On the Security of "A Novel Elliptic Curve Dynamic Access Control System"

Wen-Chung Kuo
Department of Computer Science and Information Engineering,
National Formosa University, Taiwan 632, R.O.C.
Email: simonkuo@nfu.edu.tw
Lih-Chyau Wuu
Graduate School of Engineering Science and Technology
National YunLin University of Science and Technology, Taiwan 640, R.O.C.
Email: wuulc@yuntech.edu.tw

Abstract

In 2007, Wen et al. proposed a novel elliptic curve dynamic access control system. In this paper, we will show that the scheme is vulnerable to various attacks.

1 Introduction

As the development of information data and networking technology increase rapidly, various digital multimedia can be transmitted over the Internet. In order to manage the accessing priority, many computer communication systems often employ user hierarchies to solve access control problems. A user hierarchy structure is constructed by dividing users into a number of disjoint classes $SC_1, SC_2, \ldots, SC_n$ are n disjointed classes with a binary partially ordered relation $\leq$. The meaning of $SC_i \leq SC_j$ denotes that the security class SC_j have a security clearance higher than or equal to the security class SC_i, while the opposite is not allowed. This form of access control mechanism has many proven operational and security benefits, and has therefore been widely applied for a diverse range of governmental, diplomatic, military and business systems applications[13].

Fig.1 shows the poset in a user hierarchy and the arrowhead represents a relationship that the higher-level security class is authorized with the security clearance higher than the lower-level one. For example, there is an arrow from SC_3 to SC_6, i.e. the statement $SC_6 \leq SC_3$, means that SC_3 is the predecessor of SC_6 and SC_6 the successor of SC_3. In other words, users in SC_3 can derive the secret key in SC_6 and access information held by users in SC_6, but the users in SC_6 cannot access the information held by the users in SC_3. Furthermore, if there is no other security class SC_2 in SC so that $SC_5 \leq SC_2 \leq SC_1$, then SC_1 is called the immediate predecessor of SC_5, and SC_5 the immediate successor to SC_1. [2]

Akl and Taylor [1](AT-scheme for short) first proposed a simple cryptographic key assignment scheme to solve the access control problems in 1983. However, there is a serious drawback in AT-scheme, i.e., it fails to provide the user with a convenient way to change his/her secret key under the secure considerations. In order to solve this drawback, a dynamic access control scheme is proposed with the following characteristics: (1)the key generation and derivation algorithms are

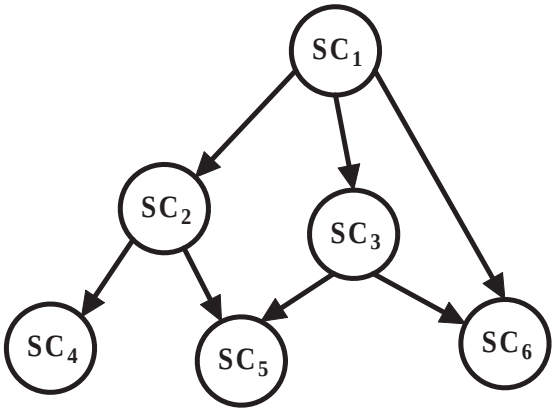

Figure 1: Poset in a user hierarchy.

as simple as possible; (2)the re-updating key problem can be efficiently solved; (3)the users can change theine secret keys anytime and anywhere for the sake of security; (4)the system can withstand the collusive attacks[2]. Until now, there are several key management schemes [5, 11, 14, 15] were forwarded for improving dynamic access control. In 1997, a novel cryptographic key assignment scheme for dynamic access control in a hierarchy based on Rabin's public key system[10] and Chinese remainder theorem[3] was proposed by (SCL-scheme for brevity). They stated that the SCL-scheme is much simpler to implement than other cryptographic key assignment schemes for access control in a hierarchy. In fact, Shen *et al.* used the Rabin's scheme to hide the user's secret key K_i. Furthermore, reducing the computation time for key assignment and the storage size for public parameters in the SCL-scheme, Hwang used the exclusive-or operation to replace the main function of Rabin's scheme[5].

Lately, a hierarchical access control scheme based on the secure filter method was proposed by K. P. Wu *et al.*[15] (WRTL-scheme for short) in 2001. They used the exponential operation formula $Sf_i(x) = \prod_{k=0}^{n-1}(x-g_i^{s_k})+k_i \bmod p$ to construct a secure filter, in which p is a large prime; s_k represents a secure code, with $0 \geq s_k \geq p-1$; g_i is the primitive root, with $1 \geq g_i \geq p-1$; and k_i is the secret key. Afterward this secure filter had been applied to the dynamic access control system[15]. However, Wen *et al.*[14] pointed out the secure filter has the following two faults. One is the secure filter employs exponential operation which takes a longer time than the simple multiplication does and the other is the exponential operation takes up a much larger storage space than the simple multiplication does.

Recently, a novel access control in user hierarchy based on elliptic curve cryptosystem was proposed by Wen *et al.*(WWC-scheme for short)[14]. According to the WWC-scheme, the special feature of this scheme can not only solve dynamic access problems in a user hierarchy but also perform in terms of both security and efficiency is quite commendable. However, the security of WWC-scheme is also insecure under the dynamic exterior attack. In other words, the security of WWC-scheme is not guaranteed when a new security class joins or a new ordered relationship is added into this scheme. In this paper, we will show that the attacker can easily recover the user's secret key without knowledge of the CA's private key.

The rest of the paper is organized as follows: In Section 2, we briefly introduce the WWC-scheme. In Section 3, we discuss the security of WWC-scheme. Conclusions are drawn in last section.

2 Review the WWC-scheme

2.1 The operations of the Elliptic Curve

We assume that the general form of elliptic curve $E_p(a,b) : y^2 = x^3 + ax + b \bmod p$, where p is a prime and the values of a, b satisfy the discriminant condition, $D = 4a^3 + 27b^2 \neq 0 \bmod p$, is used in this scheme. From this definition, we can define the rules of addition over an elliptic curve $E_p(a,b)$:[7, 9, 12]

1. $\mathcal{O}$ serves as the additive identity. Thus $-\mathcal{O} = \mathcal{O}$ and $P + \mathcal{O} = P$.

2. $-P$ is the negative of a point P; that is, if $P = (x,y)$, then $-P = (x,-y)$. Note that $P + (-P) = \mathcal{O}$.

3. If $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$, and $Q \neq -P$, then $P + Q = -R$. Here, R is the intersection point of $E_p(a,b)$ and the line segment $\overline{PQ}$. Let $P = (x_1, y_1) \in E_p(a,b)$, $Q = (x_2, y_2) \in E_p(a,b)$, then $P + Q = (x_3, y_3)$,

   - If $P \neq Q$, then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$.

   - If $P = Q$, then $\lambda = \frac{3x_1^2 + a}{2y_1}$, $x_3 = \lambda^2 - 2x_1$ and $y_3 = \lambda(x_1 - x_3) - y_1$.

Therefore, if a point G is taken as the base point over the elliptic curve $E_p(a,b)$, then the operation on nG has the following properties. $1G = G$, $2G = G + G$, $3G = 2G + G$, $\ldots, (n-1)G = (n-2)G + G$, $nG = (n-1)G + G = O$ and $(n+1)G = G$.[7]

The Table 1 lists the elements of the elliptic groups with $p = 23$[8].

Table 1. The Elliptic Group $E_{23}(1,1)$

$(0,1)$	$(0,22)$	$(1,7)$	$(1,16)$
$(3,10)$	$(3,13)$	$(4,0)$	
$(5,4)$	$(5,19)$	$(6,4)$	$(6,19)$
$(7,11)$	$(7,12)$	$(9,7)$	$(9,16)$
$(11,3)$	$(11,20)$	$(12,4)$	$(12,19)$
$(13,7)$	$(13,16)$	$(17,3)$	$(17,20)$
$(18,3)$	$(18,20)$	$(19,5)$	$(19,18)$

Example 1: Let $P = (3,10)$ and $Q = (9,7)$ be in $E_{23}(1,1)$, then we can find out $P+Q = (17,20)$ as the following operations.

Step 1 Compute $\lambda = \frac{7-10}{9-3} \bmod 23 = 11 \bmod 23$.

Step 2 Calculate $x_3 = \lambda^2 - x_1 - x_2 \bmod 23 = 17 \bmod 23$.

Step 3 Compute $y_3 = -y_1 + \lambda(x_1 - x_3) \bmod 23 = 20 \bmod 23$.

2.2 The WWC-scheme

The WWC-scheme based on elliptic curve cryptosystem [14]. We assume that a Central Authority(CA) exists and the set $SC = \{SC_1, SC_2, \ldots, SC_n\}$, where $SC_1, SC_2, \ldots, SC_n$ are n disjointed security classes with a binary partially ordered relationship $\leq$ in WWC-scheme. Therefore, $SC_i \leq SC_j$ denotes that the security class SC_j have a security clearance higher than or equal to the security class SC_i. SC_j is classified as a predecessor of SC_i, and SC_i as a successor of SC_j. The predecessors SC_j have the accessibility to information belonging to their successors SC_i, but not vice versa. Here, the WWC-scheme is summarized as follows:

Key generation. To complete the key generation phase, CA executes the algorithm below.

Step 1 Choose select an elliptic curve $E_p(a, b) : y^2 = x^3 + ax + b \bmod p$, where a, b such that $D = 4a^3 + 27b^2 \neq 0 \bmod p$, and the point G_i on $E_p(a, b)$ as the base point for SC_i.

Step 2 The CA chooses user secret codes n_j for all j satisfying $SC_i \leq SC_j$ and $j \neq i$, where n_j is a prime, and performs elliptic curve multiplication with the base point G_i to get $n_jG_i = (x_j, y_j)$ and $f(n_jG_i) = x_j \oplus y_j$.

Step 3 The CA constructs a public elliptic curve polynomial(ECP) $E_i(x)$ as follows:

$$E_i(x) = \prod_j [x - f(n_jG_i)] + k_i \bmod p. \tag{1}$$

where k_i is the secret key of the user u_i and $\prod_j$ is performed for all j such that $SC_i \leq SC_j$ and $j \neq i$.

Step 4 The CA distributes $E_i(x)$ and G_i to the user u_i of security class SC_i and publishes them.

Example 2: There are six users, i.e., $U = \{u_1, u_2, \ldots, u_6\}$ in the poset diagram shown as Fig.2. According to Eq.(1), the CA can construct the public ECP for each user. Here, we suppose the ECP of user u_1 is 0, and then we can obtain

$$\begin{aligned}
u_1 &: E_1(x) = 0 \bmod p,\\
u_2 &: E_2(x) = [x - f(n_1G_2)] + k_2 \bmod p,\\
u_3 &: E_3(x) = [x - f(n_1G_3)] + k_3 \bmod p,\\
u_4 &: E_4(x) = [x - f(n_1G_4)][x - f(n_2G_4)] + k_4 \bmod p,\\
u_5 &: E_5(x) = [x - f(n_2G_5)][x - f(n_3G_5)] + k_5 \bmod p,\\
u_6 &: E_6(x) = [x - f(n_1G_6)][x - f(n_3G_6)] + k_6 \bmod p.
\end{aligned}$$

Retrieval of Secret Key Assume that $SC_i \leq SC_j$, i.e., the predecessor SC_j can recover the secret keys k_i by using their secret code n_j. However, users in the lower class SC_i cannot access the secret key k_j of users in the upper class SC_j. Here, SC_j calculates k_i by the following steps,

Step 1 A user in the upper class SC_j uses his secret code n_j, he can compute $n_jG_i = (x_j, y_j)$.

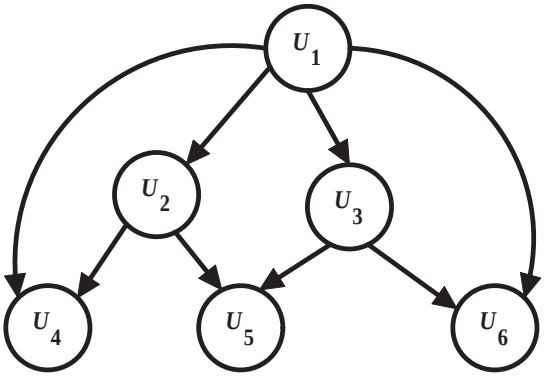

Figure 2: Dynamic access control system for six users.

Step 2 Calculate $f(n_jG_i) = x_j \oplus y_j$.

Step 3 Substitute $f(n_jG_i)$ into the Eq.(1) to obtain the secret key k_i.

For example, in the $SC_4 \leq SC_2$ poset user hierarchy shown in Fig.2, user u_2 in the upper class uses his secret code n_2 in accordance with the ECP secret key retrieval method to discover the secret key k_4 of user u_4.

2.3 Inserting new security class

Apply the above structure to the dynamic access control scheme, we suppose that a new security class SC_a is inserted into the hierarchy such that $SC_i \leq SC_a \leq SC_j$. CA will do the following process to update the partial relationship to manage the accessing priority when SC_a joins the hierarchy.

Step 1 The CA randomly selects user's secret code n_a and the secret key k_a both of which are prime. He sends n_a and k_a to user u_a by a secure channel.

Step 2 The CA adds $E_a(x)$ to the $SC_a \leq SC_j$ poset with

$$E_a(x) \quad = \quad \prod_j [x - f(n_jG_a)] + k_a \bmod p.$$

where $\prod_j$ is performed for all j satisfying $SC_a \leq SC_j$ and $j \neq a$.

Step 3 Determine the public polynomial $E_i^{'}(x)$ by the following equation,

$$E_i^{'}(x) \quad = \quad \{\prod_j [x - f(n_jG_i)]\}[x - f(n_aG_i)] + k_i^{'} \bmod p, \tag{2}$$

where $\prod_j$ is performed identical to Eq.(1) and for each SC_i such that $SC_i \leq SC_a$.

Example 3: It assumes that a new security class SC_7 is inserted into the user hierarchy such that $SC_6 \leq SC_7 \leq SC_1$ in Fig.3. Afterward CA will generate the information n_7, k_7, G_7, $E_7(x)$, and $E_6^{'}(x)$ by using the following steps,

Step 1: Randomly selects two primes n_7, k_7 and the base point $G_7 \in E_p(a,b)$ for user U_7.

Step 2: Calculate $E_6^{'}(x)$ and $E_7(x)$ such that

$$E_7(x) = [x - f(n_1 G_7)] + k_7 \bmod p, \quad (3)$$

$$E_6^{'}(x) = (x - f(n_1 G_6))(x - f(n_3 G_6))(x - f(n_7 G_6)) + k_6^{'} \bmod p. \quad (4)$$

Step 3: Use the $E_6^{'}(x)$ to replace $E_6(x)$ as the public polynomial.

Finally, CA transmits n_7 and k_7 to user u_7 via a secret channel and announces G_7, $E_7(x)$, and $E_6^{'}(x)$.

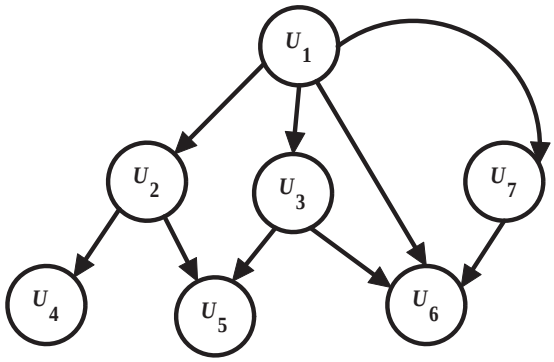

Figure 3: The consequent poset after inserting U_7.

2.4 Adding Ordered Relationships

Suppose a new ordered relationship $SC_i \leq SC_b \leq SC_a \leq SC_j$ to replace the original relationship $SC_i \leq SC_a \leq SC_j$. CA will do the following process to setup this new ordered relationship $SC_i \leq SC_b \leq SC_a \leq SC_j$.

Step 1 When $SC_b \leq SC_a$ is added to the original relationship $SC_a \leq SC_j$, the CA needs to modify the public polynomial $E_b(x)$ of SC_b to $E_b^{'}(x)$ as follows:

$$E_b^{'}(x) = \{\prod_j [x - f(n_j G_b)]\}[x - f(n_a G_b)] + k_b^{'} \bmod p.$$

where $\prod_j$ is performed identical to the original $E_b(x)$.

Step 2 The CA also use the following polynomial $E_i^{'}(x)$ to replace the original public polynomial $E_i(x)$ such that the new relationship $SC_i \leq SC_b \leq SC_a$.

$$E_i^{'}(x) = \{\prod_j [x - f(n_j G_i)]\}[x - f(n_a G_i)] + k_i^{'} \bmod p.$$

where $\prod_j$ is performed identical to the original $E_i(x)$.

Example 4: We assume that there is a new ordered relationship $SC_5 \leq SC_7$ is added and the new hierarchy structure is shown as Fig.4. Therefore, CA will reconstruct a new $E_5^{'}$ as follows:

$$E_5^{'}(x) = [(x - f(n_2 G_5))(x - f(n_3 G_5))](x - f(n_7 G_5)) + k_5^{'} \bmod p. \quad (5)$$

Then, CA transmits $k_5^{'}$ to user u_5 via a secret channel and publishes $E_5^{'}$ and G_5.

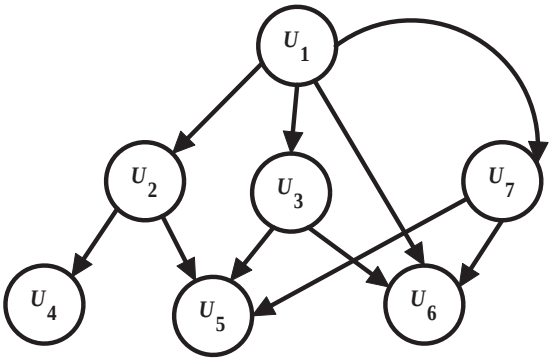

Figure 4: Adding a relationship between U_7 and U_5.

2.5 Deleting Relationships

Suppose, in an ordered relationship $SC_i \leq SC_b \leq SC_a \leq SC_j$ system, the $SC_b \leq SC_a$ poset will be deleted. Then, CA will do the following process to delete this relationship.

Step 1 From the original $SC_b \leq SC_a \leq SC_j$ ordered relationship, delete the $SC_b \leq SC_a$ relationship, forming an $SC_a \leq SC_j$. The $E_b(x)$ polynomial in SC_b will be changed to $E_b^{'}(x)$ as follows:

$$E_b^{'}(x) = \prod_j [x - f(n_j G_b^{'})] + k_b^{'} \bmod p.$$

where $\prod_j$ is performed for all j such that $SC_b \leq SC_j$ and $j \neq b$ after the deletion.

Step 2 From the original $SC_i \leq SC_b \leq SC_a$ ordered relationship, delete the $SC_b \leq SC_a$ relationship, forming an $SC_i \leq SC_b$. The $E_i(x)$ polynomial in SC_ib will be changed to $E_i^{'}(x)$ as follows:

$$E_i^{'}(x) = \prod_j [x - f(n_j G_i^{'})] + k_i^{'} \bmod p.$$

where $\prod_j$ is performed for all j such that $SC_i \leq SC_j$ and $j \neq b$ after the deletion.

Example 5: We assume that there is an ordered relationship $SC_6 \leq SC_3$ in Fig.4 is deleted and the new hierarchy structure is shown as Fig.5. Therefore, CA needs to reconstruct a new ECP:$E_6^{'}$ of user u_6 as follows:

$$E_6^{'}(x) = [(x - f(n_1 G_6^{'}))(x - f(n_7 G_6^{'}))] + k_6^{'} \bmod p. \quad (6)$$

Then, CA transmits $k_6^{'}$ and $G_6^{'}$ to user u_6 via a secret channel and publishes $E_6^{'}$ and $G_6^{'}$.

2.6 The security analysis and Discussion

In [14], Wen *et al.* discuss the security of WWC-scheme from two parts, the secret code and the secret key.

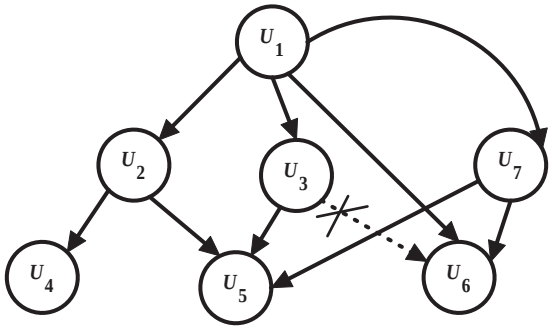

Figure 5: Deleting a relationship between U_3 and U_6.

2.6.1 Secret analysis for secret code

In this subsection, they proposed the following five attacks such as contrary attack, interior collecting attack, interior mutual attack, exterior attack and collaborative attack to analyze the security of WWC-scheme. Now, we take the collaborative attack for an example.

Collaborative attack: It is defined as m successors have a common predecessor and they collaboratively want to obtain the secret code of their predecessor in WWC-scheme. In this attack, for convenience, u_2 and u_3 have the common predecessor u_1 and they collaboratively attempt to obtain the secret code n_1 in Fig.6. The ECP's of u_2 and u_2 are generated as following,

$$E_2(x) = [x - f(n_1G_2)] + k_2 \bmod p, \quad (7)$$
$$E_3(x) = [x - f(n_1G_3)] + k_3 \bmod p. \quad (8)$$

By setting $x = 0$ in the Eqs.(7) and (8), we can obtain Eqs.(9) and (10).

$$e_1 = [k_2 - E_2(0)] = f(n_1G_2) \bmod p, \quad (9)$$
$$e_2 = [k_3 - E_3(0)] = f(n_1G_3) \bmod p. \quad (10)$$

With collaboration, users u_2 and u_3 can discover e_1 and e_2 through the known values k_2, k_3, $E_2(0)$ and $E_3(0)$. Obviously, it is very difficult to determine n_1 from both Eqs.(9) and (10) based on the known values e_1, e_2, G_2 and G_3. Therefore, Wen *et al.* claim that WWC-scheme provides qualified secure tolerance for resisting the above attacks on secret code.

2.6.2 Secret analysis for the secret key

For the secret key attacks, there possible attacks such as exterior attack, sibling attack, and ordered relationship changing attack are discussed in [14]. Here, we will roughly review the exterior attack was proposed by Wen *et al.* in 2007. For a more detailed discussion on other attacks, the reader can refer to [14].

Exterior attack: It is defined as an unauthorized user w wishes to access the secret key k_i of some user u_i in the WWC-scheme through the related public information. Wen *et al.* pointed out two possible ways to acquire k_i when user w is not a member of this hierarchy.

- The illegal user w recovers the secret key k_i directly from the ECP. The ECP of u_i is generated as Eq.(1). Hence, the illegal user w can only obtain k_i by substituting $x = 0$ into

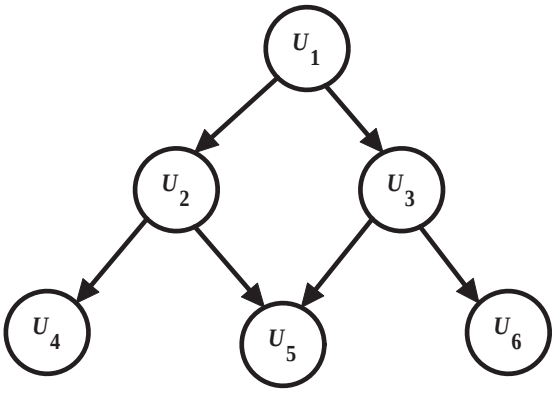

Figure 6: Dynamic access control system for six users.

Eq.(1), i.e.,

$$E_i(x) \quad = \quad \prod_j [-f(n_j G_i)] + k_i \bmod p. \tag{11}$$

Obviously, it is infeasible for the illegal user w to obtain k_i without knowing the values $f(n_j G_i)$ for all considered j.

- The illegal user w collects the secret code $n_{j'}$ of some predecessor of u_i and then computes $E_i(f(n_{j'} G_i))$ to obtain k_i. Obviously, this issue is similar to the Way 1. In other words, it is also infeasible to obtain k_i without knowing the values $f(n_{j'} G_i)$ for all considered j. Hence, the security of WWC-scheme about the exterior attack on secret key is guaranteed[14].

Finally, Wen *et al.* concluded that the WWC-scheme is practical after they analyze the security of secret keys and secret codes by using the possible attack such as contrary attack, interior collecting attack, interior mutual attack, exterior attack and collaborative attack, exterior attack, sibling attack, and ordered relationship changing attack.

3 On the security of WWC-Scheme

However, the WWC-scheme still cannot resist another case of the exterior attack which is not discussed in [14]. Before we introducing this novel exterior attack, we must review the result of product $(X - r_1)(X - r_2) \cdots (X - r_n)$ by the following theorem:
Theorem 1[4] The product $(X - r_1)(X - r_2) \cdots (X - r_n)$ can be expanded as follows.

$$(X - r_1)(X - r_2) \cdots (X - r_n) = \sum_{0 \le k \le n} (-1)^k s_k X^{n-k}, \tag{12}$$

where

$$s_k = s_k(r_1, r_2, \ldots, r_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} r_{i_1} r_{i_2} \cdots r_{i_k}.$$

For instance, $s_0 = 1$, $s_1 = r_1 + r_2 + \cdots + r_n$, $s_2 = \sum_{1 \le i < j \le n} r_i r_j$ and $s_n = r_1 r_2 \cdots r_n$.

3.1 The Novel Exterior Attack

In this section, we will define the modified exterior attack as following,

Dynamic Exterior Attack: an illegal user w wishes to access the secret key k_i of some user u_i through the related public information when a new class joins this hierarchy or a new ordered relationship is setup.

Consider the example shown in Fig.7. The public ECP of user u_6 is formed $E_6(x) = [(x - f(n_1G_6))(x - f(n_3G_6))] + k_6 \bmod p$ before user u_7 joins the hierarchy. After u_7 joins the hierarchy, the public polynomials $E_6^{'}(x)$ and $E_7(x)$ is defined as the Eqs.(3) and (4).

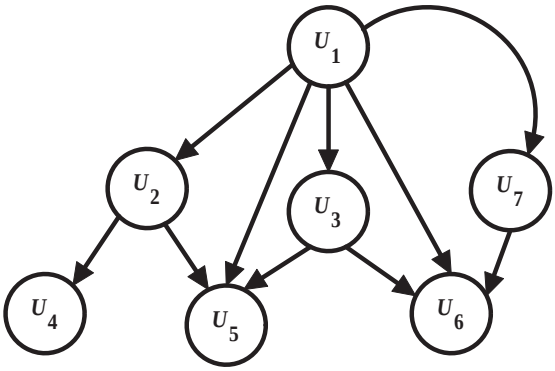

Figure 7: The consequent poset after inserting U_7

In fact, anyone can obtain the public information $E_6(x)$ before the new class SC_7 joins and also obtain $E_6^{'}(x)$ after he joins this scheme, respectively. Therefore, anyone can discover the secret key $k_6^{'}$ from the public information $E_6(x)$ and $E_6^{'}(x)$ by the following equations.

$$E_6(x) = [(x - f(n_1G_6))(x - f(n_3G_6))] + k_6 \bmod p \tag{13}$$

$$E_6^{'}(x) \quad = \quad (x - f(n_1G_6))(x - f(n_3G_6))(x - f(n_7G_6)) + k_6^{'} \bmod p. \tag{14}$$

Therefore, from the Eqs.(13) and (14), we can find out the coefficient a of x in $E_6(x)$ is $-(f(n_1G_6) + f(n_3G_6)) \bmod p$ and the coefficient b of x^2 in $-(f(n_1G_6) + f(n_3G_6) + f(n_7G_6)) \bmod p$, respectively. Therefore, we can recover the information $f(n_7G_6)$ by $a - b \bmod p$. Furthermore, we can find out the secret key $k_6^{'}$ from Eq.(14). Hence, this proposed scheme is insecure when a new class joins this hierarchy.

3.2 On the Security of Adding Ordered Relationships in WWC-scheme

Similarly, the attacker can get the public information $E_5(x)$ before the new ordered relationship $SC_5 \leq SC_7$ is added. In order to explain the novel exterior attack when adding ordered relationships in WWC-scheme, we redraw the poset diagram as following figure.

In Fig.8, the attacker w_a can find out the public information $E_5(x)$ from Eq.(15) before the new ordered relationship $SC_5 \leq SC_7$ is added.

$$E_5(x) = (x - f(n_2G_5))(x - f(n_3G_5)) + k_5 \bmod p. \tag{15}$$

The attacker w_a also obtains this public information $E_5^{'}(x)$ after this new hierarchy, including this ordered relationship $SC_5 \leq SC_7$, is setup.

$$E_5^{'}(x) \quad = \quad (x - f(n_2G_5))(x - f(n_3G_5))(x - f(n_7G_5)) + k_5^{'} \bmod p. \tag{16}$$

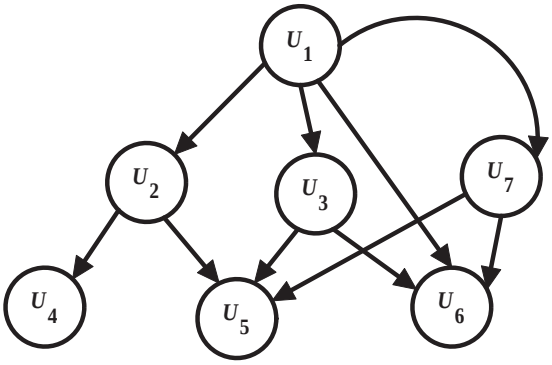

Figure 8: Adding a relationship between user U_7 and U_5 to the hierarchy.

By dynamic exterior attack, the attacker w_a can easily obtain $f(n_7G_5) = a_1 - b_1$. Where $a_1(= -(f(n_2G_5) + f(n_3G_5)) \bmod p)$ is the coefficient of x in Eq.(15) and $b_1(= -(f(n_2G_5) + f(n_3G_5)+f(n_7G_5)) \bmod p)$ is the coefficient of x^2 in Eq.(16), respectively. Therefore, it is feasible for the attacker w_1 to obtain the secret key $k_5^{'}$ with knowing the value $f(n_7G_5)$. As a result, the security for the dynamic exterior attack on secret key is not guaranteed in WWC-scheme[14].

4 Conclusions

In this paper, we have shown that an illegal user can find out the secret key when a new class joins or a new ordered relationship is added into the WWC-scheme. In other words, the security

Acknowledgments

This work was supported by National Science Council NSC 97-2221-E-150-038.

References

[1] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," ACM Transactions on Computer System, Vol.3, No.1, pp.239-247, 1983.
[2] T. S. Chen and J. Y. Huang, "A novel key management scheme for dynamic access control in a user hierarchy," Applied Mathematics and Computation, Vol.162, No.1(4), pp.339-351, March 2005.
[3] D. E. Denning, "Cryptographic and Data Security," Addison-Wesley, pp.39-48, 1982.
[4] P. Grillet, Algebra, John Wiley & Sons, Inc., 1999.
[5] M. S. Hwang, "An Improvement of Novel Cryptographic Key Assignment Scheme for Dynamic Access Control in a Hierarchy," IEICE Trans. Funda., Vol.E82-A, No.3, pp.548-550, Oct. 1999.
[6] G. B. Horng, C. L. Liu and Y. T. Hwang, "Security Analysis of a Threshold Access Control Scheme Based on Smart Cards," IEICE Trans. Funda., Vol.E87-A, No.8, pp.2177-2179, Aug. 2004.
[7] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, Vol.48, pp.203-209, 1987.
[8] Alan G. Konheim, Computer Security and Cryptography, John Wiley & Sons, Inc., 2007.
[9] V. Miller, "Uses of Elliptic Curves in Cryptography," In Advances in Cryptology (CRYPTO 85), Springer Verlag LNCS 218, pp.417-426, 1985.
[10] M. O. Rabin, "Digitalized Signatures and Public-Key Function as Intractable as Factorization," Technical Report, Computer Science, MIT/LCS/TR-212, MIT Lab., Vol.1, pp.100-123, 1979.
[11] Victor R. L. Shen, T. S. Chen and F. Lai, "Novel Cryptographic Key Assignment Scheme for Dynamic Access Control in a Hierarchy," IEICE Trans. Funda., Vol.E80-A, No.10, pp.2035-2037, Oct. 1997.
[12] William Stallings, "Cryptography and network security Principles and Practices," 4th version, Pearson Education, Inc., 2006.

[13] W. G. Tzeng, ”A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy,” IEEE Trans. on Knowledge and Data Engineering, Vol.14, No.1, pp.182-188, 2002.
[14] J. H. Wen, M. C. Wu, and T. S. Chen, ”A Novel Elliptic Curve Dynamic Access Control System,” IEICE Trans. Commun., Vol.E90-B, No.8, pp.1979-1987, 2007.
[15] K. P. Wu, S. J. Ruan, C. K. Tseng, and F. Lai, ”Hierarchical access control using the secure filter,” IEICE Trans. Information & System, Vol.E84-D, No.6, pp.700-708, June 2001. International Journal of Security and Its Applications Vol. 3, No. 2, April, 2009