社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38 (21)
2007／7／19

グループ鍵に基づいてメッセージヘッダ長を削減した無効化鍵管理方式

大久保 佑† 佐藤 敬††

† 北九州市立大学大学院国際環境工学研究科 〒808-0135 福岡県北九州市若松区ひびきの1-1
†† 北九州市立大学国際環境工学部 〒808-0135 福岡県北九州市若松区ひびきの1-1
E-mail: ††tsatoh@env.kitakyu-u.ac.jp

あらまし 正規のユーザのみが暗号化したコンテンツを復元できるような無効化鍵管理方式として，CS法やSD法が知られている．小稿では，CS法においてグループ鍵を新たに付加して割り当てることでメッセージヘッダ長を削減する２種類の無効化鍵管理方式を提案する．最初の方式は組み合わせ論的な方式であり，２番目の方式は計算量的な仮定を利用し個人鍵のサイズを削減した方式である．提案手法の性能を評価するためにシミュレーションを行い，CS法およびSD法と比較を行った．その結果，メッセージヘッダ長の平均が提案手法とSD法で同程度になることを確認した．
キーワード 放送型暗号, 鍵管理, 無効化

Group Key Based Revocation Schemes with Shorter Message Header

Tasuku OHKUBO† and Takashi SATOH††

† Graduate School of Environmental Engineering, The University of Kitakyushu 1-1 Hibikino, Wakamatsu-ku, Kitakyushu, 8080-0135 Japan
†† Faculty of Environmental Engineering, The University of Kitakyushu 1-1 Hibikino, Wakamatsu-ku, Kitakyushu, 808-0135 Japan
E-mail: ††tsatoh@env.kitakyu-u.ac.jp

Abstract Broadcast encryption allows any legitimate users to decrypt the encryption of some content. The complete subtree scheme and the subset difference scheme are well-known broadcast encryption schemes with user revocation. In this paper, we propose two revocation scheme with shorter message header by assigning additional group keys in the CS scheme. The first scheme is a combinatorial-based scheme, and the second scheme is based on some cryptographic primitives. We also perform a simulation to evaluate the first our proposed schemes and compare them with the CS scheme and the SD scheme. The result indicates that our proposed schemes have as good performance as the SD scheme in terms of the size of the message header in the broadcast.
Key words broadcast encryption, revocation scheme

1. Introduction

With the widespread use of computers and development of the information society, TV subscription service, we can join cable TV subscription service, streaming service DVD media, satellite broadcasting and so on. In such services, contents such as music and movies are required to encrypt so that only authorized users can be decoded.

Broadcast encryption [5] allows legitimate users to decrypt the encryption of some content with their own private keys. Any non-legitimate user cannot obtain any information of the content.

Naor et al. [1] presented two broadcast encryption schemes with user revocation. These schemes are the complete subtree (CS) and subset difference (SD) scheme. Towards efficient user revocation schemes a lot of researchers consider variants of these schemes, such as Layered Subset Difference (LSD) [2]. Most broadcast encryption schemes are from information theoretic perspective, however, in some recent works (e.g., [11]) the security of broadcast encryption relies on computational assumptions.

To evaluate performance of a broadcast encryption scheme, there are at least three parameters: (1) the size of message header, (2) the size of storage at user, and (3) computational cost . The CS scheme requires less storage at user than the SD scheme, while the CS scheme requires longer message

header than the SD scheme.

The aim of this study is to explore an efficient subset cover revocation scheme with shorter message header. In this paper, we propose two revocation schemes by assigning additional group keys in the CS scheme. The first is combinatorial-based scheme, and the second relies on computational assumptions.

We also perform a simulation to evaluate the first our proposed schemes and compare them with the CS scheme and the SD scheme. The result indicates that our proposed schemes have as good performance as the SD scheme in terms of the size of the message header.

In Section 2, we give a brief explanation of the complete subtree scheme. In Section 3, we present two modified complete subtree schemes with shorter ciphertexts. In Section 4, we study their performance to make a comparison between some of existing user revocation schemes and our proposed schemes. Finally, in Section 5 we give concluding remarks.

2. Subset Cover Revocation Scheme

2.1 Framework

Broadcast encryption allows any legitimate users to decrypt broadcasting message. Naor et al. [1] presented a framework for broadcast encryption with user revocation. We refer to [1] for private-key encryption.

We review a subset-cover revocation scheme.

Let n be the total number of the users in the system. Let $\mathcal{N} = \{1, \ldots, n\}$ be the set of the users in the system. Let $\mathcal{R}$ be the set of the revoked users.

[Definition 1] We consider a collection C of subsets totally covering $\mathcal{X}$. Let the collection $\mathcal{C} = \{S_1, \ldots, S_m\}$. A cover for $\mathcal{X}$ is a subset $C' \subseteq C$ such that every element in $\mathcal{X}$ belongs to at least one member of C'.

Broadcast encryption scheme consists of three phases: setup phase, encryption phase and decryption phase.

(Setup) The center finds a cover for $\mathcal{N}$ and assigns a subset key K_i to each subset S_i in the cover.

(Encryption) At encryption time, the center chooses a session key sk to encrypt some content M and divides a set of authorized users $\mathcal{N} \setminus \mathcal{R}$ into a union of some subsets. Suppose that $\mathcal{N} \setminus \mathcal{R} = \bigcup_{i=1}^{m} S_i$. Next, The center encrypts a session key sk with each subset key and sends the following broadcast

$$[i_1, i_2, \ldots, i_l, E_{K_{i_1}}(sk), \ldots, E_{K_{i_l}}(sk), E_{sk}(M)] \ ,$$

where $E_{k_i}(sk)$ is the encryption of sk under each subset key k_i and $E_{sk}(M)$ is the encryption of M under the session key sk.

(Decryption) At decryption time, any user i in $\mathcal{N} \setminus \mathcal{R}$ extracts the session key to decrypt the corresponding message with his own private key. For any user $u \in \mathcal{R}$, user u never obtain the session key sk. A coalition consisting all members of $\mathcal{R}$ cannot decrypt it.

2.2 The Complete Subtree Scheme

Our proposed schemes are based on the complete subtree (CS) scheme. We review the CS scheme briefly.

In the CS scheme, the center constructs a complete binary tree with n leaves and assigns a random key to each node in the complete tree. User u's personal key is the set of $\log n + 1$ keys associated with the nodes along the path from root to leaf u.

Given a set $\mathcal{R}$ of revoked users, the center needs to find an appropriate cover covering all nodes in $\mathcal{N} \setminus \mathcal{R}$.

3. Proposed Schemes

In this section, we present two proposed schemes. The first scheme, referred as the Scheme I, is based on combinatorial approach, and the second, referred as the Scheme II, is based on computational approach using cryptographic primitives.

3.1 Idea

Suppose that we want to revoke user u. The CS scheme finds three partitions S_1, S_2 and S_3 covering all nodes in $\mathcal{N} \setminus \mathcal{R}$ (See Figure 1).

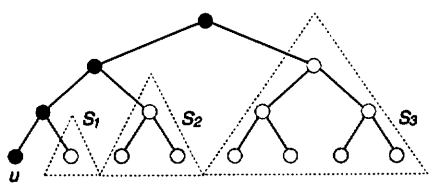

Figure 1 The complete subtree scheme

Now, we consider a group which consists of the sibling of u and the cousins of u, and assign a group key to the group. Figure 2 illustrates a simple example of how the group key improves the performance for our proposed schemes. As the sibling of u and the cousins of u share a group key, our proposed schemes requires to find two partitions. In any revocation scheme based on a subset cover less partitions implies shorter message header.

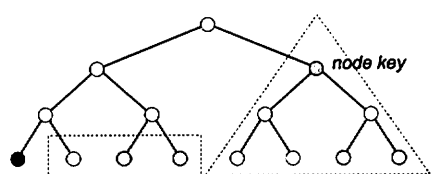

Figure 2 Group key in our proposed schemes

3.2 Scheme I

The Scheme I can be divided into three phases: setup phase, encryption phase and decryption phase.

3.2.1 Setup

During the setup phase, as in the CS scheme, the center constructs a complete binary tree with n leaves and assigns a random key (called a node key) to each node in the complete tree.

The major difference between the CS scheme and the Scheme I is assigning additional group keys. Nodes at depth $d > 1$ organize into groups of size 4. (see Fig. 3). The center

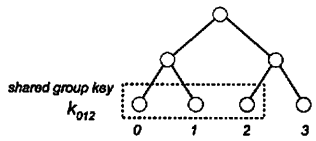

Figure 3 Group key assignment in Scheme I

assigns a random key (called a group key) to any user combination in each group. For example, k_{012} denotes the group key shared by nodes 0, 1 and 2 as shown in Fig. 3. In the Scheme I, we assign five group keys k_{02}, k_{03}, k_{012}, k_{013}, k_{023} to node 0 in the group.

User u's personal key is the set of node keys and group keys associated with the nodes along the path from root to leaf u.

3.2.2 Encryption

Encryption procedure is done in the same way as the CS scheme except use of group keys. Given a set of revoked user $\mathcal{R}$, the center runs the following encryption key search algorithm to find a subset key, referred as an encryption key later, assigned to each element of a cover for $\mathcal{N} \setminus \mathcal{R}$.

[Encryption Keys Search Algorithm]

Recall that 2^d nodes at depth d arrange into 2^{d-2} groups. Let L be a set of encryption keys. We assume that four nodes of group g are numbered 0 to 3.

(1) Let $d = \log n$ and $L = \emptyset$. Mark the nodes corresponding to the revoked users $\mathcal{R}$ as "invalid".

(2) Find the invalid nodes at depth d.

(3) Compute the set of the invalid nodes of the group. If the set is neither $\{0,1\}$ or $\{2,3\}$, then for each group key ξ in the group let $L = L \cup \{\xi\}$ and mark the parent node of the node as "invalid".

(4) Decrease d.

(5) Repeat (2) to (4) until all the nodes at some depth are invalid.

3.2.3 Decryption

At decryption, any user in $\mathcal{N} \setminus \mathcal{R}$ can recover the contents using his own personal key as in the CS scheme.

[Theorem 1] The proposed Scheme I requires $6 \log n - 4$ keys at any user and $O(\log \log n)$ operations plus a single decryption to decrypt a message.

Proof. Each node has five group keys except the the children of the root and itself. Thus, any user has $1 + \log n$ node keys and $5(-1 + \log n)$ group keys, so the total number of personal key is $6 \log n - 4$ associated with the nodes along the path from root to u. □

3.3 Scheme II

Next, we show that each user has $3 \log n - 2$ keys in the scheme II. In this scheme, we use several cryptographic primitives to reduce the size of message header. This idea is shown in [1] and [6] .

3.3.1 How to reduce the number of node keys

Let f_L and f_R be one-way trapdoor permutations over a common domain. The center publishes the one-way trapdoor permutations f_L and f_R and keeps their inverse f_L^{-1} and f_R^{-1} secret.

Let k_v be the node key assigned to node v. For each node key k_v, the center assigns

$$K_L = {f_L}^{-1}(k_v)$$
$$K_R = {f_R}^{-1}(k_v)$$

to the left child and the right child of node v as their own node keys.

The center assigns each user only one node key (terminal node key). Thus, each user can obtain all the node keys assigned to the nodes on a path from the leaf to the root applying the one-way trapdoor functions f_L and f_R.

3.3.2 How to reduce the number of group keys

Let G be a cryptographic pseudo-random bit generator that on input 1^k, outputs an ordered pair(G_L, G_R) of algorithms. $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ Let $G_L(s)$ denotes the leftmost n bits of the output of $G(s)$ and $G_R(s)$ the right most n bits of $G(S)$.

While we assign five group keys to each node in the Scheme I, we assign three group keys to each node in the Scheme II. We consider the following group key structure as depicted in Figure 4.

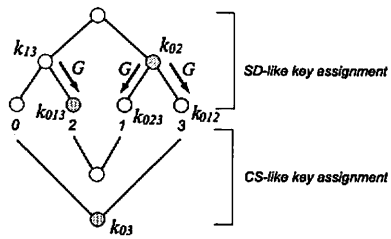

Figure 4 Group key assignment in Scheme II

We use SD-like key assignment and CS-like key assignment

in this key structure. In the SD-like key assignment, the center assigns group keys recursively. First the center assigns a random key (say, k) to the root node of the key structure. When the key of a node is k, the group key assigned to the left child of the node is $G_L(k)$ and the group key assigned to the right child of the node is $G_R(k)$. The center assigns node 0 only two group keys, k_{03} and k_{02} because node 0 can compute the other group keys k_{013}, k_{023} and k_{012} using the pseudo-random function G.

[Theorem 2] The proposed Scheme II requires $3\log n - 2$ keys at a receiver and $O(\log n)$ operations plus a single decryption to decrypt a message.

Proof. User u obtains $4+3(\log n-2) = 3\log n-2$ keys associated with the nodes along the path from root to u. Since each user has to apply the pseudo-random funtion G at most $3(\log n-2)$ times and apply one-way trapdoor permutations at most $\log n$ times to compute related group keys. □

3.4 Security

As our proposed schemes are based on a subset cover problem, we have the following theorem:

[Theorem 3] Our proposed Scheme I is secure against any revoked user coalition. Our proposed Scheme II is also secure against any revoked user coalition if there exists secure one-way trapdoor permutations and a cryptographic pseudo-random generator, where one-way trapdoor permutations require some properties (Refer to [6]).

4. Comparison

We evaluate the performance of our proposed schemes by comparing them with some existing schemes. Table 1 shows a comparison among some existing schemes and our proposed schemes. As shown in Table 1, our proposed scheme I requires $6\log n - 4$ keys, our proposed scheme I requires less personal keys than the SD scheme for $n \geqq 1024$.

Next, we fix $n = 64$ and perform simulations to evaluate the average size of the message header for our proposed scheme I , the CS scheme and the SD scheme. Figure 5 illustrates the average size of the message header for each scheme. The simulation results show that our proposed schemes have as good performance as the SD scheme in terms of the size of the message header.

5. Concluding Remarks

We have considered two new schemes for assigning additional group keys in the CS scheme. The proposed scheme I is combinatorial-based, while the proposed scheme II relies on some computational assumption. We have also evaluated our proposed schemes by comparing them with some existing schemes. The result indicates that our proposed schemes have as good performance as the SD scheme.

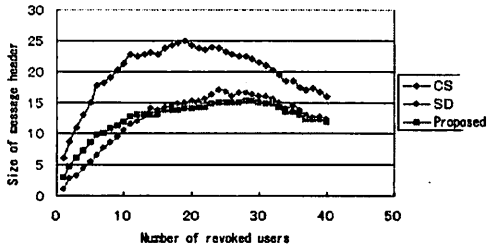

Figure 5 Comparison of message header size

Our future work is to evaluate average performance of proposed schemes for large n. In recent result by Okuaki et al. [8] they analyzed the average size of the message header for the CS scheme. We leave as an open problem theoretical analysis of the size of message header in the worst case.

References

[1] D. Naor, M. Naor and J.B. Lotspiech, "Revocation and tracing schemes for stateless receivers," CRYPTO '01, LNCS 2139, pp. 41–62, Springer-Verlag, 2001.

[2] D. Halevy and A. Shamir, The LSD broadcast encryption scheme, CRYPTO '02, LNCS 2442, pp. 47–60, Springer-Verlag, 2002.

[3] N. Attrapadung and H. Imai, Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext, ASIACRYPT '05.

[4] T. Asano, A revocation sheme with minimal storage at receivers, ASIACRYPT '02 LNCS 2501, pp. 433–450, Springer-Verlag, 2002.

[5] A. Fiat and M. Naor, Broadcast encryption, CRYPTO '93, LNCS 773, pp. 480–491, Springer-Verlag,1993.

[6] R. Nojima and Y. Kaji, Using Trapdoor Permutations in a Complete Subtree Method for Broadcast Encryption, IEICE Trans. Fundamentals, Vol. E88-A, No. 2, 2005.

[7] M. Luby and J. Staddon, Combinatorial Bounds for Broadcast Encryption. Advances in Cryptology — EUROCRYPT '98, LNCS 1403, Springer, 1998, pp. 512-526.

[8] S. Okuaki, N. Kunihiro and K. Ohta, Analysis of a message length for Complete Subtree Method (in Japanese), SCIS2007

[9] C.K. Wong, M. Gouda, and S. Lam, Secure group communications using key graphs, Proc. SIGCOMM, 1998. pp.68–79.

[10] D.M. Wallner, E.J.Harder, and R.C. Agee, Key Managment for multicast: Issues and architectures, IETF draft wallner-key, 1997.

[11] D. Boneh, C. Gentry and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", CRYPTO 2005.

Table 1 Comparison among some of existing schemes and ours

Type	Method	Header size (max)	Storage Size@User	Computation Cost
Combinatorial approach	CS [1]	$\leqq r \log \frac{n}{r}$	$1 + \log n$	$O(\log \log n)$
	Proposed Scheme I	$\leqq \lceil \frac{r}{4} \log \frac{n}{r} \rceil$	$6 \log n - 4$	$O(\log \log n)$
Computational approach	SD [1]	(ave $1.25r$) $\leqq 2r - 1$	$1 + \frac{1}{2} \log n + \frac{1}{2} \log^2 n$	$O(\log n)$
	LSD [2]	$\leqq 2kr - k$	$O(\log^{1+1/k} n)$	$O(\log n)$
	Nojima [6]	$\leqq r \log \frac{n}{r}$	1	$O(\log n)$
	SIC [3]	$\leqq 2r$	$\leqq k(\log n + 1)$	$O(kn^{1/k})$
	Proposed Scheme II	$\leqq \lceil \frac{r}{4} \log \frac{n}{r} \rceil$	$3 \log n - 2$	$O(\log n)$