An Extension of CHW Cryptographic Key Assignment Scheme 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.

Abstract

In this article, we propose an extension of Chang-Hwang-Wu's cryptographic key assignment scheme in a hierarchy. Our scheme can defend against attacks using Tan-Gu-Zhu's methods.

Indexing terms: Cryptography, Security.

Introduction: In [1], the authors proposed an efficient cryptographic key assignment scheme (named, the CHW scheme) for solving the access control problem in a hierarchy. This scheme is based upon Newton's interpolating method and a predefined one-way function. This scheme not only reduces the amount of storage space required for storing public parameters, but is also simple and efficient in generating and deriving keys.

In [2], the authors demonstrated that in some security situations, classes can collaborate to derive the secret key of their immediate ancestor in the CHW scheme. The authors also provided two modifications to slightly modify the CHW scheme so that the security would be greatly improved.

Recently, Tan-Gu-Zhu [3] proposed two counter-examples to show that the CHW scheme and the second modified version in [2] are insecure. In this article, we propose an extension of the CHW scheme which can defend against attacks using Tan-Gu-Zhu's methods.

A review of the CHW scheme and Tan-Gu-Zhu's cryptoanalysis: In [1], the authors assumed that there is a central authority (CA) in the system that is responsible for generating and distributing keys. They assigned each security class, C_i, an associated distinct pair $(p1_i, p2_i)$ as the public parameter. Assume that the security class C_i has k immediate successors $C_{i1}, C_{i2}, \cdots, C_{ik}$. The security class C_i, using Newton's interpolation method, constructs an interpolating polynomial $H_i(x)$ of degree k by interpolating at the points

$(0, SK_i)$, $(p1_{i1}, p2_{i1})$, $(p1_{i2}, p2_{i2})$, $\cdots$, $(p1_{ik}, p2_{ik})$ over $GF(P)$. Let $H_i(x) = (SK_i + \sum_{l=1}^{k} a_l x^l) \bmod P$, where a_l is an integer between 0 and $P-1$.

This key derivation is quite similar to the original key generation. Using Newton's interpolation method, they reconstruct the interpolating polynomial $H_i(x) = (SK_i + \sum_{l=1}^{k} a_l x^l) \bmod P$ by interpolating at the points $(0, SK_i)$, $(p1_{i1}, p2_{i1})$, $(p1_{i2}, p2_{i2})$, $\cdots$, $(p1_{ik}, p2_{ik})$. The secret key of C_{il} is thus obtained from $SK_{il} = f(a_l) \bmod P$, where a_l is the coefficient of the term x^l in $H_i(x)$.

In [3], Tan-Gu-Zhu proposed two counter-measure examples to show that the CHW scheme is not secure. We briefly review the two counter-examples in the following.

1. Suppose C_i and C_j have the same k immediate successors C_{il}, $l = 1, 2, \cdots, k$. In this case, CA constructs two interpolating polynomials $H_i(x) = SK_i + \sum_{l=1}^{k} a_l x^l \bmod P$ and $H_j(x) = SK_j + \sum_{l=1}^{k} b_l x^l \bmod P$ for C_i and C_j, respectively. Since $SK_{il} = f(a_l) = SK_{jl} = f(b_l) \bmod P$, we can obtain $a_l = b_l \bmod P$. Here, SK_{il} denotes the secret key of the lth immediate successor of C_i. Consequently, $SK_i = SK_j \bmod P$.

2. Suppose C_i and C_j have m and n immediate successors in total, respectively. Both C_i and C_j have the same k immediate successors in their immediate successors, $k < m$ and $k < n$. In this case, CA constructs two interpolating polynomials $H_i(x) = SK_i + a_1 x + \cdots + a_k x^k + b_1 x^{k+1} + \cdots + b_{m-k} x^m \bmod P$ and $H_j(x) = SK_j + a_1 x + \cdots + a_k x^k + d_1 x^{k+1} + \cdots + d_{n-k} x^n \bmod P$, respectively. Since C_i knows a_l, $l = 1, 2, \cdots, k$ and $(p1_{il}, p2_{il})$, $l = 1, 2, \cdots, n$, C_i can construct $H_j(x)$ and get d_l, $l = 1, 2, \cdots, n-k$, and SK_j easily. Similarly, C_j can construct $H_i(x)$ and get SK_i easily.

An Extension Scheme: From the above statements, Tan-Gu-Zhu demonstrated that C_i can derive the secret key SK_j of C_j, when C_i and C_j have the same k, $(k > 1)$, immediate successors. We now give an extension of the CHW scheme for withstanding Tan-Gu-Zhu's attacks. The main idea is that we use a dummy security class concept in the CHW scheme. Whenever C_i has the same k immediate successors with the other security class C_j, we add k dummy security classes into the hierarchy as immediate successors of C_i. Apart from the pairs $(p1, p2)$ of those dummy security classes are keep secret, the others are the same as that of the original CHW scheme.

Assume that the security class C_i has m immediate successors and C_i has the same k immediate successors with the other security class. Using Newton's interpolation method, C_i can construct an interpolating polynomial $H_i(x)$ of degree $m+k$ by interpolating at the points $(0, SK_i)$, $(p1_{i1}, p2_{i1})$, $(p1_{i2}, p2_{i2})$, $\cdots$, $(p1_{im}, p2_{im})$, $(p1_{i(m+1)}, p2_{i(m+1)})$, $\cdots$, $(p1_{i(m+k)}, p2_{i(m+k)})$ over $GF(P)$, where $(p1_{i(m+l)},\ p2_{i(m+l)})$, $l = 1, 2, \cdots, k$, are the secret parameters of the dummy security classes. Let $H_i(x) = (SK_i + \sum_{l=1}^{k+m} a_l x^l) \bmod P$, where a_l is an integer between 0 and $P - 1$. The secret key SK_{il} of the lth immediate successor of C_i is calculated using $SK_{il} = f(a_l) \bmod P$, for $l = 1, 2, \cdots, m$, where a_l is the coefficient of the term x^l in $H_i(x)$; and $f(\cdot)$ is a one-way function of degree $m + 2$ where m is a maximal number of immediate successors of each security class in the whole system.

Since the first counter-example in [3] is a special case of the second counter-example in [3], we explain how our extension scheme can withstand the second attack of Tan-Gu-Zhu's methods. Suppose C_i and C_j have m and n immediate successors, respectively, and C_i and C_j have the same k immediate successors, $k < m$ and $k < n$. In this case, CA constructs two interpolating polynomials $H_i(x) = SK_i + a_1 x + \cdots + a_k x^k + b_1 x^{k+1} + \cdots + b_{m-k} x^m + r_1 x^{m+1} + \cdots + r_k x^{m+k} \bmod P$ and $H_j(x) = SK_j + a_1 x + \cdots + a_k x^k + d_1 x^{k+1} + \cdots + d_{n-k} x^n + s_1 x^{n+1} + \cdots + s_k x^{n+k} \bmod P$, respectively. Since C_i only knows a_l, $l = 1, 2, \cdots, k$, and $(p1_{il}, p2_{il})$, $l = 1, 2, \cdots, n$, when C_i substitutes those known parameters into $H_j(x)$, we have n equations and $(n+1)$ variables. Therefore, C_i cannot construct $H_j(x)$ and get SK_j. Similarly, C_j also cannot get SK_i.

Discussion: Although this extension scheme can defend against Tan-Gu-Zhu's attack, it wastes a large amount of storage space to store the additional pairs of $(p1, p2)$ of the dummy security classes. However, the number of identical immediate successors of C_i and C_j is small in the real world. For example, many people (or employees) are only belong to a department of a company. It is a few employees are belong to two distinct departments of a company. Therefore, our extension scheme not only maintains the advantages of the proposed scheme but also enhances the security.

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.

References

[1] CHANG, C. C., HWANG, R. J., and WU, T. C.: 'Cryptographic key assignment scheme for access control in a hierarchy', *Information Systems,* 1992, **17(3)**, pp. 243-247

[2] HWANG, M. S., Yang, W. P., and CHANG, C. C.: 'Modified Chang-Hwang-Wu access control scheme', *Electronics Letters,* 1993, **29(24)**, pp. 2095-2096

[3] TAN, K. J., GU, S. J., and ZHU, H. W.: 'A study of correctness of CHW cryptographic key assignment scheme in a hierarchy', *IEE Proceedings Computers and Digital Techniques,* to be accepted.