism key by encoding key (key number). Key number is derived using Chinese reminder theorem and tribes of Gaussian or rational Farey fractions are used to encode the key number. The advantages of the proposed mechanism are i) no decoding overhead as access rights are derived without decoding the encoded the key number, ii) no need to derive the key number for already existing files. Hence this method secures access control system by encoding the key number and acts as a thin layer of security; however the performance of retrieval system remains unchanged.

General Terms

Access control mechanism, Cryptography, Network Security.

Keywords

Light weight encryption, Farey fractions, Access control mechanism, and Chinese remainder theorem.

1. INTRODUCTION

Access control is very important in information security systems, because of the increasing complexity of various sorts of information, the large number of users, and widely used communication networks. The issue of information protection includes secrecy, authenticity and availability [6] [9]. The information privacy is defined as a decision-making of a user privilege to access certain information. However, information security is a method or a technique by which the decision of information privacy is executed to protect the legitimate access and to reject the illegitimate one [1] [4] [5] [7] [10] [11].

Generally it is agreed that some kind of information protection measure is required to prevent disclosures to unauthorized persons. An access control mechanism grants the privilege to access information resources in the system to a user. For instance, users may be able to access files via READ, WRITE, EXECUTE, DELETE or APPEND commands, but different users will be given different access rights to individual files. Traditionally this can be achieved by using an access control matrix which specifies who has what access privileges to system resources.

Table 1 illustrates the access control matrix of a simple information system with three users and four files (i.e. segments of data or programs). In this case Ganesh owns file F2 that Suresh can read and Ramesh can write. Ramesh might grant right to write access to Suresh on file F3 or Ramesh might request to read file F4, which is owned by Suresh.

The concept and the implementation of access control matrix seem to be simple and easy. But we cannot store the access control matrix because it will tend to be sparse and large when the system grows large.

Table 1: **A typical Access Control Matrix**

Users / Files	F_1	F_2	F_3	F_4
Ganesh	READ	OWN	WRITE	READ
Suresh	WRITE	READ		OWN
Ramesh	READ	WRITE	OWN	

1.1 Wu and Hwang’s Access Control with Single Key-lock Mechanism

Wu and Hwang [7] proposed the single key-lock pair mechanism that fulfils the requirement of single key-lock (SKL) system. In this method a user Ui assigned a key Ki of n-digit sequence and each file Fj a lock Lj of n-digit sequence too, where n is the total number of files. In this method the attribute value aij = Ki * Lj, where the operator * means the inner product over Galois field GF (t) and t is chosen as the smallest as the access control matrix considered.

The three big disadvantages of Wu and Hwang’s method are i) the size of required storage due to the keys and locks actually exceed that of the original access matrix, ii) the operations of keys and locks are tedious, iii) the constructions of keys and locks are not simple, iv) needs to recalculate all the keys and locks when files are added or deleted.

1.2 C. C Chang SKL Pair Mechanism

C. C Chang [1] has proposed another SKL pair mechanism using Euler’s theorem of number theory. In this method the construction of keys is not simple.

1.3 Kims S. Lee et al. Hierarchical Key Storage Structure Method

Kim S. Lee et al. [4] proposed a new hierarchical key storage structure using Chinese remainder theorem. This method improves the implementation of the SKL system based on the

Chinese remainder theorem by the use of (i) a simpler approach of the extended Euclidian algorithm which provides faster calculations and (ii) a hierarchical key storage structure. This structure not only reveals the hierarchical relationships among the users, but also decrements the number of keys recalculated when a new file is added.

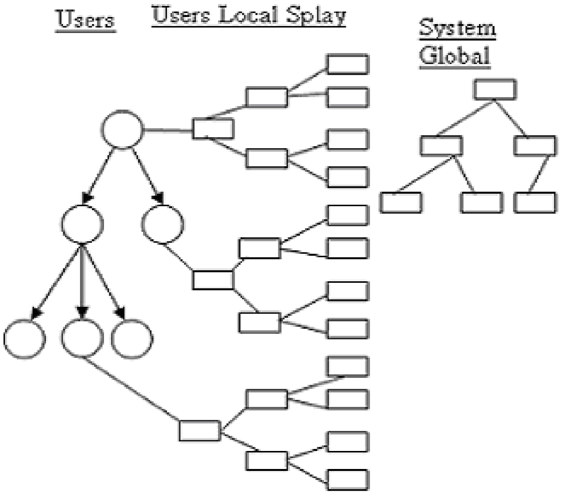

Figure 1. Hierarchical key storage structure with local splay tree directory.

In this method hierarchical structure is used to dictate the user storage of keys in the database. It is a tree structure where each node contains the calculated key. All users are formed into different groups or departments according to a group table set up by the database administrator. When a user logs on to the database, he is assigned a user node according to his unique password which has been verified by a user table. The user node contains the calculated key and a pointer that points to users own local splay tree. The local splay tree maintains file nodes which contain the file name and the unique lock number.

This local splay tree contains the files that are accessible by the user. A global splay tree is also introduced to keep track of all files and their respective owners. Since the local splay tree maintains user accessible files only, a superior user can not find files that belong to his/her inferior users.

The intervening system then retrieves the owner-pointer of the file from the global file directory and compares the relationship between the two nodes. Figure1 illustrates the hierarchical key storage structure with global and local splay tree.

1.4 Xukai Zou et al Chinese Remainder Theorem Based Hierarchical Access Control for Secure Group Communication

Xukai Zou et al. [11] proposed a new scheme for hierarchical access control group communication, in which all subgroup keys are independent. However, there are some pre-computed parameters from which an ancestor can compute the keys of all its descendants. In this scheme, every subgroup can select and change its own key independently and these keys are derived using Chinese remainder theorem.

1.5 Geon-Woo Kim et al Light-weight Access Control Mechanism Based on Authenticate Issued for Smart Home

Geon-Woo Kim et al. [3] proposed a new authorization mechanism for home network, where a number of devices with low-capacity are deployed. Their authorization mechanism uses a certificate called authenticate for access control, which contains (i) access control information and secret material (ii) a key shared between an authorization server and a relevant home resource, for making the authorization process secure. Symmetric key-based encryption algorithms are used in the authenticate

In all the above methods, access control mechanism key are developed, however these mechanisms do not specify how to secure these keys. In Xukai Zou et al. [11] method, as the every subgroup can select and change its key there is every possibility that the keys may be tampered to obtain higher access rights. In case of C. C. Chang [1], Kim S. Lee [4], Xukai Zou et al. [11] and M. L. Wu et al. keys are based on Chinese remainder theorem and number theory. These keys can be very easily factorized to obtain the access rights, and can be tampered to obtain the higher access rights. To avoid this, keys may be encrypted and stored, which is an additional overhead for the system to decrypt the keys before it can be used.

2. OUR APPROACH[1]

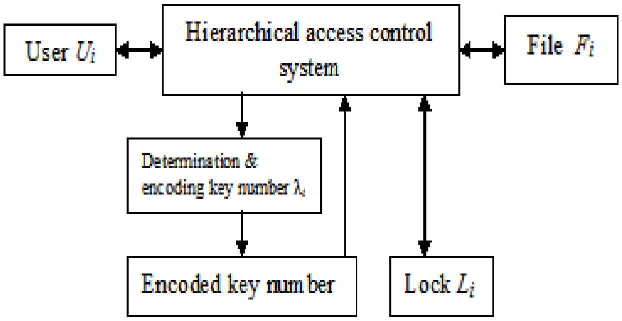
User U_i
Hierarchical access control system
File F_i
Determination & encoding key number λ_i
Encoded key number
Lock L_i

Figure 2. Encoding the key number using tribes Gaussian or rational Farey fractions.

We propose a method to encode the key (here after mentioned as key number) derived from Chinese remainder theorem. However the idea of hierarchical key storage structure that reveals the relationships among the users is retained from Kim S. Lee et al. [4] hierarchical key storage structure. Arbitrary tribes of Gaussian Farey fractions or rational Farey fractions are used to encode the key number, such that even if the user has access to key number he/she cannot determine access rights assigned and modify it accordingly to obtain unauthorized access rights. Hence the key number and the access system are secured.

This method introduces a thin layer of security to the system by encoding the key number. Figure 2 describes the proposed method of encoding the key number.

[1] Part of this work was presented at International Symposium on Data, Information & Knowledge Spectrum (ISDIKS07), 13th - 15th December, 2007, Amrita University, Kochi, India.

3. CRT AND TRIBES OF GAUSSIAN FAREY FRACTIONS

3.1 Chinese Remainder Theorem (CRT)

Theorem 1.1

Let $n_1, n_2 \ldots n_r$ be positive integers such that gcd $(n_i, n_j) = 1$ for all i,j and $i \neq j$. Then the system of linear congruencies
$x \equiv a_1(\text{mod } n_1)$, $x \equiv a_2(\text{mod } n_2)$, … $x \equiv a_r(\text{mod } n_r)$
The above set of equations has a simultaneous solution, which is unique modulo the integer $n_1, n_2 \ldots n_r$.

Example 3.1:

Let $n_1 = 3$, $n_2 = 5$, $n_3 = 7$ are relatively primes and the system of three congruencies be: $x \equiv 2(\text{mod } 3)$, $x \equiv 3(\text{mod } 5)$, $x \equiv 2(\text{mod } 7)$
Let $n = n_1 n_2 n_3 = 3 \times 5 \times 7 = 105$ and
$N_1 = n / n_1 = 35$, $N_2 = 21$ and $N_3 = 15$
Now the linear congruencies
$35x \equiv 1(\text{mod } 3)$, $21x \equiv 1(\text{mod } 5)$, $15x \equiv 1(\text{mod } 7)$ are satisfied by $x = 2$, $x = 1$ and $x = 1$ respectively.
Thus the solution of the system is given by
$\lambda = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1)$
$= 233 \text{ (mod } 105) = 23$

3.2 Tribes of Gaussian Farey Fractions

A characteristic equation is associated with Farey fractions and has fundamental solutions [2] [8]. There exists the solution for Gaussian Farey fractions and the Gaussian Farey fractions have the algebraic structures.

Let α / β be a Gaussian Farey fraction and let $\beta\varepsilon - \alpha\eta = 1$ be its characteristic equation where $\alpha = a + \mathbf{i}\, b$ and $\beta = c + \mathbf{i}\, d$.

Then $(-b, -d)$ and $(-a\,\mathbf{i}, -c\,\mathbf{i})$ are fundamental solutions of the characteristic equation. The general solution of the characteristic equation using fundamental solution $(-b, -d)$ is:
$(-b + \lambda\alpha,\ -d + \lambda\beta)$. Where $N(-b + \lambda\alpha) < N(-d + \lambda\beta)$ and
$(-b + \lambda\alpha)$ & $(-d + \lambda\beta)$ are relatively prime. (3.1)
The definition of tribe of the Gaussian Farey fraction α / β given by the set

$$T_{\alpha/\beta} = \left\{ \frac{-\mathrm{b} + \lambda\alpha}{-\mathrm{d} + \lambda\beta} \mid \forall\lambda \in J[i] \right\} \qquad (3.2)$$

And the real fractions a / c and b / d are Farey fractions.

Algebraic Structures of a tribe T $_{\alpha/\beta}$**:**

Let $T_{\alpha/\beta} = \left\{ \dfrac{-\mathrm{z_o} + \lambda\alpha}{-\mathrm{w_o} + \lambda\beta} \mid \forall\lambda \in J[i] \right\}$ be the tribe of α / β and let $\left\{ \dfrac{-\mathrm{z_o} + \lambda\alpha}{-\mathrm{w_o} + \lambda\beta} \right\}$ and $\left\{ \dfrac{-\mathrm{z_o} + \mu\alpha}{-\mathrm{w_o} + \mu\beta} \right\}$ be any two elements of the tribe $T_{\alpha/\beta}$, Where λ and $\mu \in J[i]$.

$$\left\{ \frac{-\mathrm{z_o} + \lambda\alpha}{-\mathrm{w_o} + \lambda\beta} \right\} \otimes \left\{ \frac{-\mathrm{z_o} + \mu\alpha}{-\mathrm{w_o} + \mu\beta} \right\} = \left\{ \frac{-\mathrm{z_o} + (\lambda\mu)\alpha}{-\mathrm{w_o} + (\lambda\mu)\beta} \right\} \qquad (3.3)$$

$$\left\{ \frac{-\mathrm{z_o} + \lambda\alpha}{-\mathrm{w_o} + \lambda\beta} \right\} \oplus \left\{ \frac{-\mathrm{z_o} + \mu\alpha}{-\mathrm{w_o} + \mu\beta} \right\} = \left\{ \frac{-\mathrm{z_o} + (\lambda+\mu)\alpha}{-\mathrm{w_o} + (\lambda+\mu)\beta} \right\} \qquad (3.4)$$

$\{T_{\alpha/\beta}, \oplus, \otimes\}$ is a unitary commutative integral domain, which is isomorphic to the domain of Gaussian integers.

4. ENCODING HIERARCHICAL ACCESS CONTROL MECHANISM KEY USING TRIBES OF GAUSSIAN FAREY FRACTIONS OR RATIONAL FAREY FRACTIONS

The key number is determined by Chinese reminder theorem and then encoded using Gaussian or Rational Farey Fractions.

4.1 Key Number Determination

Let there be n number of files $F_1, F_2 \ldots F_n$ in a system and a local splay tree of a user U_i, in a system. The matrix in table 2, describes the access rights to the files for the user U_i.

Table 2: **A local spare tree for user Ui**

Users / Files	F_1	F_2	**...**	F_n
Ui	a_{i1}	a_{i2}	…	a_{in}

The attributes a_{ij} are determined from function f of key k_i and lock l_i and is given by $a_{ij} = f(k_i, l_i)$, a_{ij} can have the following values as per the access rights.
$a_{ij} = 0$: for no access rights, i.e. U_i has no access right to file F_1. Similarly
1: Execute
2: Execute and Read
3: Execute, Read and Write
4: Own (Execute, Read, Write and Delete)
Select n mutually and relatively prime positive integers, $l_1, l_2 \ldots l_n$ different from attribute values a_{ij}. Each file F_j is assigned an integer l_j from the set above, while is treated as lock. The attributes $a_{i1}, a_{i2} \ldots a_{in}$ will determine the key number for the user U_i, for this consider the system of linear congruencies.
$x \equiv a_{i1}$ (mod l_1), $x \equiv a_{i2}$ (mod l_2), …$x \equiv a_{in}$ (mod l_n) (4.1)

Let the solution of the system (4.1) be λ_i. This number is called as the key number for the user U_i. For each user U_i, the unique integer λ_i is determined.

4.2 Encoding Key Number

Now we encode the key number λ_i by using either tribe of Gaussian Farey fraction α_i/β_i or Rational Farey fraction h_i/m_i to obtain the key k_i. Below illustration describes encoding of key number using the tribe of Gaussian Farey fraction.

Associate the Gaussian Farey Fraction α_i/β_i to each user U_i. The characteristic equations of α_i/β_i are given by

$$\beta_i\,\varepsilon_i - \alpha_i\,\eta_i = \pm 1,\ \pm \mathrm{i} \qquad (4.2)$$

Consider the characteristic equation,

$$\beta_i\,\varepsilon_i - \alpha_i\,\eta_i = 1 \qquad (4.3)$$

Let $\alpha_i = a_i + i\, b_i$ and $\beta_i = c_i + i\, d_i$ be two Gaussian integers where $a_i\, d_i - b_i\, c_i = 1$. Then the tribe of α_i / β_i is

$$T_{\alpha i/\beta i} = \left\{ \frac{-bi + \lambda\alpha i}{-di + \lambda\beta i} \mid \forall\lambda \in J[i] \right\} \qquad (4.4)$$

Assign the encoded key k_i to the user U_i as

$$k_i = \left\{ \frac{-bi + \lambda i\alpha i}{-di + \lambda i\beta i} \right\} = \frac{\varepsilon i}{\eta i}$$

(4.5)

By taking $\lambda = \lambda_i$, the key number which is solution of equation 4.1, therefore, the encoded key for the user U_i is $k_i = (\varepsilon_i, \eta_i)$ (4.6)

To evaluate the access rights, the access attributes are calculated by using the equation

$$k_i * l_j = \frac{\beta i(\varepsilon i + bi) + \alpha i(\eta i + di)}{2\alpha i\beta i} \pmod{l_j}$$

$$= \lambda_i \pmod{l_j} = a_{ij} \qquad (4.7)$$

Thus, the attribute a_{ij} can be evaluated with encoded key k_i and lock l_j which is the access right for the user U_i to the file F_j.

Similarly we can construct encoded key using tribes of Rational Farey fraction h_i/m_i. The attribute a_{ij} in this case is given by

$$k_i * l_j = \frac{ki(\varepsilon i - x_{0i}) + hi(\eta i - y_{0i})}{2hiki} \pmod{l_j}$$

$$= \lambda_i \pmod{l_j} = a_{ij} \qquad (4.8)$$

Example 4.1: Consider the following simple system having three users and three files as shown in Table 3.

Let $l_1 = 7$, $l_2 = 11$ and $l_3 = 13$.

By using Chinese reminder theorem, calculate the key numbers λ_1 for the user U_1.

The solution of the system of linear congruencies is given by: $x \equiv 3 \pmod 7$, $x \equiv 2 \pmod{11}$ and $x \equiv 4 \pmod{13}$

Then the key number $\lambda_1 = 6569$ by using Chinese Reminder Theorem as explained in example in section 3.1.

Table 3: A local spare tree for user *U1* with 3 files

Users / Files	*F₁*	*F₂*	*F₃*
U1	3	2	4

Let us consider arbitrary Gaussian Farey fraction

$$\frac{\alpha_i}{\beta_i} = \frac{5 + 2i}{7 + 3i}$$

So $\alpha_1 = a + i\, b = 5 + 2i$ and $\beta_1 = c + i\, d = 7 + 3i$, then encode the key number to get k_1 by using equation 4.5

$$k_1 = \left\{ \frac{-b + \lambda 1\alpha 1}{-d + \lambda 1\beta 1} \right\} = \frac{32843 + 13138\ i}{45980 + 19707\ i} = (\varepsilon_1, \eta_1)$$

Now let us verify attribute a_{11} from the equation 4.7

$$a_{11} = k_1 * l_1 = \frac{\beta 1(\varepsilon 1 + b) + \alpha 1(\eta 1 + d)}{2\alpha 1\beta 1} \pmod 7$$

$$= 6529 \bmod 7 = 3 = a_{11}$$

Notice here that the key is not decoded to get the access rights for the user to access the file F1. So there is no requirement of decoding mechanism for encoded key to determine the access rights. Similarly other access control attributes can be proved

4.3 Adding More Files to the System

Another advantage of this proposed method is that, in case more files are added to the system, no need calculate the key number (λi) for already existing files, only we need to calculate the key number for the newly added files and using any one of the two binary operations and on tribe of Gaussian Farey fractions (defined by equations 3.3 and 3.4), key number can be encoded.

Example 4.2: Assume that two more files F4 and F5 are added to the system, as shown in table 4. Then the access control matrix i.e. local splay tree for the user U1 would be as shown in table 4.

Table 4: Two more files added to the system

Users / Files	*F₁*	*F₂*	*F₃*	*F₄*	*F₅*
U1	3	2	4	2	1

The key number for the newly added files F4 and F5 is calculated as follows.

Let $l_4 = 5$ and $l_5 = 17$.

The Solution of the system of linear congruencies
$x \equiv 2 \pmod 5$, $x \equiv 1 \pmod{17}$

Let the key number for newly added files be μ_1 for user U_1, using Chinese reminder theorem as explained in example 4.1 its value will be $\mu_1 = 137$. Using binary operation $\oplus$ on tribe of Gaussian Farey fractions (defined by equation 3.4) to calculate the encoded key for user U_1 as follows.

$$k_1 = \left\{ \frac{-b + \lambda 1\alpha 1}{-d + \lambda 1\beta 1} \right\} \oplus \left\{ \frac{-b + \mu 1\alpha 1}{-d + \mu 1\beta 1} \right\}$$

$$= \left\{ \frac{-b + (\lambda 1 + \mu 1)\alpha 1}{-d + (\lambda 1 + \mu 1)\beta 1} \right\}$$

Hence the key k_1 value now is

$$k_1 = \left\{ \frac{-2 + 6706\ \alpha 1}{-3 + 6706\ \beta 1} \right\} = \left\{ \frac{33528 + 13412\ i}{46939 + 20118\ i} \right\}$$

$= (\varepsilon_1, \eta_1)$

Let us verify a_{11} the from equations 4.7

$$a_{11} = k_1 * l_1 = \frac{\beta 1(\varepsilon 1 + b) + \alpha 1(\eta 1 + d)}{2\alpha 1\beta 1} \pmod 7$$

$= 6706 \bmod 7 = 3 = a_{11}$ and for

$$a_{14} = k_1 * l_4 = \frac{\beta 1(\varepsilon 1 + b) + \alpha 1(\eta 1 + d)}{2\alpha 1 \beta 1} \pmod 5$$

$= 6706 \bmod 5 = 2 = a_{14}$

5. ANALYSIS OF ENCODING OF HACM

Proposed work computes access rights and allows the user to access the system. This section gives the time and space computational complexities of the system. The proposed access control system has 4 algorithms associated with it.

1. Chinese reminder theorem algorithm to find the solutions of the simultaneous equations (section 5.1).
2. Computing complexity of Gaussian Farey fractions (section 5.2).
3. Computing complexity of storing and retrieval of the encoded key (section 5.3)
4. Combined complexity of the system (section 5.4).

5.1 Computing Complexity of Chinese Remainder Theorem

An efficient, polynomial-time algorithm to find the solutions to the Chinese remainder theorem is based on Euclid's GCD algorithm, which is based on the following theorem.

If $a = bq + r$, where $b > 0$, then GCD (a, b) = GCD (b, r) till the division process terminates. In each of the subsequent steps, the dividend and the divisor are based on the divisor and remainder, respectively, of the previous step. Also, note that the above division process always terminates because the remainder of each step is strictly smaller than its divisor, which means smaller than the previous remainder.
Further, it can be shown that the number of division steps in computing GCD (a, b) is ≤ $\lfloor 2 \lg M \rfloor + 1$, where $M = \max(a, b)$. This expression says the time complexity of Euclid's GCD algorithm is $O(\lg \max(a, b))$, which is a polynomial-time algorithm in terms of the size of the two input integers (i.e., $\lg a + \lg b$).

Note that this process of solving a system of 3 equations is a polynomial time algorithm for arbitrary moduli m, n, and p that are pair wise co-prime, since the complexity is

$$O(\lg \max(m, n) + \lg \max(m, n, p)) = O(\lg \max(m, n, p)).$$

5.1 Time and Space Complexities of Computing Farey Sequence

For any positive integer n, the Farey sequence of order n is the set of all irreducible fractions p / q , with $0 < p < q \le n$, arranged in increasing order. An alternative definition could include 0/1 and 1/1 as special fractions. For example, the Farey sequence for $n = 5$ are given by:

$$\frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}.$$

Algorithm to combine several properties satisfied by Farey sequence, one can get a trivial iterative algorithm, which generates the next Farey fraction, based on the previous two. If p / q and p' / q' are the last two fractions, the next one is given by $\frac{p''}{q''}$ where $p'' = \left\lfloor \frac{q+n}{q'} \right\rfloor p' - p$ and $q'' = \left\lfloor \frac{q+n}{q'} \right\rfloor q' - q$. This algorithm uses $O(n^2)$ time and O (1) space.

5.3 Computing Complexity of Storing and Retrieval of the Encoded Key

In proposed method hierarchical structure is used to dictate the user storage of keys in the database. It is a tree structure where each node contains the calculated key as shown in the figure 1. All users are formed into different groups or departments according to a group table set up by the administrator. When a user logs on to the system, he/she is assigned a user node according to his/her unique password which has been verified by a user table. The user node contains the calculated encoded key and a pointer that points to users own local splay tree. The local splay tree maintains file nodes which contain the file name and the unique lock number. This local splay tree contains the files that are accessible by the user. A global splay tree is also introduced to keep track of all files and their respective owners. Since the local splay tree maintains user accessible files only, a superior user can not find files that belong to his/her inferior users.

The intervening system then retrieves the owner-pointer of the file from the global file directory and compares the relationship between the two nodes. Figure 1 illustrates the hierarchical key storage structure with global and local splay tree. When the system verifies the access right, it needs to retrieve both the encoded key and lock. If it is assumed that old single key lock system uses a splay tree to maintain lock numbers, retrieving one lock needs $O(\log_2 N)$ processing time, if N is the number of files in the system. However with the local splay tree, retrieving on lock needs $O(\log_2 n)$ processing time, where n is the average number of files in the local tree.

5.3 Combined Complexity of Encoding Hierarchical Access Control Mechanism Key Number

The encoding of key number and retrieval of the encoded key number (see from the figure 2) are two different tasks.
The encoding of the key number has 2 steps, determination of the key number and computing Farey fraction. Hence it requires O(lg max(m, n, p)) + O(n2) = O(n2) time. However to retrieving the key number does not require to decode the encoded key, hence the time complexity of retrieving key number and computing the access control attribute is O(lg n).

6. CONCLUSION

This paper describes a method to encode a key number and yet no need to decode the encoded key to determine the access rights. Chinese remainder theorem and Gaussian Farey fractions are used to encode the key. Hence encoding mechanism acts as a thin layer of security. It is showed that how ease it is to add new files to the system and assign key value to users without need to recalculate the key numbers for existing huge number of files.

The proposed method maintains the simplicity of the access control mechanism with following advantages

When a new file is added by any member in the hierarchy of users, without the new hierarchical structure, the key-lock-pair mechanism requires a recalculation of all key values in the database. However, with the presence of hierarchical key storage structure, insertion or deletion of file requires recalculation of keys on affected users.

In the key-lock-pair mechanism based on the Chinese remainder theorem, calculation of all keys depends on all locks. Since the most files in a system are not accessible by most users, these inaccessible files have lock numbers included in the key calculation. With the local splay tree, calculation of a key only depends on lock numbers that are accessible by a user. Thus the computational time is reduced.

When the system verifies the access right, it needs to retrieve both key and lock. If we assume old single key lock system uses a splay tree to maintain lock numbers, retrieving one lock needs $O(\log_2 N)$ processing time, if N is the number of files in the system. However with the local splay tree, retrieving on lock needs $O(\log_2 n)$ processing time, where n is the average number of files in the local tree.

This method introduces a thin security layer to the system by encoding the key using arbitrary Farey fraction and this thin security layer is visible only while encoding the key.

7. REFERENCES

[1] C. C. Chang, 1987, "An Information Protection Scheme Based upon Number Theory", The Computer Journal, Vol. 30, No. 3, pp. 249-253.

[2] H. Chandrashekhar and M. Nagaraj, 1994, "Tribes of Gaussian Farey Fractions", The Mathematical Student, Vol. 63, 1-4, pp.196-200.

[3] Geon-Woo Kim, Jong-Wook Han, 2008, "Light-weight Access Control Mechanism based on Authenticate issued for Smart Home", International Journal of Smart Home, Vol. 2, No. 4.

[4] Kim S. Lee, Huizhu Lu, D. D. Fisher, 1992, "A Hierarchical Single-Key-Lock Access Control Using the Chinese Remainder Theorem", Symposium on Applied Computing Proceedings, pp: 491 – 496.

[5] Manoj Kumar, 2010, "A New Secure Remote User Authentication Scheme with Smart Cards", International Journal of Network Security, Vol.11, No.3, PP.112–118.

[6] Manpreet Singh, Manjeet S. Patterh, 2010, "Formal Specification of Common Criteria Based Access Control Policy Model", International Journal of Network Security, Vol.10, No.3, PP.232–241.

[7] M. L Wu and T. Y. Hwang, 1984, "Access control with single key-lock", IEEE Transaction on Software Engineering, Vol. SE-10, No. 2, pp.185-191.

[8] M. Nagaraj & Srinivas Murthy, 1989, "Properties of Tribes of Farey Fractions", J. Ramanujan Math, Soc 4(i), pp 25-31.

[9] Sabrina De Capitani di Vimercati1, Pierangela Samarati1, and Sushil Jajodia2, 2005, "Policies, Models, and Languages for Access Control", S. Bhalla (Ed.): DNIS 2005, LNCS 3433, Springer-Verlag Berlin Heidelberg 2005, 225–237.