An Efficient Access Control Scheme for Multimedia Content Using Modified Hash Chain

Shoko Imaizumi
Division of Information Sciences
Graduate School of Advanced Integration Science
Chiba University
Chiba, Japan
Email: imaizumi@chiba-u.jp

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

***Abstract*—This paper proposes an access control scheme for multimedia content consisting of several media such as text, images, sound, and so on. The proposed scheme simultaneously controls access to each medium of multimedia content in which a hierarchy based on the quality (resolution, frame rate, bit rate, and so on) is allowed to be in one medium. The proposed scheme derives keys through hash chains, and each medium/ entity is encrypted with each individual key. By introducing modified hash chains, the proposed scheme manages only a single key for multimedia content, and it delivers only a single key to a user for the content regardless of which parts in the content the user can access; whereas the conventional access control schemes having the above mentioned features manage and/or deliver multiple keys. The single managed key is not delivered to any user. Furthermore the proposed scheme is resilient to collusion attacks. Performance analysis shows the effectiveness of the proposed scheme. The proposed scheme is more secure and simpler than the conventional scheme in terms of key management and delivery.**

***Keywords-multimedia communication*; *access control*; *key derivation*; *hash chain*; *cryptography*.**

I. Introduction

With the growth in network technology, the exchange of digital images and sound as well as text become very common regardless of whether the digital content is used for commercial purpose or not. Since such digital content is easily duplicated and re-distributed, protecting copyrights and privacy is an important issue. *Access control* based on naïve encryption (encrypting the whole content) [1] or media-aware encryption [2]–[6] has been studied widely to protect digital content.

A simple and straightforward way for realizing versatile access control to multimedia content consisting of several media to which several entities belong is encrypting each entity individually. This approach, however, has to manage a large number of keys, according to the number of entities in multimedia content. Moreover, a user has to receive a number of keys, according to the number of accessible entities.

On the other hand, for JPEG 2000 [7] coded images and/ or MPEG-4 fine granularity scalability [8] coded videos, *scalable access control* schemes have been proposed [2]–[6]. These schemes utilize one- or multi-dimensionally *hierarchical scalability* provided by coding technologies so that a user can obtain an image or a video in the permitted quality from one common codestream. In addition, *hash chain* [9], [10] is introduced to several schemes for reducing the managed and managed keys [3]–[6].

Though a hash chain-based access control scheme has been proposed for multimedia content [11], the number of managed keys increases dependently on not only the number of media but also the dimensions of hierarchies in the media. The number of delivered keys is increased as many as the number of managed keys. Moreover, malicious users can share their keys to increase accessible media/entities in this scheme.

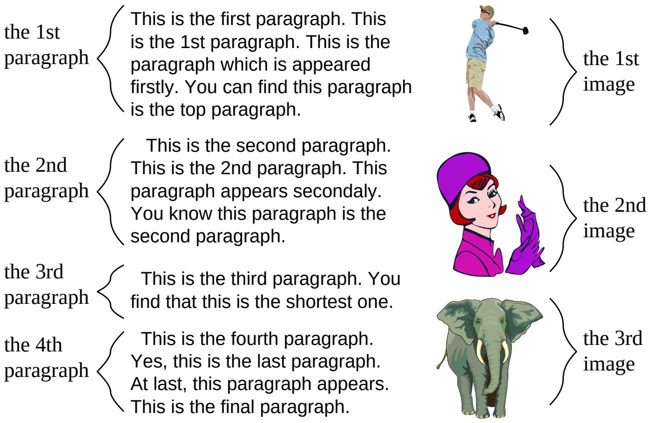
This paper proposes an access control scheme for multimedia content which the scheme manages and delivers only a single key. The proposed scheme assumes that content consists of several media and there is a scalable hierarchy on the quality in one of media. By introducing modified hash chains, the managed key is one as many as the delivered key regardless of which media/entities the user is allowed to access. The managed key is not delivered to any user in terms of security against key leakage. Moreover, the proposed scheme is resilient to collusion attacks which malicious users access much more portions beyond their rights illegally.

This paper consists of five sections. Section II mentions the conventional access control scheme for multimedia and describes the problems of the conventional scheme. The new scheme is proposed in Section III and is analyzed in Section IV. Finally, conclusions are drawn in Section V.

II. Conventional Access Control Scheme for Multimedia Content

This section briefly describes the conventional access control scheme for multimedia content [11], and summarizes problems of the conventional scheme to clarify the aim of this work.

ISBN: 978-1-61208-166-3



This is the first paragraph. This is the 1st paragraph. This is the paragraph which is appeared firstly. You can find this paragraph is the top paragraph.

This is the second paragraph. This is the 2nd paragraph. This paragraph appears secondaly. You know this paragraph is the second paragraph.

This is the third paragraph. You find that this is the shortest one.

This is the fourth paragraph. Yes, this is the last paragraph. At last, this paragraph appears. This is the final paragraph.

Figure 1. An example of multimedia content (the number of media $M = 2$, the number of entities in the first medium $D_1 = 4$, and the number of entities in the second medium $D_2 = 3$).

A. Conventional Scheme

The conventional scheme [11] assumes that content consists of M different media (image, video, sound, text, and so on) which a hierarchy (image/video resolution, frame rate, bit rate, etc) exists in each medium; In the text medium, the appearing order of paragraphs has its own meaning, and it is referred to as a *semantic* hierarchy. The scheme uses a symmetric encryption technique.

For multimedia content consisting of M different media, this scheme manages M keys. Fig. 1 shows an example of multimedia content where $M = 2$. For the m-th medium where $m = 1, 2, \ldots, M$, encryption keys are derived from managed key $K_m^{D_m}$ that corresponds to the m-th medium, where D_m represents the number of entities in the medium, i.e., the depth of the hierarchy. Encryption keys $K_m^{d_m}$'s are derived through a hash chain as

$$K_m^{d_m} = H^{D_m - d_m}\left(K_m^{D_m}\right), \; d_m = 0, 1, \ldots, D_m - 1, \quad (1)$$

where $H^{\alpha}(\beta)$ represents that cryptographic one-way hash function $H(\cdot)$ is applied to β recursively α times. The d_m-th entity in the m-th medium is encrypted with its corresponding encryption key, $K_m^{d_m}$.

A user receives M decryption keys. Each user receives different set of decryption keys, which are delivered keys, due to which media/entities the user is allowed to access, but all users receives the common encrypted multimedia content. From the delivered keys, the user derives keys for accessible entities in accessible media through the same hash chain as used in the encryption key derivation. That is,

$$K_m^{\delta_m} = H^{\Delta_m - \delta_m}\left(K_m^{\Delta_m}\right), \; \delta_m = 1, 2, \ldots, \Delta_m - 1, \quad (2)$$

where $K_m^{\Delta_m}$ is the delivered key for the m-th medium. By using Δ_m decryption keys, the user decrypts Δ_m entities from the first entity to the Δ_m-th entity.

A user who receives K_m^0 cannot access any entities in the m-th medium, because one-way property of $H(\cdot)$ prevents the user to generate any other valid keys for the m-th medium of the content. The conventional scheme introduced this *unusable key* concept in order to cope with medium-based access control.

B. Problems of the Conventional Scheme

The conventional scheme [11] has two major problems.

- the number of managed and delivered keys
- collusion attack-vulnerable

As mentioned in the previous section, the conventional scheme encrypts entities in a medium independently of other media. This feature of the conventional scheme requires managed and delivered keys as many as media in the multimedia content, i.e., M keys are managed and M keys are delivered to a user for content consisting of M different media. This conventional scheme employs ordinary hash chains [9] rather than cross-way hash trees [10] in essentials.

The latter problem is also attributed to the feature just described in the above paragraph. Though introducing unusable key concept in order to serve medium-based access control, the conventional scheme allows malicious users to collude to access inaccessible media. A user who can display images and another user who is allowed to read texts share their keys and obtain both images and text paragraphs.

In the next section, a new access control scheme for multimedia content is proposed. The proposed scheme manages only a single key and delivers also only a single key to a user regardless of which media/entities in the content the user can access. In addition, the proposed scheme is resistant to collusion attack.

III. Proposed Scheme

This section proposes a new access control scheme for multimedia content. The proposed scheme assumes that multimedia content C consists of M media and the first medium has a hierarchical structure;

$$C = \left\{G_1^1, G_2^1, \ldots, G_m^1, \ldots, G_M^1\right\}, \quad (3)$$

$$G_1^1 \supset G_1^2 \supset G_1^3 \supset \cdots \supset G_1^{D_m}, \quad (4)$$

where G_m^1 $(m = 1, 2, \ldots, M)$ represents the m-th medium content itself, and D_1 is the depth of the hierarchy in the first medium. The complementary sets represent entities in medium G_1^1 as

$$E_1^{d_m} = G_1^{d_m} - G_1^{d_m+1}, \quad d_m = 1, 2, \ldots, D_m - 1, \quad (5)$$

and

$$E_m^{D_m} = G_m^{D_m}. \quad (6)$$

The proposed scheme derives keys from single managed key K_C and encrypts content C by encrypting $E_m^{d_m}$'s using those corresponding keys. In addition, this scheme delivers only a single key to each user.

Fig. 2 shows an example conceptual diagram of the assumed multimedia content, where content C consists of

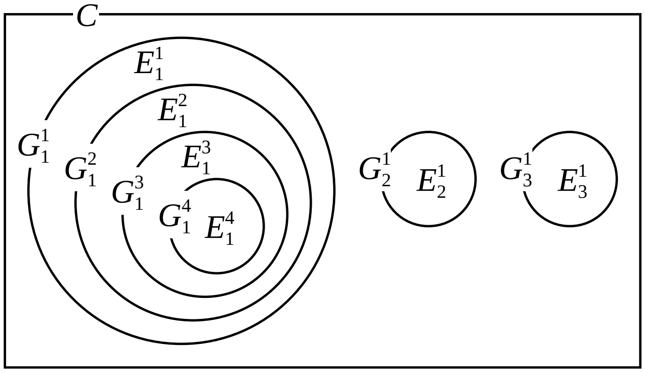


Figure 2. An example of multimedia content conceptual diagram in the proposed scheme (the number of media $M = 3$ and the depth of the hierarchical structure in the first medium $D_1 = 4$).

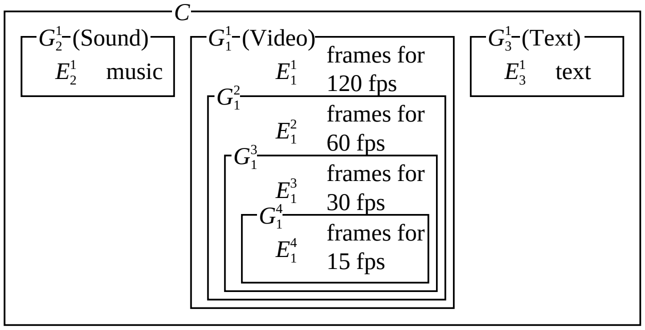

C
G_2^1-(Sound)
E_2^1 music
G_1^1-(Video)
E_1^1 frames for 120 fps
G_1^2
E_1^2 frames for 60 fps
G_1^3
E_1^3 frames for 30 fps
G_1^4
E_1^4 frames for 15 fps
G_3^1-(Text)
E_3^1 text

Figure 3. A practical example of multimedia content (the number of media $M = 3$ and the depth of video $D_1 = 4$).

three media, G_1^1, G_2^1, and G_3^1, i.e., $M = 3$, and the hierarchy depth of medium G_1^1 is four ($D_1 = 4$), i.e.,

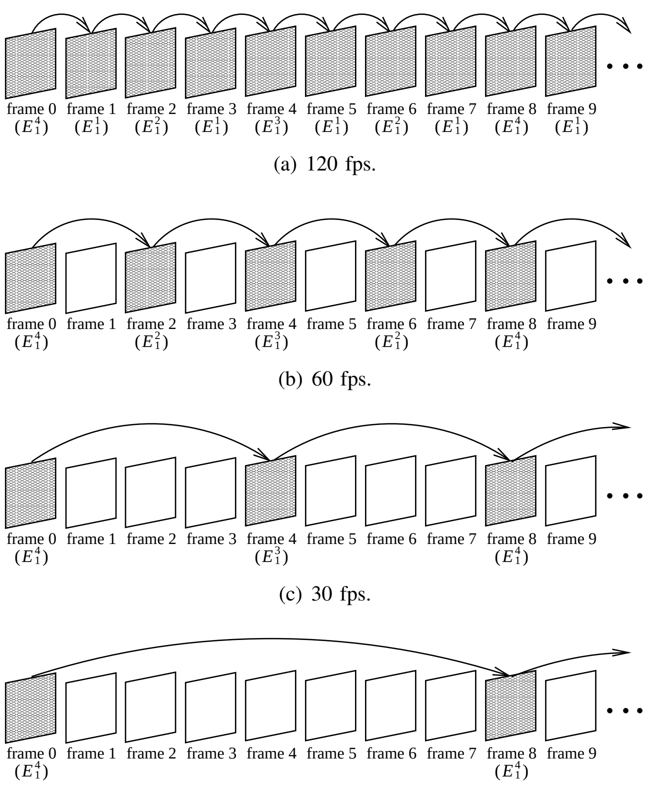
$$G_1^1 \subset G_1^2 \subset G_1^3 \subset G_1^4. \quad (7)$$

E_1^1, E_1^2, E_1^3, and E_1^4 are entities in medium G_1^1.

A. Key Derivation and Encryption

This section provides the key derivation mechanism in the proposed scheme under the condition content C is abstracted as Fig. 2. For easy understanding, more practical example is given in Fig. 3. Content C in Fig. 3 consists of video, sound, and text, i.e., $M = 3$, and video has a hierarchy with four in depth in terms of the frame rate, i.e., $D_1 = 4$. In this example, G_1^1 is digital video, and it is playable in several frame rates; 120, 60, 30, and 15 frames per second (fps). Shown in Fig. 4, frames decoded at each rate are represented by G_1^1, G_1^2, G_1^3, and G_1^4, respectively. Media G_2^1 and G_3^1 are sound and text, respectively.

In the example here, access control is provided based on not only media but also the frame rates of video. For content C shown in Fig. 3, keys for encryption are derived as shown in Fig. 5, and each key is used to encrypt and decrypt the corresponding medium/entity. For the video, $K_{E_1^1}$ is for E_1^1 which represents frames decoded at 120 fps only. Similarly, keys $K_{E_1^2}$, $K_{E_1^3}$, and $K_{E_1^4}$ are for E_1^2, E_1^3, and E_1^4, respectively. Keys $K_{E_2^1}$ and $K_{E_3^1}$ are for sound and text, respectively. It is noted that key K_C is the single managed key.



(a) 120 fps.

(b) 60 fps.

(c) 30 fps.

(d) 15 fps.

Figure 4. Decode of a movie in different frame rates (The shaded frames are decoded).

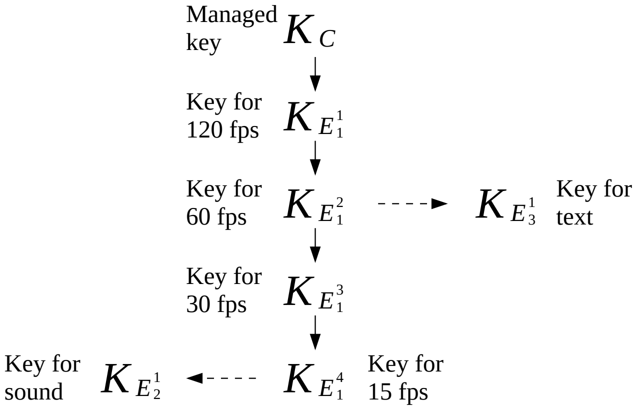

Managed key K_C
Key for 120 fps $K_{E_1^1}$
Key for 60 fps $K_{E_1^2}$
$K_{E_3^1}$ Key for text
Key for 30 fps $K_{E_1^3}$
Key for sound $K_{E_2^1}$
$K_{E_1^4}$ Key for 15 fps

Figure 5. Key derivation to control access to the content shown in Fig. 3. All users who are allowed to access video with any frame rates can access sound medium. Users who are allowed to access video with 60 fps or 120 fps can view text data. A solid arrow is an ordinary hash function and a dashed arrow is a modified hash function.

Firstly in the proposed scheme, keys $K_{E_1^{d_1}}$ are derived from K_C as

$$K_{E_1^{d_1}} = H^{d_1}\left(K_C\right), \quad d_1 = 1, 2, \ldots, D_1, \tag{8}$$

where $H(\cdot)$ is a cryptographic one-way hash function. Eq. (8) represents an ordinary hash chain [9], and the chain is shown with solid arrows in Fig. 5.

Meanwhile, keys $K_{E_2^1}$ and $K_{E_3^1}$ are derived by modified hash chains in the proposed scheme. In this example, these keys are given as

$$K_{E_2^1} = H\left(f\left(K_{E_1^4}, H\left(K_{E_1^4}\right)\right)\right), \tag{9}$$

$$K_{E_3^1} = H\left(f\left(K_{E_1^2}, H\left(K_{E_1^2}\right)\right)\right), \tag{10}$$

respectively, where $f(\cdot)$ is an function with two input and one output in which the length of inputs and output are identical. A bitwise exclusive or operation is a simple example of function $f(\cdot)$. As shown in Eqs. (9) and (10) which represent modified hash chains introduced in this paper, keys given by Eq. (8) are repeatedly used to derive other hash chains that are different from the ordinary hash chains. The modified hash chains are shown with combination of solid and dashed arrows in Fig. 5.

Each entity $E_m^{d_m}$ is encrypted using each corresponding key $K_{E_m^{d_m}}$, and encrypted content C is opened to public.

B. Delivered Key for Each User and Decryption

1) User allowed to access video, sound, and text: A user permitted to decode frames at 120 or 60 fps receives $K_{E_1^1}$ or $K_{E_1^2}$ shown in Figs. 6 (a) and (b). Eq. (8) is same as,

$$K_{E_1^{d_1}} = H\left(K_{E_1^{d_1-1}}\right), \quad d_1 = 1, 2, \ldots, D_1. \tag{11}$$

The user can obtain $K_{E_1^{d_1}}$ $(d_1 = 1, 2, 3, 4)$ using an ordinary hash chain in Eq. (11).

As shown in Fig. 5, keys $K_{E_2^1}$ and $K_{E_3^1}$ for sound E_2^1 and text E_3^1 are generated from $K_{E_1^4}$ and $K_{E_1^2}$, respectively, using modified hash chains in Eqs. (9) and (10). Thus the user can also obtain $K_{E_2^1}$ and $K_{E_3^1}$ and play sound and read text in addition to watch the video.

2) User allowed to access video and sound: A user can access frames decoded at 30 or 15 fps receives $K_{E_1^3}$ or $K_{E_1^4}$ as shown in Figs. 6 (c) and (d). The user has $K_{E_1^4}$ but does not have $K_{E_1^2}$. Thus the user can obtain only $K_{E_2^1}$ for sound E_2^1 by Eq. (9) and play sound as well as the video.

3) User allowed to access sound: A user allowed to access only sound E_2^1 receives $K_{E_2^1}$ as shown in Fig. 6 (e). $K_{E_2^1}$ is a key generated by Eq. (9). Any keys cannot be generated from $K_{E_2^1}$.

4) User allowed to access text: A user allowed to access only text E_3^1 receives $K_{E_3^1}$ as shown in Fig. 6 (f). $K_{E_3^1}$ is a key generated by Eq. (10). $K_{E_3^1}$ can generate no other key.

Table I
COMPARISONS IN TERMS OF THE NUMBER OF MANAGED AND DELIVERED KEYS, DELIVERY OF MANAGED KEYS, AND COLLUSION ATTACK RESILIENCE.

	Proposed	Conventional [11]
The number of managed keys	1	M
The number of delivered keys	1	M
Delivery of managed keys	No	Yes
Collusion attack resilience	Yes	No

C. Features

Two main features of the proposed scheme are briefly summarized here.

By introducing modified hash chains, the proposed scheme reduces both the managed and delivered keys to one. In contrast, the conventional scheme [11] manages and delivers keys as many as media.

By using modified hash chains, multiple media are related to prevent malicious users to collude. The conventional scheme is collusion attack-vulnerable, because the conventional scheme encrypts each medium separately.

In addition to the above features, the single managed key is not delivered to any users in the proposed scheme while the conventional scheme delivered the managed keys to some users.

It is noted that any arbitrary function and key combination can be used for a modified hash chain and that any arbitrary key assign can be used to properly control access to the content.

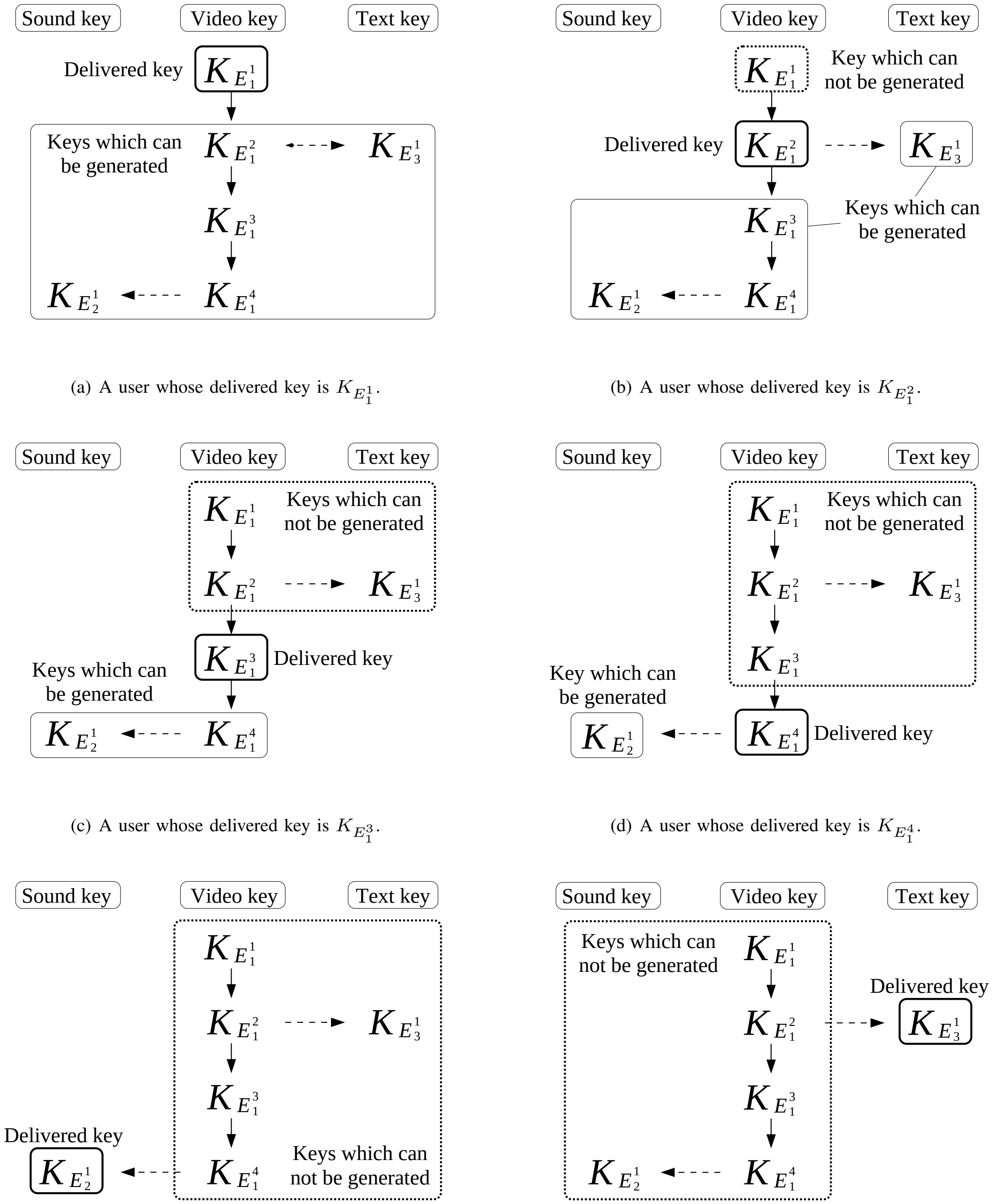
IV. Evaluation

The proposed scheme is evaluated by comparing with the conventional scheme [11] which uses ordinary hash chains [9] only. Evaluation is given in terms of the number of managed and delivered keys, delivery of managed keys, and collusion attack resilience.

Table I shows the results of comparisons. The proposed scheme manages and delivers only a single key regardless of the number of media and the depth of the hierarchical structure in a medium, whilst the conventional scheme [11] must manage and deliver keys as many as media. The single managed key is not delivered to any user in the proposed scheme, whereas the managed keys are delivered to some users in the conventional scheme [11]. In addition, the proposed scheme is resilient to collusion attacks while the conventional scheme [11] is naive for collusion attacks. The table brings out the effectiveness of the proposed scheme.

V. Conclusion

This paper has proposed a new access control scheme for multimedia content in which modified hash chains are employed. The proposed scheme manages only a single key. This scheme also delivers only a single key to a user regardless of which portions of the content to which the user can access. In the proposed scheme, the single managed


Sound key
Video key
Text key
Delivered key
Keys which can be generated
Key which can not be generated
Keys which can not be generated
Key which can be generated
$K_{E_1^1}$
$K_{E_1^2}$
$K_{E_1^3}$
$K_{E_1^4}$
$K_{E_2^1}$
$K_{E_3^1}$

(a) A user whose delivered key is $K_{E_1^1}$.

(b) A user whose delivered key is $K_{E_1^2}$.

(c) A user whose delivered key is $K_{E_1^3}$.

(d) A user whose delivered key is $K_{E_1^4}$.

(e) A user whose delivered key is $K_{E_2^1}$.

(f) A user whose delivered key is $K_{E_3^1}$.

Figure 6. A delivered key and decryption keys for each user.

key is not delivered to any user. Furthermore, the proposed scheme prevents malicious users to collude for accessing much more portions. Comparison result summarizes the effectiveness of the proposed scheme. The proposed scheme thus controls access to mulimedia content securely and simply in comparison to the conventional scheme.

Applying the proposed scheme to content in which each medium has its own hierarchical structure is a further work. Moreover, we would like to apply the proposed scheme to other security technologies such as digital watermarking and secret sharing.

REFERENCES

[1] B. B. Zhu, M. D. Swanson, and S. Li, “Encryption and authentication for scalable multimedia: current state of the art and challenges,” in *Proc. SPIE*, vol.5601, pp. 157–170, 2004.

[2] 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.

[3] Y. Wu, D. Ma, and R.H. Deng, “Progressive protection of JPEG 2000 codestreams,” in *Proc. IEEE ICIP*, pp. 3447–3450, 2004.

[4] Y. G. Won, T. M. Bae. and Y. M. Ro, “Scalable protection and access control in full scalable video coding,” in *Proc. IEEE IWDW*, pp. 407–421, 2006.

[5] S. Imaizumi, Y. Abe, M. Fujiyoshi, and H. Kiya, “Collusion attack-resilient hierarchical encryption of JPEG 2000 codestreams with scalable access control,” in *Proc. IEEE ICIP*, pp. II–137–II–140, 2007.

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

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

[8] *Streaming Video Profiles (FGS).* ISO/IEC 14496–2/FDAM 4, 2001.

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

[10] M. Joye and S. M. Yen, “One-way cross-trees and their applications,” in *Proc. IACR PKC*, pp. 355–358, 2002.

[11] 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.