A Secure Multicast Key Agreement Scheme

Hsing-Chung Chen, Chung-Wei Chen

A Secure Multicast Key Agreement Scheme*

Hsing-Chung Chen[1,2], Chung-Wei Chen[3]

[1]Dept. of Computer Science and Information Engineering, Asia University, Taichung City, Taiwan 41354
cdma2000@asia.edu.tw, shin8409@ma6.hinet.net
[2] Research Consultant with Dept. of Medical Research, China Medical University Hospital, China Medical University Taichung, 40402, Taiwan, R.O.C.
3Institute of Communications Engineering, National Tsing Hua University, Hsinchu City, Taiwan 30013
oliwad@gmail.com

Abstract. Wu et al. proposed a key agreement to securely deliver a group key to group members. Their scheme utilized a polynomial to deliver the group key. When membership is dynamically changed, the system refreshes the group key by sending a new polynomial. We commented that, under this situation, the Wu et al.'s scheme is vulnerable to the differential attack. This is because that these polynomials have linear relationship. We exploit a hash function and random number to solve this problem. The secure multicast key agreement (SMKA) scheme is proposed and shown in this paper which could prevent from not only the differential attack, but also subgroup key attack. The modification scheme can reinforce the robustness of the scheme.

Keywords. Cryptography; security; secure multicast; conference key; key distribution.

1 Introduction

Many security protection schemes [1-11, 14] have been developed for an individual multicast group. Some schemes address secure group communications by using secure filter [1-4] to enhance performance of the key management. Wu et al. [4] proposed a key agreement to securely deliver a group key to specific members efficiently. The system conceals the group key within a polynomial consisting of the common keys shared with the members. In the Wu et al.'s scheme, the polynomial is called as a secure filter. Through their scheme, only the legitimate group members can derive a group key generated by a central authority on a public channel. Nevertheless, for the dynamic membership, the scheme is suffered from the differential attack which we describe later. The dynamic membership means the addition and subtraction of the

* This work was supported in part by the Ministry of Science and Technology, Taiwan, Republic of China, under Grant MOST 104-2221-E-468-002. Hsing-Chung Chen (Jack Chen) is the corresponding author.

group members. Naturally, the membership changes by the reason caused by network failure or explicit membership change (application driven) [5, 6]. If an adversary collects the secure filters broadcasted among the group members, as the membership changes, the group keys sent to the group members with the secure filter will be discovered through the differential attack [11].

The secure multicast key agreement (SMKA) scheme is proposed in this paper, which is a kind of secure filter to resist against the differential attack. The proposed secure filter is based on the properties of a cryptographically secure one-way hash function. Moreover, the complexity of the modified secure filter is almost the same with the complexity of the original one.

The rest of this paper consists of the following parts. The section 2 gives an overview of the secure filter and the differential attack against the secure filter for the dynamic membership. The section 3 introduces our scheme. The section 4 gives the security proof of our scheme. Then we conclude our scheme in the section 5.

2 The secure filter and the differential attack

2.1 Wu et al.'s Scheme

In Wu et al.'s Scheme [4], assume that there is a central authority which is in charge of distributing a group key to the group members, denoted as G, where $G=[M_1,M_2,\cdots M_n]$ in which the M_i indicates i-th group member. The M_i shares a common key k_i with the central authority. As the central authority starts to send a group key s to the members in the G, the central authority computes the secure filter as follows.

$$f(x)=\prod_{i=1,k_i\in K}^{n}(x-h(k_i))+s \mod p$$

$$=\sum_{i=1}^{n}a_i x^i \mod p$$

Then the central authority broadcasts the coefficient of each item. For the M_i, upon receiving the coefficients, he can derive s by computing $f(h(k_i))$. Any adversary can not derive the s because he doesn't know any k_i, where $i=[1,2,\cdots,n]$.

2.2 A Differential Attack on Wu et al.'s Scheme

The differential attack utilizes the linear relationship of the coefficients in the secure filter to compromise the group keys. The differential attack is described as follows. Assume that an adversary, Ad, where $Ad\notin G$. The Ad collects each secure filter used to send a group key at each session which means a period of the time for the membership unchanged. Observe that the coefficients of the secure filter, we learn the relationship as follows.

$$
\begin{aligned}
a_n &= 1 \mod p, \\
a_{n-1} &= \sum_{i=1}^{C_1^n} h(x_i) \mod p, \\
a_{n-2} &= \sum_{i=1, i \neq j}^{C_2^n} h(x_i) h(x_j) \mod p, \\
&\vdots
\end{aligned}
$$

The coefficients of the secure filter are the linear relationship of the secure factors. As membership changes, the differential value of the coefficients will disclose the secure factors in the secure filter. For example, as the M_3 is excluded from the group, which may be caused by network failure, then the central authority re-computes the following secure filter to refresh the group key, where n' means the membership as the M_3 is excluded below.

$$
f'(x) = \prod_{i=1, k_i \in K, i \neq 3}^{n'} (x - h(x_i)) + s' \mod p
$$

$$
= \sum_{i=1}^{n'} a_i x^i \mod p
$$

For the coefficient $a_{n'-1}$, the adversary can compute $a_{n-1} - a_{n'-1}$ to derive $h(x_3)$. Through the $h(x_3)$, the adversary can derive the previous group keys through the preceding secure filters. Moreover, as the M_3 returns into the group, the central authority will refresh the group key through another secure filter composed of the secure factor $h(x_3)$. Then the adversary who already derives the $h(x_3)$ through the differential attack can derive any group key as long as the M_3 is in the group.

3 Our Scheme

In this section, we introduce our scheme. First, we define the environment and notation. And then we introduce our scheme. The notations used in the rest of this paper are shown in Table 1.

Table 1. Notations

CA	central authority
n	number of the group members at the session t
$h(\cdot)$	cryptographically secure one-way function
c_t	random number used at the session t
s_t	group key for the session t
M_i	i -th group member
k_i	common key only shared with the CA and the i -th user
x_i	secure factor of the modified secure factors
$f_t(x)$	modified secure filter for the session t

3.1 SMKA Scheme

The secure multicast key agreement (SMKA) scheme is proposed in this section. Assume that there are n group members at the session t. The set of these group members at the session t is denoted as G_t, where $G_t = [M_1, M_2, \cdots, M_n]$. The M_i denotes i -th group member, where $i \in [1, 2, \cdots, n]$. The set of the common keys is denoted as K_t, where $K_t = [k_1, k_2, \cdots, k_n]$. Before the CA starts to send the group key s_t for the session t to the members in the G_t, the CA generates a random number c_t. Then the CA computes the secure factors below.

$$x_i = h(k_i \| c_t), \tag{1}$$

where $k_i \in K_t$ and $i = \{1, 2, \cdots, n\}$. Next, the CA generates a group key s_t and calculates the modified secure filter below.

$$f_t(x) = \prod_{i=1}^{n}(x - x_i) + s_t \mod p. \tag{2}$$

Then the CA can derive the extension of the $f_t(x)$ as following.

$$f_t(x) = a_n x_n + a_{n-1}x_{n-1} + \cdots + a_0 \mod p. \tag{3}$$

The CA broadcasts the set of the coefficients, denoted as A, and c_t, where $A = [a_n, a_{n-1}, \cdots, a_0]$. After receiving the A and the c_t, the group member M_i compute the secure factor, x_i through the procedure of (1) with the common key k_i and c_t. Next, the M_i derive s_t by calculating $f_t(x_i) = f_t(h(k_i \| c_t))$. In the next session

$t+1$, the CA generates a new random number c_{t+1} and repeats the procedures of (1) to (3) to send the secret s_{t+1} to the G_{t+1}, where the G_{t+1} may not be the same as G_t.

4 Security and Complexity Analyses

In this section, we show that the modified secure filter can resist against the differential attack. Moreover, we proof that the modified secure filter can also prevent from the subgroup key attack [13, 14] which could compromise other common keys through factorizing algorithm [15].

Proposition 1. *A cryptographically secure hash function $h(\cdot)$ has the properties: intractability, randomness, collision-free, unpredictability.*

The proposition 1 is assumed commonly on cryptography [15]. The intractability means that, for only given a hash value y, where $y = h(x)$, the value of x is intractable. The randomness means that, for a variable x, the elements in the set of the result $y = h(x)$, denoted as Y, are uniformly distributed. The collision free means that, given y, where $y = h(x)$, the probability of discovering x', where $x \neq x'$, that $h(x)$ equals $h(x')$ is negligible. The unpredictability means that hash functions exhibit no predictable relationship or correlation between inputs and outputs.

Theorem 1. *An adversary cannot discover the group keys through the differential attack.*

Proof: Assume that an adversary can know the membership of the group exactly. He records the distinct membership at different session. For the session t, the adversary can collect the modified secure filter below.

$$f_t(x) = a_n x_n + a_{n-1} x_{n-1} + \cdots + a_0 \mod p . \tag{4}$$

The coefficient of $f_t(x)$ can be derived below.

$$a_n = \sum_{i=1}^{n} h(x_i \,\|\, c_t) \mod p, \tag{5}$$

$$a_{n-1} = \sum_{i=1, i \neq j}^{C_2^n} h(x_i \,\|\, c_t) h(x_j \,\|\, c_t) \mod p,$$

$$\vdots$$

For any session t', where $t' \neq t$, the adversary can discover another modified secure filter for different membership in which the number of group member is n' below.

$$f_{t'}(x) = a_{n'}x_{n'} + a_{n'-1}x_{n'-1} + \cdots + a_0' \mod p\,. \tag{6}$$

The coefficient of $f_{t'}(x)$ can be presented below.

$$a_{n'} = \sum_{i=1}^{n'} h(x_i \| c_{t'}) \mod p, \tag{7}$$

$$a_{n'-1} = \sum_{i=1, i\neq j}^{C_2^{n'}} h(x_i \| c_{t'})h(x_j \| c_{t'}) \mod p,$$

$$\vdots$$

According to the Proposition 1, we can learn that the coefficients in (5) and (7) are predictable for an adversary. Therefore, it induces that the adversary cannot predict the linear relationship between these coefficients. Hence, the adversary cannot engage the differential attack successfully to compromise the group key distributed within a secure filter.

□

Theorem 2. *A legitimate group member cannot discover other common keys shared between the CA and other group members.*

Proof: According to the Proposition 1, assume that a legitimate group member has enough ability to factorize the value of $f_t(0)$ and discover the other secure factors of the $f_t(x)$; he only can discover the hash values not tractable to the common keys. Therefore, the common keys cannot be discovered by the adversary. Then we prove that the modified secure filter can resist against the subgroup key attack.

According to Theorem 1 and Theorem 2, we proof that the modified secure filter can resist against the differential attack as well as the subgroup key attack [13, 14].

□

5 Conclusions

In this paper, the navel key agreement scheme by using the new secure filter to improve the robustness in order to support the security functionality on dynamically changing members in the Wu's secure filter [4]. The proposed secure filter is based on the properties of a cryptographically secure hash function. Via the security analysis, we proved that the modified secure filter can resist against the differential attack. Moreover, the modified secure filter can prevent from the subgroup key attack. The modified secure filter almost has the same complexity with the original secure filter. For a group communication, the dynamic membership is an unavoidable issue. Though the secure filter proposed in [4] gave a simple and robustness distribution scheme for the group secret, it is suffered from the problems of the dynamic membership. The modified secure filter can enhance the secure filter for the dynamic membership and keep the efficiency.

References

1. H.-C. Chen, S.-J. Wang and J.-H. Wen, "Packet Construction for Secure Conference Call Request in Ad Hoc Network Systems," *Information Sciences*, vol. 177, issue 24, pp. 5598–5610 (2007)
2. H.-C. Chen, "Secure multicast key protocol for electronic mail systems with providing perfect forward secrecy," *Security and Communication Networks*, Vol. 6, No. 1, pp. 100–107 (2013)
3. H.-C. Chen, C.-Y. Yang, H.-K. Su, C.-C. Wei and C.-C. Lee, "A Secure E-Mail Protocol Using ID-based FNS Multicast Mechanism," *Computer Science and Information Systems*, Special Issue on Mobile Collaboration Technologies and Internet Services, Volume 11, Issue 3, pp. 1091-1112 (2014)
4. K. P. Wu, S.J. Ruan, F. Lai, and C. K. Tseng, "On Key Distribution in Secure Multicasting," in *Proceedings of 25th Annual IEEE International Conference on Local Computer Networks*, pp. 208 (2000)
5. Y. Kim, A. Perrig, and G. Tsudik, "Communication-Efficient Group Key Agreement," *IEEE Transactions on Computer*, Vol. 53, No. 7, pp. 905-921 (2001)
6. Y. Kim, A. Perrig, and G. Tsudik, "Tree-Based Group Key Agreement," *ACM Transactions on Information and System Security*, Vol. 7, Issue 1, pp. 60-96 (2004)
7. A. Fekete, N. Lynch, and A. Shvartsman, "Specifying and Using a Partionable Group Communication Service," *ACM Transactions on Computer Systems*, Vol. 19, Issue 2, pp. 171-216 (2001)
8. X. Chen, G. Lenzini, S. Mauw, and J. Pang, "Design and Formal Analysis of A Group Signature Based Electronic Toll Pricing System," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 4, No. 1, pp. 55-75 (2013)
9. S. Craß, T. Dönz, G. Joskowicz, E. Kühn, and A. Marek, "Securing a Space-Based Service Architecture with Coordination-Driven Access Control," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 4, No. 1, pp. 76-97 (2013)
10. S. Malik and J.-H. Lee, "Privacy Enhancing Factors in People-Nearby Applications," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 6, No. 2, pp. 113-121 (2015)
11. A. D. Kent, L. M. Liebrock, and J. Wernicke, "Differentiating User Authentication Graphs," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 5, No. 2, pp. 24-38 (2014)
12. L. E. Moser, Y. Amir, P.M. Melliar-Smith, and D. A. Agarwal, "Extended Virtual Synchrony," in *Proceedings of the IEEE 14th International Conference on Distributed Computing Systems*, pp. 55-65 (1994)
13. J. H. Wen, M. C. Wu and T. S. Chen, "A Novel Elliptic Curve Method for Secure Multicast System," *Far East Journal of Mathematical Sciences*, vol. 28, issue 2, pp. 449-467 (2008)
14. K. P. Wu, S.J. Ruan, C. K. Tseng, and F. Lai, "Hierarchical Access Control Using the Secure Filter," *IEICE Transaction On Information & System*, Vol. E84-D, No. 6, pp. 700-708 (2001)

15. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press. (1997)