An Improvement of Novel Cryptographic Key Assignment Scheme for Dynamic Access Control in a Hierarchy *

Min-Shiang Hwang

Department of Information Management
ChaoYang University of Technology
Wufeng, Taichung County 413, Taiwan, R.O.C.
Email: mshwang@mail.cyut.edu.tw
http://www.cyut.edu.tw/∼mshwang/

October 31, 2012

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC88-2213-E-324-002.

An Improvement of Novel Cryptographic Key Assignment Scheme for Dynamic Access Control in a Hierarchy

Abstract

This letter presents a cryptographic key assignment scheme for dynamic access control in a hierarchy. A scheme for extending a previous cryptographic key assignment scheme to reduce the computation required for key generation and derivation algorithms is also proposed.

Key words: cryptography, access control, user hierarchy,

1 Introduction

Recently, Shen, Chen, and Lai proposed a novel cryptographic key assignment scheme for dynamic access control in a hierarchy [?]. Their scheme was based on both Rabin's public key system [?] and the Chinese remainder theorem [?]. The scheme which they proposed was much simpler to implement than other cryptographic key assignment scheme for access control in a hierarchy.

Shen, Chen, and Lai stated that their scheme reduced both the computation time for key assignment and the storage size for public parameters. They also stated that with their scheme existing keys do not need to be altered while updating. In this letter, we propose a scheme which extends Shen, Chen, and Lai's scheme so that both the computation time for key assignment and the storage size for public paramenters are reduced. Our revised scheme also does not need to alter the existing keys while updating.

2 Overview of the Shen-Chen-Lai Scheme

For access control in a hierarchy, the users and their own information items are divided into a number of disjointed sets of security classes, $SC_1, SC_2, \cdots, SC_n$. Let $\leq$ be a binary partially ordered relation on the set $SC = \{SC_1, SC_2, \cdots, SC_n\}$. $SC_j \leq SC_i$ means that the users in SC_j have a security clearance lower than or equal to those in SC_i. In other words, users in SC_i can derive the secret keys in SC_j and access information held by users in SC_j, but the users in SC_j cannot access the information held by the users in SC_i.

There are two algorithms in the Shen-Chen-Lai Scheme for access control in a hierarchy: the key generation algorithm and the key derivation algorithm. The key generation algorithm is based on the Chinese remainder theorem; and the key derivation algorithm is based on Rabin's public key system.

The key generation algorithm is completed by central authority (CA), whose main role is to generate public and secret information to each security class. After the key generation algorithm, CA assigns five parameters to each security class SC_i, denoted as H_i, b_i, n_i, C_i, and ID_i. Here, H_i is secret information owned by the SC_i. $H_i = \sum(r_j||r'_j)X_j \bmod N$, where $i \neq j$ and $SC_j \leq SC_i$. The other parameters (b_i, n_i, C_i, ID_i) are public information. The paraments are defined as follows:

- r_i, r'_i, b_i are random integers for security class SC_i.
- p_i, q_i, m_i are secret parameters for SC_i. Here, $p_i = r_i \times 2^{b_i} + 1$, $q_i = r'_i \times 2^{b_i} - 1$, and $m_i = p_i \times q_i$.
- $n_i, i = 1, \cdots n$, are random pairwise coprime integers.
- $K_i, i = 1, \cdots n$, are random integers as secret key of SC_i.
- ID_i is a specific identity code of SC_i.

- $M_i, i = 1, \cdots n$, are concatenate the K_i with its identity code ID_i and let $1 \leq M_i \leq m_i$.

- C_i is a ciphertext which enciphers a plaintext (M_i) in the encryption procedure of Rabin's scheme. In other words, $C_i = M_i(M_i + b_i) \bmod m_i$.

- $N = \prod_{i=1}^{n} n_i$.

- $X_j = y_i\ (N/n_i)$, where y_i satisfies $y_i(N/n_i) \bmod n_i = 1$.

From the key derivation algorithm of Shen, Chen, and Lai's scheme, any successor SC_j's secret key K_j be derived from SC_i with the decryption procedure from Rabin's scheme. If $SC_j \leq SC_i$ and SC_i wants to derive the secret key of SC_j, SC_i can use the secret information (H_i) owned by himself. SC_i obtains $(r_j||r'_j)$ by computing $H_i \bmod n_j$. Then M_j is obtained by computing $(-b_j/2)+((-b_j/2)^2+C_j)^{1/2} \bmod p_j$, $(-b_j/2)+((-b_j/2)^2+C_j)^{1/2} \bmod q_j$, where p_j and q_j is equal to $r_j 2^{b_j}+1$ and $r'_j 2^{b_j}-1$, respectively. Since $K_j = M_j - ID_j$, SC_i thus obtains the secret key K_j.

In the previous work [?], the authors used Rabin's scheme to hide the secret key K_i. In the next section, we improve Shen, Chen, and Lai's scheme to reduce the computation time for key assignment and storage space for public paramenters. The security and the ability of dynamic access control in this new scheme is the same as that of the Shen-Chen-Lai scheme.

3 The Improved Scheme

Shen, Chen, and Lai used Rabin's scheme to hide the secret key K_i. Since the main function of Rabin's scheme in Shen-Chen-Lai's scheme is only to camouflage the secret information, we can instead use the execute-or operation to perform the same function.

To reduce the computation time and storage space, we propose an extended scheme which is a modification of Shen, Chen, and Lai's scheme. Here, we let K_i denote a secret key of SC_i. The improved scheme is stated as follows.

1. Randomly select $n_i, i = 1, \cdots, n$, and compute $N = \prod_{i=1}^{n} n_i$. This step is same as steps 1, 2, and 3 of Shen-Chen-Lai's scheme.

2. Randomly select a positive integer r_i for security class SC_i.

3. Randomly select an integer as secret key (K_i) of SC_i.

4. Compute $w_i = r_i \oplus K_i$.

5. Choose y_i such that $y_i(N/n_i) \bmod n_i = 1$ for all $i = 1, \cdots, n$.

6. Take any security class SC_i from the hierarchy by bottom-up traversal.

7. If SC_i is a set of leaf security classes, $H_i = 0$.

8. If SC_i is not a set of leaf security classes, compute $H_i = \sum(H_j + r_j y_j(N/n_j) \bmod N$ for all SC_j which are the immediate successors of SC_i.

After the above steps, each security class $(SC_i, i = 1, \cdots, n)$ has three paramenters: (H_i, w_i, n_i). H_i is a secret parameter, and w_i and n_i are public parameters.

By using SC_i successors' public parameters, SC_i can derive any successor SC_j's secret key K_j as follows.

$$r_j = H_i \bmod n_j. \tag{1}$$

By one execute-or operation, SC_i obtains the secret key K_j as follows.

$$K_j = r_j \oplus w_j. \tag{2}$$

We compare the computations in the key assignment algorithm of our scheme with that of Shen-Chen-Lai's scheme. Our scheme requires only one additional execute-or operation above the Shen-Chen-Lai scheme. However, our scheme need not to compute p_i, q_i, m_i, and C_i as in the Shen-Chen-Lai's scheme, as stated in Section 2 above. The computational time in key assignment algorithm of this new extended scheme is thus found to be less than that of the Shen-Chen-Lai scheme.

Next, we compare the computations in the key derivation algorithm of our scheme with those in the Shen-Chen-Lai scheme. Our scheme only requires a single computation of Equation (1) and a single computation of Equation (2). However, Shen-Chen-Lai's scheme requires a single computation of Equation (1) and four computations each of p_i, q_i, M_j, and K_j, as stated in Section 2. Thus the computational time in key derivation algorithm of this new revised scheme is found to be less than that of the Shen-Chen-Lai scheme.

The storage space of our scheme is only required for three parameters: (H_i, w_i, n_i). However, Shen-Chen-Lai's scheme requires storage for five parameters: $(H_i, b_i, n_i, C_i, ID_i)$. Obviously, the storage space required by our scheme is less than that of the Shen-Chen-Lai scheme.

In terms of security analyses, the secret key of SC_i in our scheme is derived by using H_i and by decomposing execute-or operation ($K_i = r_i \oplus w_i$). Since H_i and r_i are secret information and an illegal user only has the public information w_i and n_i, he cannot derive the secret key and H_i. In addition, two or more security classes SC_j, $SC_j \not\geq SC_i$ cannot collaborate to derive SC_i's secret key.

Our scheme also can function dynamically, which is similar to the Shen-Chen-Lai scheme. The revised scheme not only retains all the advantages of Shen, Chen, and Lai's original proposal, but also reduces the computation time for key assignment and key derivation, and downsizes the storage space for public parameters.

4 Conclusions

It is shown here that Shen, Chen, and Lai's scheme required a large computation time to generate and derive keys. A revised scheme which is a slight modification of the Shen-Chen-Lai scheme is proposed. This scheme also can function dynamically in the same manner as that the Shen-Chen-Lai scheme.

Acknowledgements

The author wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC88-2213-E-324-002.