2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

Hierarchical Key Assignment Scheme for Multimedia Access Control with Modified Hash Chain

Shoko Imaizumi, Naokazu Aoki,
and Hiroyuki Kobayashi
Graduate School of Advanced Integration Science
Chiba University
1–33 Yayoicho, Inage-ku, Chiba-shi, Chiba, Japan
Email: imaizumi@chiba-u.jp

Hitoshi Kiya
Dept. of Information and Communication Systems
Tokyo Metropolitan University
6-6 Asahigaoka, Hino-shi, Tokyo, Japan
Email: kiya@sd.tmu.ac.jp

***Abstract*—We propose a key assignment scheme and applying it to control hierarchical access to multimedia content. By introducing a modified hash chain, the proposed scheme manages one key composed of a single segment. The managed key is not distributed to any users, providing security against key leakage. Collusion attacks are prevented by the order of key assignment. Our scheme also reduces the number of hash calculations. Analysis of performance demonstrated this scheme is valid.**

***Index Terms*—key management; hash function; access control; content distribution network**

I. Introduction

Scalable transmission has become popular with the continuing growth in network technology. Access control schemes to protect media content has been widely studied [1]–[8]. A simple and straightforward way to accomplish versatile access control is by individually encrypting all entities, which belongs to media content. This approach, however, has to manage a large number of keys, given a large number of entities.

Access control schemes allow users to obtain media content at the permitted quality from one common enciphered codestream. Ordinary hash chains [9], called OHCs after this, have also been introduced to several schemes to reduce the number of key segments [5]–[8]. These OHC-based schemes of access control increase the number of key segments, depending on the hierarchical depth of scalability of the media. In addition, each key consists of multiple key segments in these schemes.

In this paper, we propose a hierarchical scheme of assigning keys to control access to multimedia content. We have assumed that multimedia content consists of multiple media and there is hierarchical scalability in each medium. By introducing a modified hash chain, called an MHC after this, the scheme we propose manages one key composed of a single key segment. The managed key is not distributed to any users, providing security against key leakage. Our scheme is also resilient to collusion attacks, in which malicious users illegally access multimedia content at higher quality than that allowed by their access rights. Moreover, this scheme reduces the number of hash calculations.

II. Requirements

A. Collusion Attack Resilience

Collusion attacks are caused by multiple users to obtain multimedia content at higher quality than that allowed by individual access rights, and a conventional scheme [5], called Scheme I after this, allows users to collude. The attacks are due to the multiple key segments comprising each key. The arrows in Fig. 1 indicate the order in which keys are assigned. $K_{E_{d_1,d_2}}$ is a key for entity E_{d_1,d_2}, and $K_{E_{3,2}}$ is the initial key. Initial key $K_{E_{3,2}}$ is divided into two key segments $K_{1(3)}$ and $K_{2(2)}$. Each key segment is allocated to each dimension, and key segments $K_{1(d_1)}$ and $K_{2(d_2)}$ are derived from previous key segments $K_{1(d_1+1)}$ and $K_{2(d_2+1)}$, using OHCs [9]. By concatenating them, key $K_{E_{d_1,d_2}} = K_{1(d_1)} \parallel K_{2(d_2)}$, is derived.

Alice is allowed to access multimedia content U at $Q_{0,2}$ and she receives key $K_{E_{0,2}}$ in Fig. 1 (a), which consists of two key segments $K_{1(0)}$ and $K_{2(2)}$. She can derive keys $K_{E_{0,1}}$ and $K_{E_{0,0}}$ and decipher $E_{0,2}$, $E_{0,1}$, and $E_{0,0}$. Whereas, Bob, in Fig. 1 (b), receives $K_{E_{3,0}}$, consisting of $K_{1(3)}$ and $K_{2(0)}$, and he derives $K_{E_{2,0}}$, $K_{E_{1,0}}$, and $K_{E_{0,0}}$ to decipher $E_{3,0}$, $E_{2,0}$, $E_{1,0}$, and $E_{0,0}$ to gain access U at $Q_{3,0}$. It is possible to illegally derive $K_{E_{3,2}}$ in this scheme by sharing $K_{1(3)}$ and $K_{2(2)}$, so they can decipher all entities shown in Fig. 1 (c) and access U at $Q_{3,2}$. The scheme we propose is resistant to collusion attacks.

B. Fewer Key segments

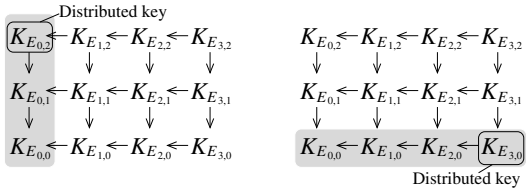
Key assignment schemes that manage one key consisting of multiple key segments and subordinately derive other keys from the managed keys have been proposed [5]–[8].

First, Scheme I [5], which is vulnerable to collusion attacks, needs two of key segments. The number of key segments in Scheme I, S_{I}, is

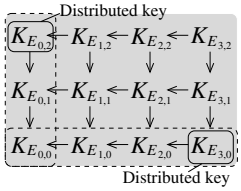
$$S_{\mathrm{I}} = 2. \tag{1}$$

The second scheme [6], called Scheme II after this, can control access to multimedia content with collusion attack resilience.

978-0-7695-4712-1/12 $26.00 © 2012 IEEE
DOI 10.1109/IIH-MSP.2012.77



(a) Keys obtained by Alice. (b) Keys obtained by Bob.



(c) Keys obtained by their collusion attack.

Fig. 1. Alice and Bob's collusion attack in the vulnerable scheme [5] (the shaded keys are obtained).

The number of key segments in Scheme II, S_{II}, is

$$S_{\mathrm{II}} \leq D_1, \quad D_1 \geq D_2 \geq \cdots \geq D_J, \tag{2}$$

where J is the number of media which is controlled access to, and D_j is the hierarchical depth of scalability in the j-th medium. A conventional scheme [7], called Scheme III after this, is resilient against collusion attacks, and manages multiple keys, each of which is composed of a single key segment. Note that one key consisting of i key segments is equal to i keys, each of which consists of a single key segment. Thus, the number of key segments in Scheme III, S_{III}, is

$$S_{\mathrm{III}} = J. \tag{3}$$

Another conventional method [8], called Scheme IV after this, has also collusion attack resilience, and manages one key consisting of a single key segment,

$$S_{\mathrm{IV}} = 1, \tag{4}$$

which is the same as the scheme we propose.

C. Less Hash Calculations

To decrease the number of key segments, a cryptographic one-way hash function is introduced in Schemes I, II, III and IV. The maximum number of hash calculations in these schemes, C_{I}, C_{II}, C_{III}, and C_{IV}, are

$$C_{\mathrm{I}} = D_1 + J - 2, \tag{5}$$

$$C_{\mathrm{II}} = D_1 \cdot J, \tag{6}$$

$$C_{\mathrm{III}} = \sum_{j=1}^{J} (D_j - 1), \tag{7}$$

$$C_{\mathrm{IV}} = D_1 + J - 2, \tag{8}$$

where $D_1 \geq D_2 \geq \cdots \geq D_J$. Thus, the number of these hash calculations must increase, when the hierarchical depth of scalability, D_j, deepens. The proposed scheme is designed not to substantially increase the number of hash calculations.

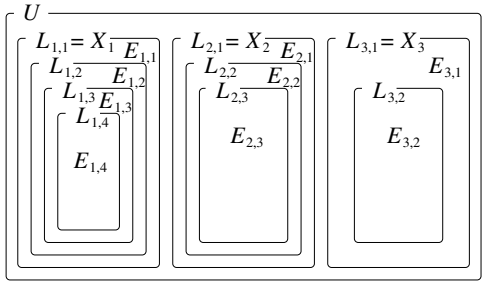


Fig. 2. Conceptual diagram of multimedia content U (the number of media $J = 3$ and the hierarchical depths of scalability in each medium $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$).

D. Flexible Control

Scheme IV [8] is resilient to collusion attacks and manages one key consisting of a single key segment, as mentioned in the previous section. Hash calculations in Scheme IV is also the least of these four schemes. This scheme, however, assumed that only a single medium has scalability and can be decoded at different quality, and that others do not have hierarchical scalability and can be decoded at only a fixed quality. Access control for multimedia content should be more flexible to decode each medium at different quality.

III. Proposed scheme

This section proposes a new scheme of assigning keys to control access to multimedia content that manages one key consisting of a single key segment. This scheme is resilient to collusion attacks, the same as Schemes II, III, and IV, and it does not increase the number of hash calculations.

We have assumed that multimedia content U consists of J of media X_j's and each medium X_j has scalability,

$$U = \{X_1, X_2, \ldots, X_j, \ldots, X_J\}, \tag{9}$$

$$X_j = L_{j,1}, \tag{10}$$

$$L_{j,1} \supset L_{j,2} \supset \cdots \supset L_{j,D_j}, \tag{11}$$

where $j = 1, 2, \ldots, J$, and L_{j,D_j} is the hierarchy of the scalability. The complementary sets represent entities in medium X_j as

$$E_{j,d_j} = L_{j,d_j} - L_{j,d_j+1}, \quad d_j = 1, 2, \ldots, D_j - 1, \tag{12}$$

and

$$E_{j,D_j} = L_{j,D_j}. \tag{13}$$

The proposed scheme derives keys from single managed key K_U and encrypts multimedia content U by encrypting E_{j,d_j}'s, using those corresponding keys.

Fig. 2 shows a conceptual diagram of multimedia content U, which is composed of three media, X_1, X_2, and X_3, i.e., $J = 3$. The hierarchical depths of scalability in media X_j's are four, three and two ($D_1 = 4$, $D_2 = 3$, and $D_3 = 2$), i.e.,

$$L_{1,1} \supset L_{1,2} \supset L_{1,3} \supset L_{1,4}, \tag{14}$$

$$L_{2,1} \supset L_{2,2} \supset L_{2,3}, \tag{15}$$

$$L_{3,1} \supset L_{3,2}, \tag{16}$$

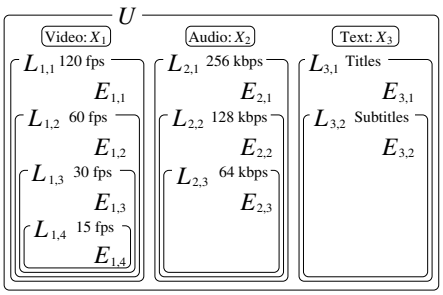


Fig. 3. Practical example of multimedia content U (the number of media $J = 3$ and the hierarchical depths of scalability in each medium $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$).

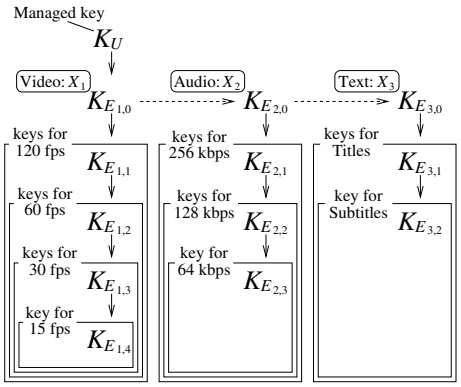


Fig. 4. Key derivation to control access to the multimedia content in Fig. 3. Solid arrows represent OHCs and Dashed arrows represent an MHC.

and E_{j,d_j}'s are entities in medium X_j.

For easy understanding, more practical example of Fig. 2 is given in Fig. 3. Multimedia content U consists of video (X_1), audio (X_2), and text (X_3) in Fig. 3, i.e., $J = 3$, and each medium has scalability whose depths are four, three, and two, i.e., $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$.

A. Key Assignment and Encryption

Access control is provided based not only on media, but also on scalability in the proposed scheme. Keys for entities are derived, as shown in Fig. 4, and each key is used to encrypt and decrypt the corresponding entity. For example, $K_{E_{1,1}}$ is a key for entity $E_{1,1}$ which represents video frames decoded at only 120 fps. $K_{E_{1,2}}$, $K_{E_{1,3}}$, and $K_{E_{1,4}}$ are keys for $E_{1,2}$, $E_{1,3}$, and $E_{1,4}$, respectively. Keys $K_{E_{2,d_2}}$ and $K_{E_{3,d_3}}$ are similarly for entity of audio E_{2,d_2} and entity of text E_{3,d_3} ($d_2 = 1, 2, 3$ and $d_3 = 1, 2$). Note that K_U is the managed key consisting of a single key segment.

First, Key $K_{E_{1,0}}$ is derived from K_U by

$$K_{E_{1,0}} = h\left(K_U\right), \tag{17}$$

where $h(\cdot)$ is a cryptographic one-way hash function. Similarly, keys $K_{E_{j,d_j}}$'s are respectively derived by

$$K_{E_{j,d_j}} = h^{d_j}\left(K_{E_{j,0}}\right), \quad d_j = 1, 2, \ldots, D_j, \quad j = 1, 2, 3, \tag{18}$$

where $h^{\alpha}(\beta)$ means that $h(\cdot)$ is applied to β recursively α times. Keys $K_{E_{2,0}}$ and $K_{E_{3,0}}$ are explained in the next paragraph. Eq. (18) represents OHCs [9], which have been indicated by the solid arrows in Fig. 4. Eq. (18) is also represented as

$$K_{E_{j,d_j}} = h\left(K_{E_{j,d_j-1}}\right), \quad d_j = 1, 2, \ldots, D_j, \quad j = 1, 2, 3. \tag{19}$$

Keys $K_{E_{2,0}}$ and $K_{E_{3,0}}$ are derived by an MHC. These keys are given by

$$K_{E_{j,0}} = h\left(s\left(K_{E_{j-1,0}}\right)\right), \qquad j = 2, 3,$$

where $s(\cdot)$ is a cyclic shift. Replacing the combination of $s(\cdot)$ and $h(\cdot)$ with $f(\cdot)$, which is an MHC, Eq. (20) is represented as

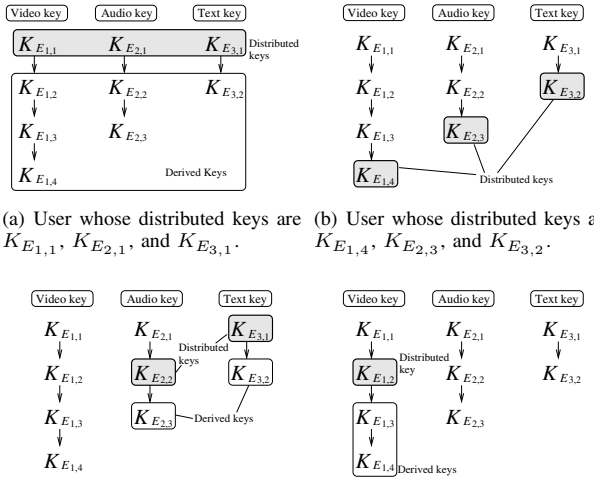
$$K_{E_{j,0}} = f\left(K_{E_{j-1,0}}\right). \tag{20}$$

The MHC is indicated by the dashed arrows in Fig. 4.

Each entity E_{j,d_j} is enciphered with key $K_{E_{j,d_j}}$, and then, multimedia content U is opened to public. Note that any arbitrary algorithm for symmetric enciphers can be used in the proposed scheme.

B. Key distribution and Decryption

1) User allowed to access three media: A user allowed to access multimedia content U at the highest quality receives three keys $K_{E_{1,1}}$, $K_{E_{2,1}}$, and $K_{E_{3,1}}$, as shown in Fig. 5 (a). He or she derives all of other keys to decrypt all entities, using OHCs given in Eq. (19). Users allowed to access three media



(a) User whose distributed keys are $K_{E_{1,1}}$, $K_{E_{2,1}}$, and $K_{E_{3,1}}$.

(b) User whose distributed keys are $K_{E_{1,4}}$, $K_{E_{2,3}}$, and $K_{E_{3,2}}$.

(c) User whose distributed keys are $K_{E_{2,2}}$ and $K_{E_{3,1}}$.

(d) User whose distributed key is $K_{E_{1,2}}$.

Fig. 5. Distributed keys and derived keys for each user.

TABLE I
COMPARISON WITH SCHEME I [5], II [6], III [7] AND IV [8]. RESULTS FOR (A) COLLUSION ATTACK RESILIENCE, (B) NUMBER OF KEY SEGMENTS, (C) MAXIMUM NUMBER OF HASH CALCULATIONS, AND (D) NUMBER OF MEDIA WITH SCALABILITY. NOTE THAT $D_1 \geq D_2 \geq \cdots \geq D_J$.

Scheme	(A)	(B)	(C)	(D)
Prop.	Yes	1	$\sum_{j=1}^{J} D_j + J$	J
I [5]	No	2	$D_1 + J - 2$	J
II [6]	Yes	$\leq D_1$	$D_1 \cdot J$	J
III [7]	Yes	J	$\sum_{j=1}^{J} (D_j - 1)$	J
IV [8]	Yes	1	$D_1 + J - 2$	1

at arbitrary quality also receive three keys $K_{E_{1,d_1}}$, $K_{E_{2,d_2}}$, and $K_{E_{3,d_3}}$.

We also assume that a user allowed to access each medium at the lowest quality, i.e., video at 15 fps, audio at 64 kbps, and subtitle data. He or she receives three keys $K_{E_{1,4}}$, $K_{E_{2,3}}$, and $K_{E_{3,2}}$, as shown in Fig. 5 (b). The user cannot, however, derive any keys from his or her distributed keys.

2) User allowed to access two media: Fig. 5 (c) shows a user allowed to access two of the three media. He or she can access audio at 128 kbps and title data. The user receives two keys $K_{E_{2,2}}$ and $K_{E_{3,1}}$, and derives $K_{E_{2,3}}$ for audio and $K_{E_{3,2}}$ for text, using OHCs given in Eq. (19).

3) User allowed to access a single medium: If a user can access only movie at 60 fps, he or she receives key $K_{E_{1,2}}$, as shown in Fig. 5 (d). The user dependently derives keys $K_{E_{1,3}}$ and $K_{E_{1,4}}$ using an OHC given in Eq. (19). Users who can access a single medium receive a single key.

Thus, the number of keys each user receives is equal to the number of media to which he or she is permitted to access. Users use only OHCs to derive keys from their distributed keys. Keys K_U, $K_{E_{1,0}}$, $K_{E_{2,0}}$, and $K_{E_{3,0}}$ are never distributed to any users to provide security against key leakage in our scheme.

IV. PERFORMANCE ANALYSIS AND COMPARISON

Table I compares the results for collusion attack resilience, the number of key segments, the number of hash calculations, and flexibility of access control, which are described in Section II. The proposed scheme was evaluated by comparing them with four conventional schemes, i.e., Schemes I [5], II [6], III [7], and IV [8], which only used OHCs.

The proposed scheme is resilient to collusion attacks as well as Schemes II, III, and IV, while Scheme I is naive against these attacks. We assume that Alice is the user described in Section III-B2, who is allowed to access audio at 128 kbps and title data, and Bob is the user explained in Section III-B3, who can access only movie at 60 fps. Alice receives keys $K_{E_{2,2}}$ and $K_{E_{3,1}}$, as shown in Fig. 5 (c). She derives $K_{E_{2,3}}$ and $K_{E_{3,2}}$ from her distributed keys. Bob receives $K_{E_{1,2}}$ and derives $K_{E_{1,3}}$ and $K_{E_{1,4}}$, as shown in Fig. 5 (d). They obtain seven valid keys in total, but they cannot illegally derive any keys from these seven keys.

Our scheme manages one key consisting of a single key segment, regardless of both the number of media and the hierarchical depth of scalability, while Schemes I, II, and III must manage multiple keys or key segments, as seen in Eq. (1), (2), and (3). The managed key is not distributed to any users in the proposed scheme to provide security against key leakage, whereas the managed keys or key segments are distributed to some users in Schemes I, II, and III.

The maximum number of hash calculations in the proposed scheme is $\sum_{j=1}^{J} D_j + J$. It should not be simply compared with that in Scheme IV, because Scheme IV can control access to scalability of only a single medium in multimedia content. If Scheme IV is extended to control access to scalability of each medium, the maximum number of hash calculations becomes the same as the proposed scheme and the users need to calculate hash values $J - 1$ times more than our scheme.

The scheme we proposed has accomplished flexible scheme, which can control access to not only media but also scalability of each medium in multimedia content.

V. CONCLUSION

This paper proposed an efficient scheme of key assignment for multimedia access control, in which an MHC is employed. The proposed scheme can control access to scalability not only in a single medium, but also in each medium. The scheme manages one key consisting of a single key segment, regardless of both the number of media and the hierarchical depth of scalability. The single managed key is not distributed to any users to provide security against key leakage. Our scheme also prevents collusion attacks, in which malicious users illegally access the multimedia content at higher quality than that allowed by their access rights.

ACKNOWLEDGMENT

This work was supported by KAKENHI (23800010).

REFERENCES

[1] D. Xie and C. C. J. Kuo, "Multimedia data encryption via random rotation in partitioned bit streams," in *Proc. IEEE ISCAS*, pp.5533–5536, 2005.

[2] Z. Zhang, Q. Sun, W. C. Wong, J. Apostolopoulos, and S. Wee, "Rate-distortion-authentication optimized streaming of authenticated video," *IEEE Trans. Circuits Syst. for Video Technol.*, vol.17, pp.544–557, May 2007.

[3] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," in *Proc. SPIE*, vol.4472, pp.95–104, 2001.

[4] Z. Shahid, M. Chaumont, and W. Puech, "Selective and scalable encryption of enhancement layers for dyadic scalable H.264/AVC by scrambling of scan patterns," in *Proc. IEEE ICIP*, pp.1273–1276, 2009.

[5] M. Joye and S. M. Yen, "one-way cross-trees and their applications," in *Proc. IACR PKC*, pp.355–358, 2002.

[6] X. Zhu and C. W. Chen, "A collusion resilient key management scheme for multi-dimensional scalable media access control," in *Proc. IEEE ICIP*, pp.2825–2828, 2011.

[7] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proc. IEEE ICIP*, pp.1977–1980, 2006.

[8] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "An efficient access control method for composite multimedia content," *IEICE Electronics Express*, vol.7, no.20, pp.1534–1538, 2010.

[9] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol.24, no.11, pp.770–772, 1981.