Honam Mathematical J. **28** (2006), No. 2, pp. 185 -196

THE MULTILEVEL SECURITY PROBLEM OVER CLASS SEMIGROUPS OF IMAGINARY QUADRATIC NON-MAXIMAL ORDERS

YONGTAE KIM

Abstract. A scheme based on the cryptography for enforcing multilevel security in a system where hierarchy is represented by a partially ordered set was first introduced by Akl et al. But the key generation algorithm of Akl et al. is infeasible when there is a large number of users. In 1985, MacKinnon et al. proposed a paper containing a condition which prevents cooperative attacks and optimizes the assignment in order to overcome this shortage. In 2005, Kim et al. proposed key management systems for multilevel security using one-way hash function, RSA algorithm, Poset dimension and Clifford semigroup in the context of modern cryptography. In particular, the key management system using Clifford semigroup of imaginary quadratic non-maximal orders is based on the fact that the computation of a key ideal K_0 from an ideal EK_0 seems to be difficult unless E is equivalent to O. We, in this paper, show that computing preimages under the bonding homomorphism is not difficult, and that the multilevel cryptosystem based on the Clifford semigroup is insecure and improper to the key management system.

Received April 18, 2006. Revised June 15, 2006.

2000 Mathematics Subject Classification : 11Y40, 94A60.

Key words and phrases :class semigroup, non-invertible ideal, power of ideals/classes, public key cryptosystem.

† This research was partially supported by Gwangju National University of Education Research Grant 2005.

1. Introduction

The multilevel security problem arises in organizations where hierarchical structures such as government, diplomacy, business and military exist. In 1982, Akl et al. [1] presents a solution to the multilevel security problem based on cryptography, and they generate the keys K_i relying on the fundamental assumption behind the RSA. The key generation algorithm of them has the advantage that only copy of a piece of information is stored or broadcast and its disadvantage is the large number of keys held by each user. In an effort to overcome this shortage, MacKinnon et al. [10] proposed a paper containing an additional condition which prevents cooperative attacks and optimizes the assignment by giving an improved algorithm to remove the nodes of the longest chain. In 2005, Kim et al. [8] proposed key management systems for multilevel security using one-way hash function, RSA algorithm, Poset dimension and Clifford semigroups. In particular, the key management system using Clifford semigroups of imaginary quadratic non-maximal orders is based on the fact that the computation of the key ideal K_0 from an ideal EK_0 seems to be difficult unless E is equivalent to O. Using the properties of commutative semilattice of idempotents, in this paper, we show that computing preimages of the key ideal K_0 under the bonding homomorphism is not difficult, and that the multilevel cryptosystem based on the Clifford semigroup is insecure and improper to the key management system.

2. Multilevel security problem and its cryptographic solution

The notion of the multilevel security and the key management can be found in [1,10]. Assume that the users of computer system are divided into a number of disjoint sets, $U_1, U_2, \cdots, U_n$, which are called security classes. By the partially ordered relation $\leq$ on the set $S = \{U_1, U_2, \cdots, U_n\}$ of classes, the relation $U_i \leq U_j$ in the partially ordered set $(S, \leq)$ means that users in U_i have a security clearance lower than or equal to those in U_j, in other words, users in U_j can have access to information held by users in U_i, while the opposite is not allowed. Let x_m be a piece of information, that a central authority(CA) desires to store in (or broadcast over) the system. Then the meaning of the subscript m is that object x is accessible to users in class U_m and the users in all classes U_i such that $U_m \leq U_i$. In addition to above conditions, the access to information should be as decentralized as possible so that authorized users are able to independently retrieve x_m as soon as it is stored or broadcast by the CA. In [1], Akl et al. proposed a cryptographic solution to the multilevel security problem in three steps as follows.

Step 1 : The CA generates n (deciphering) keys, $K_1, K_2, \cdots, K_n$, for use with the crytoalgorithm.

Step 2 : For $i = 1, 2, \cdots, n$, key K_i is distributed to all users in U_i who keep it secret.

Step 3 : In addition, for $i, j = 1, 2, \cdots, n$, all users in U_j also obtain K_i if $U_i \leq U_j$.

Let E_K and D_K be enciphering and deciphering procedure under the control of the ciphering key K. When an information x_m is to be stored (or broadcast) it is first encrypted with K_m to obtain $x' = E_{K_m}(x_m)$ and then stored or broadcast as the pair $[x', m]$. This guarantees that only users in possession of K_m will be able to retrieve x_m from $x_m = D_{K_m}(x')$. This solution has the advantage that only copy of x_m is stored or broadcast and its disadvantage is the large number of keys held by each user. In order to solve the key storage problem, Akl et al.[1] proposed a key management system in which a user in U_j stores only own key K_j, and can compute from this the key K_i if and only if $U_i \leq U_j$. In such a system, however, there exists the possibility of two users collaborating to compute a key to which they are not entailed. In [10], MacKinnon et al. formulate a condition which prevent such cooperative attacks and characterize all keys assignments which satisfy the condition, and they proposed the following algorithm;

Algorithm : Longest Chain

Step 4 : Find the longest chain $\{i_1, \cdots, i_k\}$ in the poset.

Step 5 : Assign to this chain the smallest available prime p (which now becomes unavailable).

Step 6 : Remove nodes $i_1, \cdots, i_k$ from the poset.

Step 7 : If the poset is not empty, go to Step 4.

Although its running time is $O(|S|^2)$, this algorithm is just an heuristic and the authors generate the keys K_i relying on the fundamental assumption behind the RSA.

3. The structure of the class semigroup $Cls(O)$

In this section, we introduce some facts concerning class semigroups of orders in imaginary quadratic fields. Most of the terminologies, throughout this paper, are due to Gauss[6], and notations and some preliminaries are due to Cox[4], Zanardo and Zannier[13] and Jacobson[7]. The notations O, Z and Q denote the imaginary quadratic non-maximal order, the ring of integers and the field of rational numbers respectively. Let $D_1 < 0$ be a square free rational integer, $D = 4D_1/r^2$, where $r = 2$ if $D_1 \equiv 1 \bmod 4$, and $r = 1$ if $D_1 \equiv 2, 3 \bmod 4$. Then $K = Q(\sqrt{D_1})$ is an imaginary quadratic field of discriminant D. Note that $K = Q(\sqrt{D})$. If $\alpha, \beta \in K$, we denote by $[\alpha, \beta]$ the set $\alpha Z + \beta Z$. An order in K having conductor f with discriminant $D_f = f^2 D$ is denoted by $O = [1, f\omega]$, where $\omega = (D + \sqrt{D})/2$. An (integral)ideal A of O is a subset of O

such that $\alpha+\beta \in A$ and $\alpha\lambda \in A$ whenever $\alpha, \beta \in A, \lambda \in O$. For $\alpha \in K, \alpha', N(\alpha)$ and $Tr(\alpha)$ denote the complex conjugate, norm and trace of α respectively. Let $\gamma = f\omega$. Then any ideal A of O (any O-ideal) is given by $A = [a, b+c\gamma]$, where $a, b, c \in Z$, $a > 0, c > 0$, $c \mid a, c \mid b$ and $ac \mid N(b+c\gamma)$. If $c = 1$, then A is called primitive, which means that A has no rational integer factors other than 1. Then $A = [a, b+\gamma]$ is O-ideal if and only if a divides $N(b+\gamma)$. We say that A and B are equivalent ideals of O and denote $A \sim B$ if there exist non-zero $\alpha, \beta \in K$ such that $(\alpha)A = (\beta)B$ (this relation actually is equivalent relation). We denote the equivalence class of an ideal A by $\overline{A}$. An ideal class $\overline{I}$ is called idempotent if $\overline{I}^2 = \overline{I}$ and the ideal I is also called idempotent. Let $I(O)$ be the set of non-zero fractional ideals of O, and $P(O)$ the set of non-zero principal ideals of O. Then $Cls(O) = I(O)/P(O)$ will be the class semigroup of the order O. We remind that the commutative semigroup $\mathcal{S}$ is called a Clifford commutative semigroup if one of the following equivalent statements holds (Confer [13]).

C1) every element x of $\mathcal{S}$ is contained in a subgroup G of $\mathcal{S}$,

C2) every element x of $\mathcal{S}$ is regular, i.e. there exists $y \in \mathcal{S}$ such that $x = x^2y$ (such an x is called von Neumann regular),

C3) $\mathcal{S}$ is a semilattice of groups.

In the sequel, we will set the positive definite quadratic form $u(x,y) = ax^2+bxy+cy^2$ as (a,b,c) for brevity, and call η the root of $u(x,y)$ if $u(\eta,1) = 0$, where η lies in the upper half plane. We begin with introducing the following lemma.

Lemma 3.1. *([9], Lemma 3.2) Let $u(x,y) = (a,b,c)$ be a positive definite quadratic form with discriminant D_f, where $k = \gcd(a,b,c)$. Let η be the root of $u(x,y)$. Then the ideal $[a, a\eta]$ is invertible if and only if $k = 1$ in the order $O = [1,\gamma]$ of K.*

In particular, if $a = k$, then we denote the ideal $[k, k\eta]$ by E_k. By simple calculations and Lemma 1, it is easily shown that $E_k = [k, \gamma]$

for any divisor $k \mid f$. To clarify the structure of $Cls(O)$, we need the following two lemmas.

Lemma 3.2. *([13, Theorem 10]) Let $I = [a, b+\gamma]$ be a non-zero O-ideal and* $\gcd(I) = k$. *Then we have $E_k^2 = kE_k, II' = aE_k, IE_k = kI$.*

Note that E_k's are the only idempotent elements in the order O. For a quadratic form $u(x,y) = (a,b,c)$, we define

$$\gcd(u(x,y)) = \gcd(a,b,c), u_1(x,y) = (1/\gcd(u(x,y)))u(x,y),$$

$$\gcd(I) = \gcd(a, Tr(b+\gamma), N(b+\gamma)/a)$$

for a non-zero O-ideal $I = [a, b+\gamma]$, and denote the discriminant of I by $Tr(b+\gamma)^2 - 4N(b+\gamma)$.

Lemma 3.3. *Suppose that I and J are O-ideals with same discriminant D_f such that* $\gcd(I) = k_1, \gcd(J) = k_2$. *Then* $\gcd(IJ) = lcm(k_1, k_2)$.

Proof. Let $u(x,y)$ and $v(x,y)$ be positive definite quadratic forms with discriminant D_f corresponding to the ideals I and J respectively. We now define $u(x,y) = k_1u_1(x,y)$ and $v(x,y) = k_2v_1(x,y)$, where $k_1 = \gcd(u(x,y))$ and $k_2 = \gcd(v(x,y))$. In this case, if $f = k_1d_1 = k_2d_2$, then $u_1(x,y)$ and $v_1(x,y)$ are primitive with discriminant d_1^2D and d_2^2D respectively. From Gauss[6, art.236], the direct composition $U_1(x,y)$ of $u_1(x,y)$ and $v_1(x,y)$ has the discriminant d^2D, where $d = \gcd(d_1, d_2)$. From elementary number theory, we have $f = kd$, where $k = lcm(k_1, k_2)$. From this fact, if we denote $U(x,y)$ the direct composition of $u(x,y)$ and $v(x,y)$, then we have $\gcd(U(x,y)) = k$. This completes the proof. □

It is well-known that the cardinality of $Cls(O)$ is finite. Now we are ready to clarify the structures of the group G_δ and the semigroup $Cls(O)$.

Theorem 3.4. *([9], Theorem 3.7) The class semigroup* $Cls(O) = \cup_{k|f} G_{\overline{E_k}}$, *where* $G_{\overline{E_k}}$ *is the set of all classes containing O-ideals I with* $\gcd(I) = k$.

Note that $G_{\overline{E_1}} (= Cl(O)$, the class group) contains all the equivalence classes of invertible ideals in O and $\mathcal{E}$, which is the set of all the equivalence classes of idempotent in O, is the semilattice since $Cls(O)$ is the Clifford semigroup. In $Cls(O)$, for $\overline{E_i}, \overline{E_j} \in \mathcal{E}$ such that $\overline{E_j} \leq \overline{E_i}$ in the partial order defined on $\mathcal{E}$, there exists a bonding homomorphism $\phi_{\overline{E_i E_j}} : G_{\overline{E_i}} \to G_{\overline{E_j}}$. In [13], Zanardo and Zannier proved the following theorem which ensures the existence of the surjective bonding homomorphisms among the groups $G_{\overline{E_k}}$, and gave the method for finding a preimage of a non-invertible ideal under the bonding homomorphism.

Theorem 3.5. *(Confer [13, Theorem 16 and Theorem 17]) Let* $E_k = [k, \gamma]$, *where* $k \mid f$, *and let I be an O-ideal such that* $\overline{I} \in G_{\overline{E_k}}$. *Then* $JE_k = kI$ *for some invertible ideal J. Therefore all the bonding homomorphisms of the Clifford semigroup* $Cls(O)$ *are surjective.*

The general and efficient algorithms for multiplication of ideals are referred to [3,4,5].

4. Analyses of KMS

In [8], Kim et al. proposed four key management systems(KMS) for multilevel security. Among them, we now revisit the KMS using the Clifford semigroups of imaginary quadratic non-maximal orders to consider its security. The KMS proceeds as described in [8].

4.1. KMS using the properties of semilattice of idempotents

The parameters needed to class semigroups of imaginary quadratic non-maximal orders are first selected, and then the idempotents of the class semigroups are introduced.

1. a sufficiently large conductor f.
2. an idempotents $\overline{E_k}$ of $Cls(O)$ is the equivalent class of an ideal of the form $E_k = [k, \gamma]$, where k is a divisor of f.
3. for $\overline{E_h}, \overline{E_k} \in \mathcal{E}$, where the ideal $E_h = [h, \gamma]$, the partial order $\leq$ on $\mathcal{E}$ defined by $\overline{E_k} \leq \overline{E_h}$ if $h|k$.
4. a key ideal K_0.

If $\overline{E_i}, \overline{E_j}$ are idempotents, where $\overline{E_j} \leq \overline{E_i}$, then the bonding homomorphism $\phi_{\overline{E_i}\overline{E_j}} : G_{\overline{E_i}} \to G_{\overline{E_j}}$ is defined by $\phi_{\overline{E_i}\overline{E_j}}(\overline{K}) = \overline{E_j K}$, where $\overline{K} \in G_{\overline{E_i}}$. First, the CA assigns an idempotent ideal E_{k_i} to each class U_i, and selects a random key K_0, and computes $E_{k_2}K_0, E_{k_3}K_0$, and then distributes each of them to the classes U_2 and U_3 respectively. The CA next computes $E_{k_2}E_{k_4}K_0, E_{k_2}E_{k_5}K_0, E_{k_3}E_{k_6}K_0$, and $E_{k_3}E_{k_7}K_0$, and then distributes them to U_4, U_5, U_6 and U_7 respectively in the third row of Fig.1. In this way, the CA computes the keys of all classes, and distributes each of them respectively. Then the users in an upper class can compute all keys belonging to classes lower than itself. In particular, the authors in [8] claimed that the computation of K_0 from $E_{k_i}K_0$ seems to be difficult unless E_{k_i} is equivalent to O.

4.2. Analyses of the KMS

In this section, we like to analyze the KMS above by considering the structure the class semigroups and the properties of their ideals in the following points of view. Let E_h, E_k, K_0 and the corresponding bonding homomorphism $\phi_{\overline{E_h}\overline{E_k}} : G_{\overline{E_h}} \to G_{\overline{E_k}}$ be the same as above, and we assume that $\overline{E_k} \leq \overline{E_h}$, where $\overline{E_h} \in G_{\overline{E_h}}$.

4.2.1. *Computing preimages under the bonding homomorphism.* 1. Kim et al.[8] are right in saying that the users in an upper class can compute all keys belonging to classes lower than itself.
2. The authors claimed that the computation of K_0 from E_kK_0 seems to be difficult unless E_k is equivalent to O. It, however, is not difficult

to calculate K_0 from $J = E_k K_0$. In fact; Jacobson[7] says that the algorithm in Theorem 2 is one to one on the level of ideals, but given an equivalence class $\overline{J} \in G_{\overline{E}_k}$, one can apply it to any ideal representative equivalent to J, thereby randomizing over the ideal classes in $Cl(O)$ whose images under ϕ_k are equal to $\overline{J}$.

4.2.2. *Choosing the key ideal.* 1. In [8], the authors choose the key ideal K_0 arbitrarily. It, however, is not easy to select a non-invertible ideal of a non-maximal order.
2. In general, for an (invertible or not) ideal K_0 with $\gcd(K_0) = h$, Theorem 3.5 ensures that there exists an invertible O-ideal K such that $KE_h = hK_0$, and thus $\overline{K_0 E_k} = \overline{KE_k}$ by Lemma 3.2. From this fact, without loss of generality, $G_{\overline{E_h}}$ can be replaced by $Cl(O)$, and h can be always taken 1. For brevity, we denote ϕ_k the bonding homomorphism of $Cl(O)$ to $G_{\overline{E_k}}$.

4.2.3. *Security of the KMS.* 1. Theorem 3.5 describes an algorithm for computing the required preimages given only a representative of an ideal class in $G_{\overline{E_k}}$ and k under ϕ_k. In general, we have $| G_{\overline{E_k}} |<| Cl(O) |$, which means that the preimage of a representative of an ideal class in $G_{\overline{E_k}}$ under ϕ_k is not unique. Since there are $|Ker(\phi_k)|$ different preimages of $\overline{J}$ under ϕ_k, the worst case number of attempts before one expect to succeed with this strategy is at most $|Ker(\phi_k)|$, which is significantly small in general. The procedure for computing preimage by changing under ϕ_k can be randomized by changing the representative of the ideal equivalence class. If the first chosen preimage does not find I, the process is simply repeated until it is found.
2. On the other hand, if the number of users U_i of the KMS are large, then so are the number of idempotents E_{k_i} of the class semigroup $Cls(O)$ used. From Theorem 3.4, the number of prime factors of f becomes

large, and thus each length of the prime factor is relatively small if f is fixed, which means that the multilevel security problem in $Cls(O)$ of the above KMS is reduced to the multilevel security problem in the class group $Cl(O)$(Recall that the class group $Cl(O)$ is a proper subgroup of $Cls(O)$ by Theorem 3.4) and a lot of number of finite fields corresponding to the prime factors of f. Thus, the cryptosystems in the class semigroup $Cls(O)$ using non-invertible ideal offer less security than cryptosystems in class group $Cl(O)$. In this case, the conductor f can be factored completely so that the structure of $Cls(O)$ can be easily revealed by Theorem 3.4, and thus the cryptosystem based on $Cls(O)$ can be easily broken.

3. By Lemma 3.3, we have $\overline{E_{k_1}E_{k_2}} = \overline{E_{k_2}}$ if $k_2|k_1$, and thus the deciphering key $\overline{E_{k_1}E_{k_2}K_0}$ of the user U_2 in Step 1 and Step 2 is equal to $\overline{E_{k_2}K_0}$. That is, the multiplication of two idempotents which are totally ordered by the partial order $\leq$ on $\mathcal{E}$ becomes to be the idempotent of lower user in the level of class. Thus, the possibility of finding the key K_0 is equal to all users.

4. In addition, if $\overline{E_{k_2}} \leq \overline{E_{k_1}}$, where $E_{k_1} = [k_1, \gamma]$ and $E_{k_2} = [k_2, \gamma]$, then k_1 is a divisor of k_2, which means that a user in U_2 of the lower class in Step 3 is able to calculate the ideal E_{k_1} by factoring k_2 of the upper class. Consequently, the meaning of the level of information security will be lost under the multilevel cryptosystem based on the Clifford semigroup.

5. Conclusion

A cryptographic scheme for enforcing multilevel security in a system where hierarchy is represented by a partially ordered set was introduced by Akl et al. They generate the keys K_i relying on the fundamental assumption behind the RSA. But the key generation algorithm of Akl et al. is infeasible when there is a large number of users. To overcome this shortage, in 1985, MacKinnon et al. proposed a paper containing a condition which prevents cooperative attacks and optimizes the assignment. In 2005, Kim et al. proposed key management systems for multilevel security using one-way hash function, RSA algorithm, Poset dimension and Clifford semigroup in the context of modern cryptography. In particular, the key management system in [8] using Clifford semigroup of imaginary quadratic non-maximal orders is based on the fact that the computation of a key ideal K_0 from an ideal EK_0 seems to be difficult unless E is equivalent to O. Using the properties of commutative semilattice of idempotents, in this paper, we show that computing preimages of the key ideal K_0 under the bonding homomorphism is not difficult, and that the multilevel cryptosystem based on the Clifford semigroup is insecure and improper to the key management system.

References

[1] Selim G. Akl, Peter D. Taylor, *Cryptographic Solution to a Multilevel Security Problem*, CRYPTO 1982(1982) pp.237-249.

[2] Selim G. Akl, Peter D. Taylor, *Cryptographic Solution to a Problem of Access Controlin Hierarchy*, ACM Trans. Computer System 1(3)(1983) pp.239-248.

[3] J. Buchmann, H. C. Williams, *A key-exchange system based on imaginary quadratic fields*, J. Cryptology 1(1988)pp.107-118.

[4] D. Cox, *Primes of the form* $x^2 + ny^2$, Wiley,New York(1989).

[5] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin(2000).

[6] C. F. Gauss, *Disquisitiones Arithmeticae* , translated by Clarke A. A., Springer-Verlag, New York(1986).

[7] Michael J. Jacobson Jr. , *The security of cryptosystems based on class semigroups of imaginary quadratic non-maximal orders* ASISP 2004, LNCS 3108(2004)pp.149-156.

[8] Hwankoo Kim, Bongjoo Park, JaeCheol Ha, Byoungcheon Lee, DongGook Park, *New Key Management Systems for Multilevel Security*, ICCSA 2005, LNCS 3481(2005)pp.245-253.

[9] Yongtae Kim, *On the structures of class semigroups of quadratic non-maximal orders*, Honam Mathematical Journal vol.26 no.3(2004) pp.247-256.

[10] Stephen J. MacKinnon, Peter D. Taylor, Henk Meijer, Selim G. Akl, *An Optimal Algorithm for Assignment Cryptographic Keys to Control Access in a Hierarchy*, IEEE Trans. on Computers vol.34 no.9(1985) pp.797-802.

[11] S. Paulus, T. Tagaki, *A new public-key cryptosystem over a quadratic order with quadratic decryption time*, Journal of Cryptology 13(2000)pp.263-272.

[12] R. L. Rivest, A. Shamir, L. Adelman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of ACM 21(1978)pp.120-126.

[13] P. Zanardo, U. Zannier, *The class semigroup of orders in number fields*, Math. Proc. Camb.Phil. Soc. 115(1994)pp.379-391.

Yongtae Kim
Dept. of Mathematics Education,
Gwangju National Univ. of Education,
Gwangju, South Korea
Email : ytkim@gnue.ac.kr