Multi-dimensional Key Assignment for Hierarchical Media Access Control with Collusion Resilience

Shoko Imaizumi, Naokazu Aoki, and Hiroyuki Kobayashi
Division of Information Sciences
Graduate School of Advanced Integration Science
Chiba University
Chiba, Japan
Email: imaizumi@chiba-u.jp, aoki@faculty.chiba-u.jp, kobahiro@faculty.chiba-u.jp

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

***Abstract*—We propose a multidimensional key assignment scheme using modified hash chains (MHCs) to hierarchically control access to scalable media. By introducing MHCs, the proposed scheme manages one key composed of a single key segment. The single managed key is not distributed to any user, providing security against key leakage. Collusion attacks caused by multiple users to obtain media with higher quality than that allowed by their access rights are prevented with the key assignment order. Our scheme also inhibits the growth of hash calculation. Performance analysis shows the validity of the proposed scheme.**

***Keywords-key assignment*; *access control*; *collusion attack*; *hash chain*; *cyclic shift*; *scalable media*.**

I. INTRODUCTION

With the growth in network technology, scalable transmission has become popular. Hierarchical access control to protect scalable media has been studied widely [1]–[8]. A simple and straightforward way to realize versatile access control for scalable media, to which several entities belong, is encrypting each entity individually. This approach, however, has to manage a large number of keys, given a large number of entities in a medium.

Hierarchical access control schemes have been proposed for scalable media [3]–[8], such as JPEG 2000 [9] coded images and/or MPEG-4 fine granularity scalability [10] coded videos, so that each user can obtain a medium at the permitted quality from one common enciphered codestream. OHCs (Ordinary hash chains) [11], hereafter, have also been introduced to several schemes for reduction of the number of key segments, which compose each key [5]–[7]. These OHC-based access control schemes increase the number of key segments, depending not only on the dimensions of scalability, but also on the hierarchical depth of scalability. Another scheme, which is also based on OHCs, has been proposed to reduce the number of key segments to one, but this scheme assumes the controlled media has only a single hierarchy [8].

In this paper, we propose an efficient key assignment scheme for hierarchical media access control. We assume that there is multi-dimensional scalability in each scalable medium. By introducing MHCs (modified hash chains), hereafter, the proposed scheme 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 media at higher quality than that allowed by their access rights. Moreover this scheme inhibits increasing the amount of hash calculation by using cyclic shifts.

This paper is organized as follows. Section II briefly describes hierarchical access control and mentions three requirements for hierarchical access control of scalable media. The new scheme is proposed in Section III, and is analyzed in Section IV. Finally, conclusions are drawn in Section V.

II. PRELIMINARIES

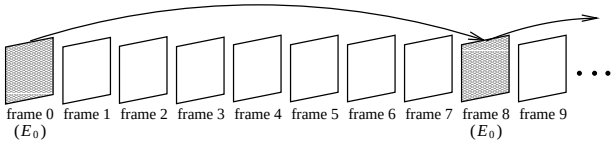
We briefly describe hierarchical access control for scalable media, and also summarize three requirements on key assignment for hierarchical access control, introducing some conventional schemes [5]–[7] to clarify the aim of this work.

A. Hierarchical Access Control

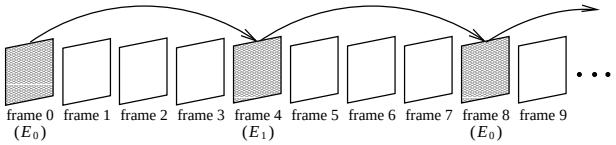
Firstly, we assume that scalable medium X has one-dimensional scalability ($J = 1$) and the scalability is frame rate, of which the hierarchical depth is $D_1 = 4$. As shown in Fig. 1, medium X should be decoded at 15 (Q_0), 30 (Q_1), 60 (Q_2), or 120 (Q_3) frames per second (fps). Fig. 2 shows a practical diagram of medium X. L_{d_1} $(d_1 = 0, 1, 2, 3)$ represents a set of frames decoded at 15, 30, 60, or 120 fps. Entity E_3 is a complementary set of L_2, that is frames decoded at 120 fps only. Similarly, E_2 and E_1 represent complementary sets of L_1 and L_0, respectively. E_0 represents the same as L_0, that is a set of frames decoded at each frame rate.

For another example, we also assume that scalable medium X has two-dimensional scalability ($J = 2$). One

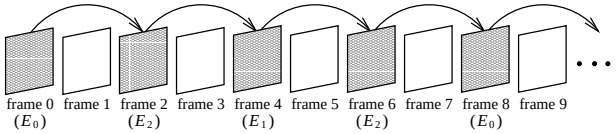
 ISBN: 978-1-61208-231-8



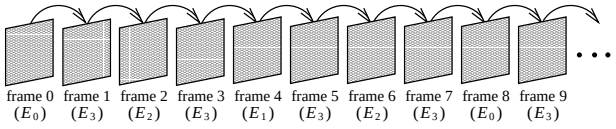
(a) 15 fps (Q_0).



(b) 30 fps (Q_1).



(c) 60 fps (Q_2).



(d) 120 fps (Q_3).

Figure 1. Hierarchical decoding of one-dimensional scalable medium X at frame rate Q_{d_1} ($J = 1$ and $D_1 = 4$ ($d_1 = 0, 1, 2, 3$)).

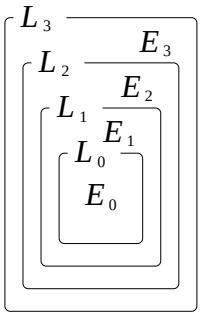
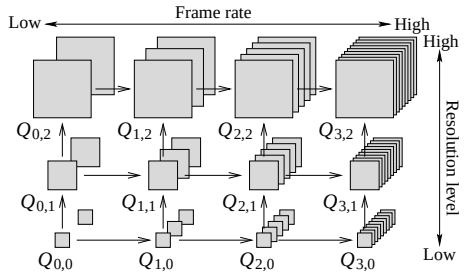
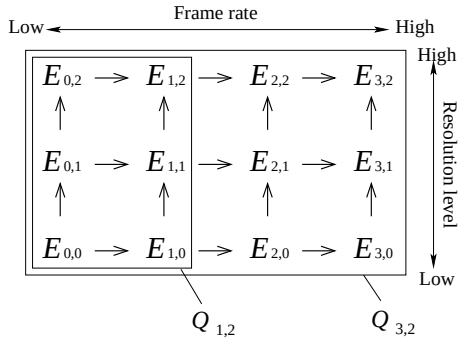


Figure 2. Practical diagram of medium X.

of the dimensions is frame rate and the other is resolution level, and the hierarchical depths of them are $D_1 = 4$ and $D_2 = 3$. Fig. 3 outlines an example of scalable decoding in which the scalable media with two-dimensional scalability ($D_1 = 4$ and $D_2 = 3$) are decompressed at different quality. The highest quality is $Q_{3,2}$. Medium X with quality $Q_{3,2}$ is obtained by decompressing all entities. To decode medium X at $Q_{1,2}$, six entities $E_{1,2}$, $E_{1,1}$, $E_{1,0}$, $E_{0,2}$, $E_{0,1}$, and $E_{0,0}$ are decompressed. Thus, access control for scalable media should encipher the codestream entity-by-entity using different keys.



(a) Decoding quality Q_{d_1,d_2}.



(b) Decoding order of entity E_{d_1,d_2}.

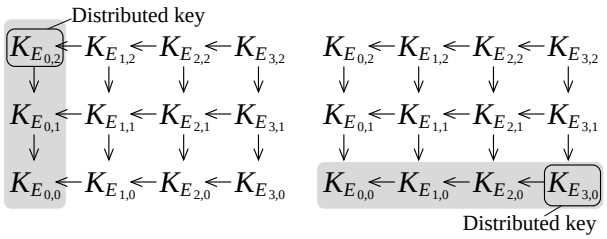
Figure 3. Hierarchical decoding of two-dimensional scalable medium X at frame rate and resolution level Q_{d_1,d_2} ($J = 2$, $D_1 = 4$ ($d_1 = 0, 1, 2, 3$), and $D_2 = 3$ ($d_2 = 0, 1, 2$)).

B. Requirements

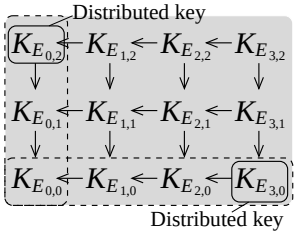
This section describes three requirements on key assignment for hierarchical access control of scalable media, i.e., collusion attack resilience, the less number of managed key segments, and the less amount of hash calculation.

1) Collusion Attack Resilience: Collusion attacks are caused by multiple users to obtain medium X with higher quality than that allowed by their access rights, and the conventional scheme [5], Scheme I hereafter, allows users to collude. The attacks are due to multiple key segments composing each key. In Fig. 4, the arrows indicate key assignment order. $K_{E_{d_1,d_2}}$ is a key for entity E_{d_1,d_2}, and $K_{E_{3,2}}$ is the initial key. As shown in Fig. 5, 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 [11]. By concatenating them, key $K_{E_{d_1,d_2}} = K_{1(d_1)} \parallel K_{2(d_2)}$ is derived.

In Fig. 4(a), Alice is allowed to access medium X at $Q_{0,2}$ and receives key $K_{E_{0,2}}$, 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. 4(b), receives $K_{E_{3,0}}$, consisting of $K_{1(3)}$ and $K_{2(0)}$, and 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 $E_{0,0}$ for access to medium X at $Q_{3,0}$. In this scheme, they are possible to illegally derive $K_{E_{3,2}}$ by sharing $K_{1(3)}$ and



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



(c) Keys obtained by their collusion attack.

Figure 4. Alice and Bob's collusion attack in the vulnerable scheme [5] (the shaded keys are obtained).

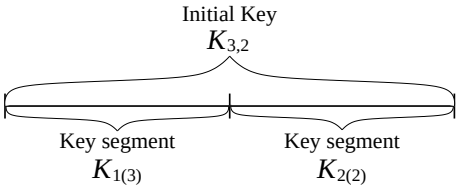


Figure 5. Initial key consisting of two key segments [5].

$K_{2(2)}$ with each other, so they can decipher all entities as shown in Fig. 4(c) and access medium X at $Q_{3,2}$. The proposed scheme is resistant to collusion attacks.

2) The Less Number of Key segments: Key assignment schemes that manage one key consisting of multiple key segments and subordinately derive other keys from the managed key have been proposed [5]–[7]. In these schemes, a key consists of multiple key segments.

First, Scheme I [5], which is vulnerable to collusion attacks, needs the same number of key segments as the number of the dimensions of scalability, J. The number of key segments in Scheme I, S_{I}, is

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

The second and third schemes [6], [7], Scheme II and Scheme III hereafter, control access to scalable media with collusion attack resilience. The number of key segments in Schemes II and III, S_{II} and S_{III}, are

$$S_{\mathrm{II}} = \prod_{j=2}^{J} D_j, \quad D_1 \geq D_2 \geq \cdots \geq D_J, \tag{2}$$

$$S_{\mathrm{III}} \leq \prod_{j=2}^{J} D_j, \quad D_1 \geq D_2 \geq \cdots \geq D_J, \tag{3}$$

respectively, whereas the proposed scheme needs a single key segment.

3) The Less Amount of Hash Calculation: To decrease the number of key segments, a cryptographic one-way hash function is introduced in Schemes I, II, and III. The maximum amount of hash calculation in these schemes, C_{I}, C_{II}, and C_{III}, are

$$C_{\mathrm{I}} = \sum_{j=1}^{J} \left(D_j - 1 \right), \tag{4}$$

$$C_{\mathrm{II}} = \prod_{j=1}^{J} D_j - 1, \tag{5}$$

$$C_{\mathrm{III}} = \prod_{j=1}^{J} D_j, \tag{6}$$

respectively. Thus, these amounts of hash calculation must increase, deepened the hierarchical depth of scalability, D_j. The proposed scheme is designed not to increase hash calculation substantially.

III. Proposed scheme

In this section, we propose a new key assignment scheme for access control of scalable media that manages one key consisting of a single key segment. The proposed scheme is resilient to collusion attacks the same as Schemes II and III, and does not increase the amount of hash calculation.

A. Key Assignment and Encipherment

As an example of scalable media for explanation, we assume three-dimensional scalable medium X ($J = 3$) shown in Fig. 6, where it is composed of four kinds of frame rates ($D_1 = 4$), three resolution levels ($D_2 = 3$), and two layers ($D_3 = 2$). Fig. 7 shows our proposed key assignment order, where $K_{E_{d_1,d_2,d_3}}$ is the key for entity E_{d_1,d_2,d_3} and K_m is the managed key. This order is resilient to collusion attacks. It is noted that a key is not composed of multiple key segments and consists of a single key segment in the proposed scheme.

Firstly key $K_{E_{3,2,1}}$ is derived from K_m as

$$K_{E_{3,2,1}} = h\left(K_m\right), \tag{7}$$

where $h(\cdot)$ is a cryptographic one-way hash function, i.e., the SHA-2 family (SHA-224, SHA-256, SHA 384, and SHA-512) [12]. Similarly, keys $K_{E_{d_1,d_2,d_3}}$'s are assigned on each of d_2 or d_3 ($d_2 = 2, 1, 0$ and $d_3 = 1, 0$) as

$$K_{E_{d_1,d_2,d_3}} = h^{3-d_1}\left(K_{E_{3,d_2,d_3}}\right), \quad d_1 = 2, 1, 0, \tag{8}$$

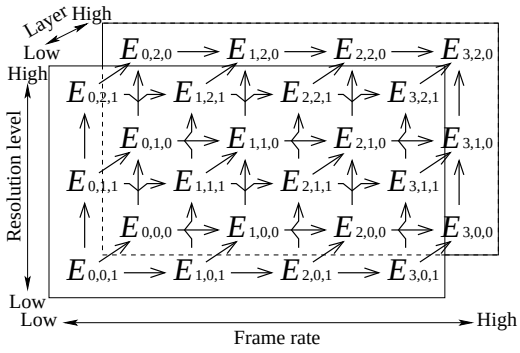


Figure 6. Decoding order of entity E_{d_1,d_2,d_3} in three-dimensional scalable medium X ($J = 3$, $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$).

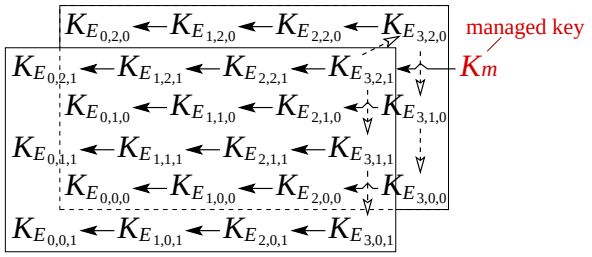
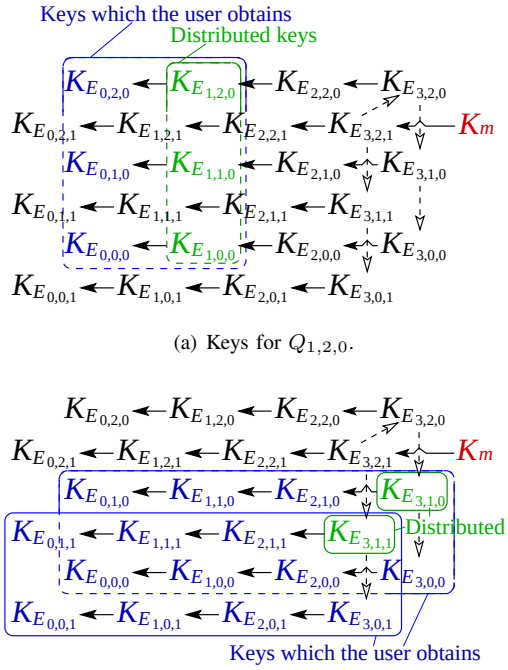


Figure 7. Key assignment to control access to three-dimensional scalable medium X shown in Fig. 6. Solid arrows are OHCs and dashed arrows represent MHCs.



(a) Keys for $Q_{1,2,0}$.

(b) Keys for $Q_{3,1,1}$.

Figure 8. Distributed and derived keys that the user needs to decompress medium X shown in Fig. 6 at certain quality.

respectively, where $h^{\alpha}(\beta)$ represents that $h(\cdot)$ is applied to β recursively α times. Keys $K_{E_{3,d_2,d_3}}$'s, except $K_{E_{3,2,1}}$, are given in the next paragraph. Eq. (8) represents OHCs [11], and the OHCs are shown with solid arrows in Fig. 7. Eq. (8) is also represented as

$$K_{E_{d_1,d_2,d_3}} = h\left(K_{E_{d_1+1,d_2,d_3}}\right), \quad d_1 = 2,1,0. \tag{9}$$

Meanwhile, keys $K_{E_{3,d_2,d_3}}$'s, except $K_{E_{3,2,1}}$, are assigned by MHCs. In this example, keys $K_{E_{3,1,d_3}}$, $K_{E_{3,0,d_3}}$ are given on each d_3 ($d_3 = 1,0$) as

$$K_{E_{3,d_2,d_3}} = h\left(s\left(K_{E_{3,d_2+1,d_3}}\right)\right), \quad d_2 = 1,0, \tag{10}$$

where $s(\cdot)$ is a cyclic shift. It is noted that the amount of each cyclic shift doesn't have to be secret information and that they can be opened to the public. Replacing the combination of $s(\cdot)$ and $h(\cdot)$ with $f(\cdot)$, which is an MHC, Eq. (10) is represented as

$$K_{E_{3,d_2,d_3}} = f\left(K_{E_{3,d_2+1,d_3}}\right), \quad d_2 = 1,0. \tag{11}$$

Key $K_{E_{3,2,0}}$ is also derived as

$$\begin{aligned} K_{E_{3,2,d_3}} &= h\left(s\left(K_{E_{3,2,d_3+1}}\right)\right) \\ &= f\left(K_{E_{3,2,d_3+1}}\right) \\ d_3 &= 0. \end{aligned} \tag{12}$$

It is noted that the amounts of cyclic shifts are secret information. The MHCs are shown with dashed arrows in Fig. 7.

By introducing MHCs, all keys $K_{E_{d_1,d_2,d_3}}$'s for all entities E_{d_1,d_2,d_3}'s are assigned based on managed key K_m. With key $K_{E_{d_1,d_2,d_3}}$, each entity E_{d_1,d_2,d_3} is enciphered. It is noted that any arbitrary symmetric encipher algorithm can be used in the proposed scheme.

B. Distributed keys and Decipherment

Here, it is considered that a user is allowed to access medium X with quality $Q_{1,2,0}$. The user receives keys $K_{E_{1,2,0}}$, $K_{E_{1,1,0}}$, and $K_{E_{1,0,0}}$ as shown in Fig. 8(a). To decompress medium X at $Q_{1,2,0}$, the user needs to decipher six entities $E_{1,2,0}$, $E_{1,1,0}$, $E_{1,0,0}$, $E_{0,2,0}$, $E_{0,1,0}$, and $E_{0,0,0}$. Three keys $K_{E_{0,2,0}}$, $K_{E_{0,1,0}}$, and $K_{E_{0,0,0}}$ are derived from distributed keys $K_{E_{1,2,0}}$, $K_{E_{1,1,0}}$, and $K_{E_{1,0,0}}$ as

$$K_{E_{0,d_2,0}} = h\left(K_{E_{1,d_2,0}}\right), \quad d_2 = 2,1,0. \tag{13}$$

By using six keys $K_{E_{1,2,0}}$, $K_{E_{1,1,0}}$, $K_{E_{1,0,0}}$, $K_{E_{0,2,0}}$, $K_{E_{0,1,0}}$, and $K_{E_{0,0,0}}$, corresponding entities are deciphered and decompressed to present medium X at $Q_{1,2,0}$.

As another example, we also assume that a user can access medium X with quality $Q_{3,1,1}$. The user receives two keys $K_{E_{3,1,1}}$ and $K_{E_{3,1,0}}$ as shown in Fig. 8(b). To access medium X at $Q_{3,1,1}$, the user has to obtain 16 of keys $K_{E_{d_1,d_2,d_3}}$'s ($d_1 = 3,2,1,0$, $d_2 = 1,0$, and $d_3 = 1,0$). $K_{E_{3,0,1}}$ and $K_{E_{3,0,0}}$ are derived from distributed keys $K_{E_{3,1,1}}$ and

 ISBN: 978-1-61208-231-8

Table I
COMPARISON WITH SCHEMES I [5], II [6], AND III [7]

Scheme	Collusion resilience	# Key segments	Max # hash calculation
Prop.	Yes	1	$\prod_{j=1}^{J} D_j - 1$
I [5]	No	J	$\sum_{j=1}^{J} (D_j - 1)$
II [6]	Yes	$\prod_{j=2}^{J} D_j$	$\prod_{j=1}^{J} D_j - 1$
III [7]	Yes	$\leq \prod_{j=2}^{J} D_j$	$\prod_{j=1}^{J} D_j$

$K_{E_{3,1,0}}$ using MHCs as

$$\begin{aligned} K_{E_{3,0,d_3}} &= h\left(s\left(K_{E_{3,1,d_3}}\right)\right) \\ &= f\left(K_{E_{3,1,d_3}}\right), \\ d_3 &= 1, 0. \end{aligned} \tag{14}$$

Then, 12 of keys $K_{E_{d_1,d_2,d_3}}$'s ($d_1 = 2, 1, 0$, $d_2 = 1, 0$, and $d_3 = 1, 0$) are assigned using OHCs as given in Eq. (8), and the user can decompress medium X at $Q_{3,1,1}$.

In the proposed scheme, the managed key is never distributed to any users in terms of security against key leakage.

IV. PERFORMANCE ANALYSIS AND COMPARISON

This section verifies that the proposed scheme meets requirements described in Section II-B. Table I shows the comparison result in terms of collusion attack resilience, the number of key segments and the amount of hash calculation, which are described in Section II-B. The proposed scheme is evaluated by comparing with three conventional schemes, i.e., Schemes I [5], II [6], and III [7], which use only OHCs.

A. Collusion Attack-Resistance

The proposed scheme is resilient to collusion attacks as well as Schemes II and III, while Scheme I is naive for the attacks.

In Fig. 6, we assume that Alice is allowed to access medium X at $Q_{0,2,0}$ and Bob is allowed to decompress it at $Q_{3,0,1}$. Alice receives three keys $K_{E_{0,n_2,0}}$'s ($n_2 = 2, 1, 0$). She cannot derive any keys from these distributed keys. In other hand, Bob receives two keys $K_{E_{3,0,1}}$ and $K_{E_{3,0,0}}$ and derives six keys $K_{E_{n_1,0,n_3}}$'s ($n_1 = 2, 1, 0$ and $n_3 = 1, 0$) using Eq. (8). They obtain ten valid keys in total, but they can not illegally derive any keys which they are not permitted to derive from these ten keys.

B. The Number of Key Segments

The proposed scheme manages one key consisting of a single key segment regardless of the dimensions of scalability and the hierarchical depth of scalability, while Schemes I, II, and III must manage multiple key segments, as given in Eqs. (1), (2), and (3).

The managed key is not distributed to any users in the proposed scheme in terms of security against key leakage, whereas the managed key segments are distributed to some users in Schemes I, II, and III.

C. The Amount of Hash Calculation

The maximum amount of hash calculation in the proposed scheme is $\prod_{j=1}^{J} D_j - 1$, which is the same as that in Scheme II, C_{II}, as given in Eq. (5). C_{III} is $\prod_{j=1}^{J} D_j$, as given in Eq. (6), and Scheme III must calculate once more than with the proposed scheme. Although C_{I} is less than those in other schemes, Scheme I is vulnerable for collusion attacks. It is noted that the proposed scheme needs cyclic shifts to assign some of keys.

V. CONCLUSION

This paper has proposed a novel key assignment scheme for hierarchical media access control, in which MHCs are employed. The proposed scheme can control access to scalable media with multi-dimensional scalability. The scheme manages one key composed of a single key segment. The single managed key is not distributed to any users. This scheme also prevents collusion attacks, in which malicious users illegally access media at higher quality than that allowed by their access rights. Performance analysis showed the effectiveness of our scheme. Future work will focus on applying this scheme to real systems.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number 23800010.

REFERENCES

[1] D. Xie and C.-C.J. Kuo, "Multimedia data encryption via random rotation in partitioned bit streams," in *Proc. IEEE ISCAS 2005*, 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 46th Annual Meeting, Applications of Digital Image Processing XXIV*, 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 2009*, pp. 1273–1276, 2009.

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

[6] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "Efficient collusion attack-free access control for multidimensionally hierarchical scalability content," in *Proc. IEEE ISCAS 2009*, pp. 505–508, 2009.

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

 ISBN: 978-1-61208-231-8

[8] S. Imaizumi, M. Fujiyoshi, and H. Kiya, “An Efficient Access Control Scheme for Multimedia Content Using Modified Hash Chain,” in *Proc. IARIA ICSNC 2011*, pp. 175–180, 2011.

[9] *Information technology — JPEG 2000 image coding system – Part 1: Core coding system*, ISO/IEC 15444–1, 2004.

[10] *Information technology — Coding of audio – Visual objects – Part 2: Visual*, ISO/IEC 14496–2, 2004.

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

[12] NIST, *Secure Hash Standard*, FIPS PUB 180–4, 2012.

 ISBN: 978-1-61208-231-8