On the Security of Multilevel Cryptosystems over Class Semigroups of Imaginary Quadratic Non-maximal Orders*

Yongtae Kim[1], Chang Han Kim[2], and Taek-Young Youn[3]

[1] Dept. of Mathematics Education,
Gwangju National Univ. of Education,
Gwangju, Korea
ytkim@gnue.ac.kr
[2] Dept. of Information and Security,
Semyung Univ., Jecheon, Korea
chkim@semyung.ac.kr
[3] Center for Information Security Technologies(CIST),
Korea Univ., Seoul, Korea
taekyoung@cist.korea.ac.kr

Abstract. A cryptography for enforcing multilevel security in a system where hierarchy is represented by a partially ordered set was introduced by Akl et al. 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 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.

Keywords: Hierarchy, Key generation algorithm, Class semigroup, Key exchange system.

1 Introduction

An organization with hierarchical structure such as government, diplomacy and military can require users highly placed in the hierarchy to keep a security clearance lower than or equal to those lowly placed. In this context a cryptography

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 92–100, 2006.

for enforcing multilevel security in a system where hierarchy is represented by a partially ordered set(poset) was introduced by Akl et al. [1]. They generate the keys K_i relying on the fundamental assumption behind the RSA. The key generation algorithm of Akl et al. [1] 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. [9] 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 [1,9]. 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