An Improvement of a Dynamic Cryptographic Key Assignment Scheme in a Tree Hierarchy *

Min-Shiang Hwang

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, TAIWAN 413, R.O.C.
Email: mshwang@mail.cyt.edu.tw
Fax: 886-4-3742337

September 14, 2001

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC87-2218-E-324-001.
Abstract

This paper shows how several security classes in Liaw-Wang-Lei’s cryptographic key assignment scheme can collaborate to derive the secret key of their immediate ancestor in some cases. We also propose two schemes which are a slight modification of the proposed scheme to enhance the level of security.

Keywords: Access control, cryptography, data security, multilevel

1 Introduction

Recently, Liaw, Wang, and Lei [1] proposed an efficient cryptographic key assignment scheme for solving the access control problem in a tree structure. Basically, the scheme is based on Newton’s interpolating method and a one-way function. The scheme not only achieve dynamic key assignment, but also are simple and efficient for generating and derivating keys. However, we show that several security classes can collaborate to derive the secret key of their immediate ancestor in this article. We also propose two schemes for modifying the Liaw-Wang-Lei’s scheme slightly so that the security will be greatly improved.

2 The Weakness of Liaw-Wang-Lei’s Scheme

Recently, Liaw, Wang, and Lei proposed an efficient dynamic cryptographic key assignment scheme, which was based on Newton’s interpolating method and a one-way function, for solving the access control problem in a hierarchy.

In the subject paper [1], the authors assigned each security class $C_i$ an associated distinct pair $(t_{1i}, t_{2i})$ as the public parameter and a secret key $K_i$. Assume that the security class $C_i$ has $d$ immediate successors $C_{i_1}, C_{i_2}, \cdots, C_{i_d}$.
The security class $C_i$ constructs an interpolating polynomial $NP_i(x)$ of degree $d$ by interpolating on the points $(0, K_i), (t_{1i}, t_{2i}), 1 \leq j \leq d$, over $GF(P)$, where $P$ denotes a large prime number. Let $NP(x) = (\alpha_d(x - x_{d-1})(x - x_{d-2}) \cdots (x - x_0) + \cdots + \alpha_1(x - x_0) + \alpha_0) \mod P$, where $(\alpha_0, x_0) = (0, K_i)$, and $(\alpha_j, x_j) = (t_{1i}, t_{2i}), 1 \leq j \leq d$. The secret key $K_{ij}$ of $C_{ij}$ is calculated by his immediate ancestor $C_i$, $K_{ij} = F(NP_i(t_{2i})) \mod P$, for $j = 1, 2, \cdots, d$, where $F$ denotes a pseudo one way function, $F(X) = X^2 + 1 \mod P$. The pairs of public parameters $(t_{1i}, t_{2i}), P$, and $F$ are known to all security classes in the scheme. The security class $C_i$ keeps only its own key $K_i$ secret.

To derive $K_{ij}$ of $C_{ij}$, the security class $C_i$ reconstructs the interpolating polynomial $NP_i(x)$ by interpolating on the points $(0, K_i), (t_{1i}, t_{2i}), (t_{1i}, t_{2i}), \cdots, (t_{1i}, t_{2i})$. The secret key $K_{ij}$ is thus obtained by computing $F(NP_i(t_{2i})) \mod P$, where $t_{2i}$ is the public key of $C_{ij}$.

The weakness in the security of Liaw-Wang-Lei’s scheme is as follows. Let $C_{ij}, 1 \leq j \leq d$, be $d$ immediate successors of the security class $C_i$. Since the points $(t_{1i}, t_{2i})$ for $C_{ij}, j = 1, \cdots, d$, are known to each security class, we can construct an interpolating polynomial $NP_i(x)$ with one unknown point $(0, K_i)$ and $d$ known points $(t_{1i}, t_{2i}), j = 1, \cdots, d$. The formula is as follows.

$$NP_i(x) = (\alpha_d(x - x_{d-1})(x - x_{d-2}) \cdots (x - x_0) + \cdots + \alpha_1(x - x_0) + \alpha_0) \mod P,$$

$$= e_1 + e_2 K_i \mod P,$$

where $(\alpha_0, x_0) = (0, K_i), (\alpha_j, x_j) = (t_{1i}, t_{2i}), 1 \leq j \leq d$, and $e_1, e_2$ are constants. Next, we take the polynomial $NP_i(t_{2i})$ in Equation (1) as a parameter of $F$. Since $F$ is a one-way function of degree $d$, we have

$$F(NP_i(t_{2i})) = K_{ij},$$

$$= (e_{jd} K_i^d + e_{jd-1} K_i^{d-1} + \cdots + e_{j1} K_i + e_{j0}) \mod P,$$ for $j = 1, 2, \cdots, d$. 

2
By Gauss’s elimination method [2], there are a unique solution for \( d \) equations with \( d \) variables. Therefore, \( d \) immediate successors of security class \( C_i \) can collaborate to derive the secret key \( K_i \) of \( C_i \). In fact, only one security class is needed to break the scheme when the one-way function is in Quadratic Residuosity modulo (i.e., \( F(X) = e_2X^2 + e_1X + e_0 \mod P \)) [3]. When the one-way function is a polynomial of degree \( d \), only \( d-1 \) immediate successors are needed for a conspiracy attack. The following example illustrates this case.

**Example 2.1**

Suppose that there are nine security classes in the system, as shown in Figure 1. Let the prime number \( P = 13 \) and the one-way function \( F(X) = X^2 + 1 \mod 13 \). Under the proposed scheme, the secret key \( K_i \) and public parameters \((t_{1i}, t_{2i})\) for each security class \( C_{ij} \) are as shown in Table 1. The following steps will show how \( C_4 \) and \( C_5 \) can collaborate to derive the secret key of \( C_1 \).

1. Construct an interpolating polynomial of \( C_1 \) with one unknown variable \( K_1 \). So we have

\[
NP_1(x) = 2(x - 8)(x - K_1) + (x - K_1) \mod 13.
\]

2. Substitute the public parameters \((t_{214}, t_{215})\) of \( C_4 \) and \( C_5 \) into Equation (2), respectively,

\[
NP_1(t_{214}) = NP_1(8) = 8 - K_1 \mod 13,
\]

\[
NP_1(t_{215}) = NP_1(3) = 12 + 9K_1 \mod 13.
\]

3. Substitute \( NP_1(t_{214}) \) and \( NP_1(t_{215}) \) into the one-way function \((F(X) = X^2 + 1 \mod 13)\) with the secret keys \((K_4, K_5)\) of \( C_4 \) and \( C_5 \), respectively. Thus,

\[
11 = (8 - K_1)^2 + 1 \mod 13,
\]
\[ = (K_1^2 + 10K_1) \mod 13, \quad (4) \]

and

\[ 4 \quad = \quad (12 + 9K_1)^2 + 1 \mod 13, \]
\[ = \quad (3K_1^2 + 8K_1 + 2) \mod 13. \quad (5) \]

4. By the Gaussian elimination method, we obtain \( K_1 = 2 \) from Equation (4) and Equation (5).

In fact, either \( C_4 \) or \( C_5 \) can derive the secret key of \( C_1 \) because the one-way function is Quadratic Residuosity modulo \([3]\).

![Tree structure](image)

**Figure 1: An example of the tree structure.**

**Table 1: The keys and public parameters for each security class.**

<table>
<thead>
<tr>
<th></th>
<th>Public key pair ((t_1, t_2) = (\alpha_i, x_i))</th>
<th>Secret key (K_i = F(NP(t_2)))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(C_0)</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>(C_1)</td>
<td>(1, 4)</td>
<td>2</td>
</tr>
<tr>
<td>(C_2)</td>
<td>(2, 7)</td>
<td>5</td>
</tr>
<tr>
<td>(C_3)</td>
<td>(3, 6)</td>
<td>10</td>
</tr>
<tr>
<td>(C_4)</td>
<td>(1, 8)</td>
<td>11</td>
</tr>
<tr>
<td>(C_5)</td>
<td>(2, 3)</td>
<td>4</td>
</tr>
<tr>
<td>(C_6)</td>
<td>(1, 6)</td>
<td>4</td>
</tr>
<tr>
<td>(C_7)</td>
<td>(2, 9)</td>
<td>11</td>
</tr>
<tr>
<td>(C_8)</td>
<td>(3, 8)</td>
<td>5</td>
</tr>
</tbody>
</table>
3 Our Schemes

We have shown that Liaw-Wang-Lei’s scheme is insecure. Since the purpose of
the Newton’s interpolate polynomial is only hiding secret keys in their scheme, the
powerful and high secure one-way function is needed.

From the above discussion and example, we see that $d - 1$ security classes
can collaborate to attack the one-way function of degree $d$. We now give two
extended schemes which improve of Liaw-Wang-Lei’s scheme for withstanding
this type of attack.

**Scheme 1:** Take different prime number $P$ within Galois field $GF(P)$ to
the Newton’s interpolating polynomial and the predefined one-way function.
For example, Let $P_1$ and $P_2$ be two large but not equal prime numbers. We
can construct $NP(x) = (\alpha_d(x - x_{d-1})(x - x_{d-2})\cdots(x - x_0) + \cdots + \alpha_1(x - x_0) + \alpha_0) \mod P_1$ as Newton’s interpolating polynomial for each security class
in the system. And take $F(X) = X^2 + 1 \mod P_2$ as our predefined one-way
function.

**Scheme 2:** Choose a one-way function of degree $d + 2$, where $d$ is the maxi-
mal number of immediate successors of each security class in the whole system.

The above extended schemes not only retains the advantages of the scheme
in [1] but also enhances the security.

4 Conclusions

We have shown how several security classes in Liaw-Wang-Lei’s cryptographic
key assignment scheme can collaborate to derive the secret key of their imme-
diate ancestor in some cases. We also have proposed two extended schemes
which are a slight modification of the proposed scheme. The proposed schemes

5
not only retains the advantages of Liaw-Wang-Lei’s scheme but also enhances the security.

References

