Content Protection Scheme to Realize Edit Control Including Diversion Control and Composition Control

Tatsuya Fujimoto[1], Keiichi Iwamura[1] and Masaki Inamura[2]
[1]*Department of Electrical Engineering, Tokyo University of Science, 6-3-1Niijuku, 125-8585, Katsushika-ku, Tokyo, Japan*
[2]*School of Science and Engineering, Tokyo Denki University, Ishizaka, 350-0394, Hatoyama-machi, Saitama, Japan*

Keywords: Edit Control, Diversion Control, Composition Control, Digital Signature, Aggregate Signature.

Abstract: We have proposed a copyright protection technology suitable for editable contents, which can control the change, deletion, and addition of partial contents. In this paper, we propose a new scheme that can control the diversion of partial contents to other contents and composition of contents, in addition to control of the change, deletion, and addition of partial contents using digital signatures based on the author's intention. This scheme realizes edit control between two or more contents, and is effective with Internet contents such as consumer generated media represented by YouTube. We also evaluate the security of our proposed scheme against various attacks.

1 INTRODUCTION

With the advances in network connectivity, there has been a rapid increase in the distribution of online content. In recent years, a concept of consumer generated media (CGM) is prevalent, as per which anyone can be a content provider and can distribute contents on the Internet. YouTube (YouTube, URL) and CLIP (CLIP, URL) are typical examples of CGM-services. In CGM, the creation of secondary content is called mashup, which is a process of creating new content using existing content on the Internet. Mashup is performed frequently.

Typical conventional copyright protection technology (ARIB, 2013) provides viewing control and copy control which is not suitable for the CGM-service. This is because viewing control is meaningless for authors who have created the content, and want it to be seen widely, and copy control interferes only with the secondary usage of content. In contrast, copyright protection technology recommended for CGM-services presupposes the content editing, and can protect the author's copyright when the content is exhibited secondarily.

Previously, we proposed a copyright protection technology (Inamura et al., 2013) and (Koga et al., 2015), that divided content into partial contents, and controlled edits with respect to the change, deletion, and addition of the partial contents using digital signatures. However, the technology could not control the diversion of partial contents and the composition of contents. This means that the technology reported in (Inamura et al., 2013) and (Koga et al., 2015) considers only the edit control in a content. Therefore, the edit control between two or more contents became unrealizable, and the partial contents could be used contrary to the author's intention in other contents.

Therefore, in this paper, we extend the range of the edit control from the change, deletion, and addition of partial content to the diversion of partial contents and the composition of contents only using digital signatures. This means that our proposed scheme can ensure edit control between two or more contents.

The rest of this paper is organized as follows: In Section 2, we describe the digital signature used in this paper and the conventional edit control scheme. In Section 3, we propose a new edit control scheme for realizing diversion control and composition control between contents in addition to the edit control within a content. In Section 4, the security of our scheme are discussed. Finally, Section 5 concludes the paper.

2 RELATED WORKS

2.1 Aggregate Signature Scheme based on BLS Signature

Boneh, et al. have proposed an aggregate signature

Fujimoto, T., Iwamura, K. and Inamura, M.
Content Protection Scheme to Realize Edit Control Including Diversion Control and Composition Control.
DOI: 10.5220/0005994501160123
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 2: ICE-B*, pages 116-123
ISBN: 978-989-758-196-0

scheme (Boneh et al., 2003) based on the Boneh-Lynn-Shacham (BLS) signature (Boneh et al., 2001) using the operation on an elliptic curve and pairing. This scheme aggregates two or more different signatures for every message into one signature of steady length without relying on the number of signers.

We denote

$$L = \{u_{i\_1}, \cdots, u_{i\_t}\} \quad (1)$$

as a set of signer's group who participate in generating aggregate signature, and

$$J = \{i\_1, \cdots, i\_t\} \quad (2)$$

as a set of symbol of signer's who participate in generating aggregate signature. Then, the scheme of construction of aggregate signature is as follows:

2.1.1 Key Generation

Key Generation center calculates

$$v_i = x_i g \quad (3)$$

where g is a generator of $\mathbb{G}_1$, x_i is value of Z_p (x_i means a private key of $u_i \in L$), and v_i means a public key of u_i.

2.1.2 Signing

We denote $H: \{0,1\}^* \rightarrow \mathbb{G}_2$ is one-way hash function. m_j is a message of a signer u_j. Then, signer u_j calculates

$$h_j = H(m_j) \quad (4)$$

and set

$$\sigma_j = x_j h_j \quad (5)$$

as the own signature corresponding to m_j. After signing, we collect all signatures and calculate an aggregate signature σ.

$$\sigma = \sum \sigma_j \, (j \in J) \quad (6)$$

2.1.3 Verification

Verifier collects $m_{i\_1}, \cdots, m_{i\_t}, \sigma, g$ and the verification keys $v_j (j \in J)$. Then, verifier calculates

$$h_j = H(m_j) \quad (7)$$

from all m_j and judges whether the following is realized using pairing:

$$e(g, \sigma) = \prod e(v_j, h_j) \, (j \in J) \quad (8)$$

If the aggregate signature is created correctly, the upper equation is realized.

2.2 Edit Control

In (Inamura et al., 2013), an edit control scheme of that is responsible for the change, deletion, and addition of partial content within a single content has been proposed. This scheme extends the sanitizable signature (Miyazaki et al., 2003) which can control only deletion. In this scheme, an author divides his/her content into partial contents, sets signatures of each partial content, and aggregates those signatures to one signature for the content. Hereafter, we call the signature of partial content the edit control signature. If an author permits editing of the partial content, he/she exhibits the edit control signature. When an editor changes the partial content, the edit control signature is deleted from the aggregate signature and a new signature of the editor's partial content is added to the aggregate signature. If the author does not permit editing of the partial contents, he/she keeps the edit control signature secret. In this case, the editor cannot edit the partial content since he/she cannot change the edit control signature in the aggregate signature.

In (Inamura et al., 2013), edit control for the change, deletion, and addition is realized by three kinds of signatures, namely change control signature, deletion control signature and addition control signature, respectively. The operation of deletion is performed by actually deleting the partial content. Therefore, when edit is performed repeatedly, the composition of content may change and control may become impossible. Therefore, the technique reported in (Inamura et al., 2013) targets only one-time edit, and can control the edit only in one content as mentioned before.

The scheme proposed in (Koga et al., 2015) simultaneously realizes edit control and right succession and. The right succession shows the hierarchical relation between authors. However, it cannot also control the diversion of partial contents to other contents and the composition of contents. Therefore, this scheme has the same drawback as (Inamura et al., 2013) with respect to edit control.

3 OUR PROPOSED SCHEME

3.1 Entity

Since our scheme treats two or more contents produced by two or more authors, we introduce the i-th author without using the word "editor." Therefore, we define two entities called the i-th author and a verifier, as follows.

3.1.1 The I-Th Author

He/she is concerned with a work, can set up edit control signatures to the partial contents, and update the aggregate signatures. For simplicity, we express the work using a tree structure, as shown in Figure 1. We refer to the author who is in the deepest portion of the tree as the 1-st author, and the author who is in the portion of the tree route as the n-th author, when the tree height is n-1. When an original content of an author is used by the i-th author, he/she is called the (i-1)-th author. Therefore, i is defined as the position in the work. The i-th author can set the edit control signature to the partial contents that he/she has produced or edited, only when edit is permitted by the edit control signatures defined by the (i-1)-th authors. In Figure 1, A_{11} to A_{16} are the primary contents made by two or more 1-st authors, and the 2-nd authors create the secondary contents A_{21} and A_{22} using the primary contents of 1-st authors. Finally, the 3-rd author produces the final content A_{31}. Here, the 2-nd authors can edit according to the setting of the edit control signature by each 1-st author, and the 3-rd author follows the setting of the entire edit control signature by the 1-st and 2-nd authors. The author of A_{23} with the original content is called the 2-nd author, because it is utilized by the 3-rd author.

3.1.2 Verifier

The verifier verifies whether a given content has a valid signature. If this function is available in a reproduction machine, we can construct a system such that the content cannot be reproduced if it does not have a valid signature.

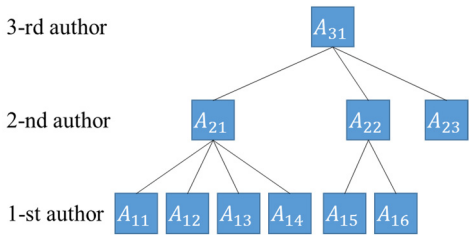

Figure 1: Examples of entities in a work with the tree structure.

3.2 Contents and Partial Contents

In our proposed scheme, the partial contents consist of two kinds of data: empty data and real data. The empty data are placed on the portion, that is due to be added or eliminated, and the real data constitutes the displayed contents. The empty data are treated as control data for controlling addition and deletion, and control data are not carried as contents displayed.

An author produces one or more partial contents and makes it available to the public as a form. Content comprises start data, one or more partial contents, and last data. The start data and the last data are the control data. Each data is identified by an identifier.

Each author has an author ID, each content has a content ID, and each partial content has a partial content ID. For example, A_{11} in Figure 1 is a content made by author ID_{11}. Its content ID is IC_{11}. If it is assumed that A_{11} is composed of m partial contents A_{111}～A_{11m}, A_{11} has the start data before A_{111} as A_{110} and the last data after A_{11m} as A_{11m+1}. We set I_{110}～I_{11m+1} as the partial content ID of A_{110}～A_{11m+1}. Among A_{111}～A_{11m}, empty data are set to the portion, that can be added or the deleted portion of partial contents.

We call the author ID of a partial content aID, and each partial content is linked to its corresponding aID. This link is guaranteed for the trusted content administration center (CAC) to sign to linked data (the hash value of the connection with the partial contents and aID). The reproduction machine eliminates the contents with the partial contents, which do not have a valid signature certified by CAC, and are treated as invalid content. The CAC signs only when it accepts a partial content as the original content. We call this signature the administration signature.

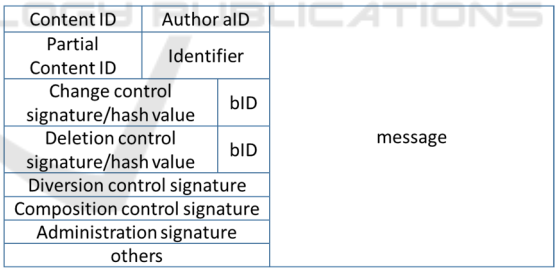

Figure 2: Example of structure of partial content.

A partial content is linked in the header to various parameters required for verification. These include content ID, author ID (= aID), partial content ID, identifier of data, change control signature and deletion control signature or hash values for the signatures, bID, which is the author ID for an author who specified that no edit is permitted, diversion control signature, composite control signature, administration signature, and others, as shown in Figure 2. In Figure 2, the message expresses the content of partial content. These parameters can be overwritten and changed. However, if an attacker changes these data maliciously, the equation by

pairing does not realize in the algorithm shown in 3.6. Thus, we can detect illegal edit.

Our scheme detects edit contrary to an author's intention, but does not prevent legitimate content from becoming unjust content by violating processing such as overwrites or changes in the parameters. Since edit of contents is performed to just copied contents, the original contents are not influenced by violation processing. Therefore, even if an attacker performs violation processing, the attacker gains no merit by changing only the edited contents to unjust contents.

3.3 Edit Control in One Contents

We set the following two types of signature to control the change, deletion, and addition of partial content: change control signature and deletion control signature. Addition control is realized by change control as the addition of content is performed by changing empty data to real data. Deletion refers to changing real data to empty data. However, the deletion needs to be controlled independent of change. For example, contents of a fixed form such as a four-frame cartoon allow each frame to be changed but does not allow the deletion of frames to prevent breaks in the fixed form. More specifically, in a movie credit title deletion is allowed but change is not. Each signature is exhibited when permitting the edit, and when editing is not allowed, the signature is kept secret and the hash value used for the signature and bID are exhibited as shown in Figure.2.

If the change of empty data is allowed, then the empty data can be changed to real data. If the change of empty data is not allowed, then the deletion of the partial contents is considered as fixed. On the other hand, the deletion control to empty data is meaningless as the deletion of empty data replaces empty data. Therefore, we set empty data allows either change and deletion to be permitted or change and deletion to be prohibited.

An aggregate signature is generated for each change control signature and deletion control signature. Each aggregate signature is composed of a start signature, the group of edit control signatures of partial contents, and a last signature. The public cannot open or view the start signature and the last signature. The aggregate signatures are linked to the contents and opened to the public. We treat the content published without the aggregate signature as unauthorized content.

Figure 3 shows the four states that are used to control partial content. State {11} allows the change and deletion of partial content. State {10} allows change, but deletion is not allowed. State {01} does not allow change, but allows deletion. State {00} allows neither change nor deletion. In Figure 3, P means partial content including real data and empty data, R means real data, and E means empty data. Figure 3 shows the transition states between each state of the partial content

The proposed scheme achieves continuous edit, which cannot be realized in (Inamura et al., 2013), since the four state transitions are controlled according to each edit control signature and the form of the contents does not change.

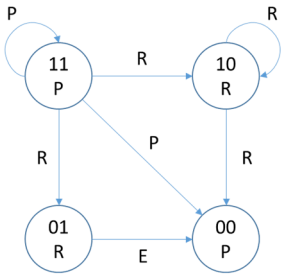

Figure 3: Control state transition of the partial contents.

3.4 Diversion Control of Partial Contents

When the change and deletion of the partial content is permitted, it can be used in other contents using each edit control signature. To control the diversion of partial contents, we introduce a diversion control signature. The diversion control signature is opened to the public only when allowing diversion of the partial contents.

Basically, content has only one content ID, therefore the diversion control signatures of each partial content includes the same content ID. We can detect diversion only by examining the consistency of the content ID. However, when content has many partial contents with different content ID, we must identify the original content ID. To identify the original content ID, the primary author who creates the content sets specific values, such as 0, as the content ID of the partial content which permits diversion. Therefore, a content consists of the original partial contents with the original content ID, which do not allow divert, and the partial contents with a specific value as content ID, which allow diversion or are diverted.

The diversion control signature is always verified by the key of aID. Therefore, only the author of aID can set up the diversion control signature and the author who diverts the partial contents cannot change the signature, unlike the edit control signatures

mentioned in section 3.3. On the other hand, the edit control of the diverted partial contents is possible as mentioned in the previous session, since each edit control signature is processed independently. However, when a partial content does not be allowed the change and/or deletion, the edit control signatures need to be recreated by the author who diverts. In addition, a partial content, which is changed or added as new partial content, is necessary to be set the content ID of the diverted content in the signature to match the contents ID.

3.5 Composition Control of Contents

The content composition is to line up some contents in a specific order and compose them as one content. We refer to the contents generated by the composition processing as the composite content. A composite content has structural data as a control data which describes the composition of contents in addition to the contents group that comprises the composite contents.

We introduce the composition control signature to all of the partial contents, and generate the aggregate signature. All the composition control signatures in a content are opened to the public only when allowing composition of the contents.

In cases where the composition of both content A and content B were permitted, both the contents are compounded, and we can prohibit the compounding of any other contents between content A and content B. In this case, at least one of the partial contents of each A and B must be edited, the composition control signatures are exchanged, and the composition, change and deletion control signatures of the partial contents must be hidden, to avoid reuse of the edit control signatures. The edit of partial contents in the composite contents can be done as mentioned in section 3.3, since each control signature is set independently. However, the composition control signature is recreated when the partial content is edited.

On the other hand, it is necessary to change only the structural data, if the author compounds the contents without making them compoundable to uncompoundable. In this case, authors can be freely re-compounded. However, it does not infringe the primary author's intention to allow composition.

3.6 Algorithm

In this section, we explain the concrete algorithm of the proposed scheme. In this algorithm, it is assumed that the binding between the signers and the verification keys is guaranteed by a Certification Authority, and information that is being prepared is not obtained by a third party.

3.6.1 Key Generation

ID_{ij} is the author ID defined according to the location of a work. ID_{ij} has a private key s_{ij} to sign and exhibits verification key

$$v_{ij} = s_{ij}g \tag{9}$$

to it. All of the signing keys differ.

3.6.2 Signing

The author always performs the signature generation process before publishing the original content that has obtained an administration signature. The definition of each ID is as shown in section 3.2. To prevent duplication, the content ID of each content is different, and the author can be identified from the content ID (here, the first half of IC_{ij} is equal to ID_{ij}). We refer to the main contents of a partial content with the exception of header, message as shown in Figure 2.

(1) Author ID_{ij} determines the control permissions of change, deletion, addition and diversion for each partial content and the composition for the content. For empty data, only {00} and {11} are permitted for change and deletion. Author ID_{ij} determines the content ID, where IC_{ij} is set to zero for partial contents that are allowed to be diverted.

(2) Author ID_{ij} makes the start data A_{ij0}* and the last data A_{ijm+1}*. Here, d is the message of control data. Then, author ID_{ij} generates the start signature α_{ij} and the last signature β_{ij}, Here, each start and last signature is different for every edit as r is a different constant. The constant r varies according to the edit with respect to change, deletion, diversion and composition.

$$A_{ij0}{}^{*} = IC_{ij} \parallel I_{ij0} \parallel d \tag{10}$$

$$A_{ijm+1}{}^{*} = IC_{ij} \parallel I_{ijm+1} \parallel d \tag{11}$$

$$\alpha_{ij} = s_{ij}H\left(IC_{ij} \parallel I_{ij0} \parallel H\left(A_{ij0}{}^{*}\right) \parallel r\right) \tag{12}$$

$$\beta_{ij} = s_{ij}H\left(IC_{ij} \parallel I_{ijm+1} \parallel H\left(A_{ijm+1}{}^{*}\right) \parallel r\right) \tag{13}$$

(3) Author ID_{ij} makes data A_{ijk}* for the message of each partial content A_{ijk} (the message of empty data is d), where

$$A_{ijk}{}^{*} = IC_{ij} \parallel I_{ijk} \parallel A_{ijk} \tag{14}$$

(4) Author ID_{ij} uses p and r properly according to the edit and permission, and generates a hash value for each edit. Here, p=1 when an edit is allowed, and p=0 when no edit is allowed.

$$h_{ijk} = H\left(IC_{ij} \parallel I_{ijk} \parallel H\left(A_{ijk}{}^{*}\right) \parallel p \parallel r\right) \tag{15}$$

(5) Author ID_{ij} makes each edit control signature for each of the partial contents as follows (h_{ijk} differs in every edit):

Change control signature:

$$\sigma_{ijk} = s_{ij} h_{ijk} \tag{16}$$

Deletion control signature:

$$\tau_{ijk} = s_{ij} h_{ijk} \tag{17}$$

Diversion control signature:

$$\chi_{ijk} = s_{ij} h_{ijk} \tag{18}$$

Composition control signature:

$$\delta_{ijk} = s_{ij} h_{ijk} \tag{19}$$

(6) Author ID_{ij} makes each aggregate signature (α_{ij}, β_{ij} differs in every edit) as follows:
Change aggregate signature:

$$\sigma_{ij} = \alpha_{ij} + \sum \sigma_{ijk} + \beta_{ij} \tag{20}$$

Deletion aggregate signature:

$$\tau_{ij} = \alpha_{ij} + \sum \tau_{ijk} + \beta_{ij} \tag{21}$$

Diversion aggregate signature:

$$\chi_{ij} = \alpha_{ij} + \sum \chi_{ijk} + \beta_{ij} \tag{22}$$

Composition aggregate signature:

$$\delta_{ij} = \alpha_{ij} + \sum \delta_{ijk} + \beta_{ij} \tag{23}$$

(7) A partial content attaches parameters required for signature verification, as shown in Figure 2. Here, it attaches edit control signatures if it permits an edit, and it attaches hash values in Step(4), and bID=aID if editing is not allowed. The aggregate signatures are attached to the contents.

3.6.3 Edit

Let us consider the case where Author ID_{ab} changes the partial content A_{ijk} in the content A_{ij} which is created by Author ID_{ij} to A_{abk}, which he/she created, and deletes, adds, and diverts the partial content A_{ijk}.

(1) Author ID_{ab} confirms whether editing of contents A_{ij} is allowed by signature verification. If it is not allowed, the edit is stopped.

(2) When a diversion is permitted, author ID_{ab} can divert the partial content.

(3) When a change, deletion or addition is permitted, author ID_{ab} can substitute A_{ijk} to A_{abk}, and decide the edit permission of A_{abk} according to Figure 3. Here, A_{ijk} is a real data in change and deletion, and A_{ijk} is an empty data in addition. A_{ab} is a real data in change and addition, and A_{ab} is an empty data in deletion.

(4) Author ID_{ab} generates the data A_{abk}* and the hash value to the substituted partial contents according to the edit (r differs in every edit). IC_{ij} is not changed when diversion is not permitted, but when diversion is permitted, IC_{ij} is set to 0.

$$A'_{abk}{}^{*} = IC_{ij} \parallel I_{ijk} \parallel A'_{abk} \tag{24}$$

$$h'_{abk} = H\left(IC_{ij} \parallel I_{ijk} \parallel H(A_{abk}{}^{*}) \parallel p \parallel r\right) \tag{25}$$

(5) Author ID_{ab} generates edit control signatures $\sigma_{abk}, \tau_{abk}, \chi_{abk}$ and δ_{abk} of A_{abk} as same as Step(5) during Signing process.

(6) Author ID_{ab} updates each aggregate signature as follows.
Change aggregate signature:

$$\sigma_{ij} = \sigma_{ij} - \sigma_{ijk} + \sigma_{abk} \tag{26}$$

Deletion aggregate signature:

$$\tau_{ij} = \tau_{ij} - \tau_{ijk} + \tau_{abk} \tag{27}$$

Diversion aggregate signature:

$$\chi_{ij} = \chi_{ij} - \chi_{ijk} + \chi_{abk} \tag{28}$$

Composition aggregate signature:

$$\delta_{ij} = \delta_{ij} - \delta_{ijk} + \delta_{abk} \tag{29}$$

(7) The edited partial content includes parameters required for signature verification as shown in Figure 2.

3.6.4 Composition

Edit and composition can be repeated arbitrarily.

(1) When Author $ID_{i+1,j}$ composes content A_{ia} and content A_{ib}, he/she verifies whether the composition of A_{ia} and A_{ib} is allowed.

(2) If the composition is allowed, he/she marks the composition order of A_{ia} and A_{ib} in the structural data.

(3) If Author $ID_{i+1,j}$ fixes the relation of A_{ia} and A_{ib}, he/she recreates the aggregate signatures of A_{ia} and A_{ib} as follows. However, a partial content in both A_{ia} and A_{ib} needs the edit and hiding of the composition, change and deletion control signatures. Here, $\delta_{iat}, \delta_{ibq}$ and $\delta'_{iat}, \delta'_{ibq}$ are the signature of the partial content before and after the edit, respectively.

$$\delta_{ia} = \delta_{ia} - \delta_{iat} + \delta'_{ibt} + \delta'_{ibq} \tag{30}$$

$$\delta_{ib} = \delta_{ib} - \delta_{ibq} + \delta'_{ibq} + \delta'_{iat} \tag{31}$$

3.6.5 Verification

p=0 when each edit control signature is hidden, and p=1 when each edit control signature is visible.

(1) The administration signature of the entire partial content is verified.

(2) If the entire administration signature is valid, the verifier decomposes the composite content into specific contents using structural data. The following processing is performed for each content.

(3) The verifier verifies whether the partial contents of each content have proper content ID. The content IDs are unified except for specific contents ID such as 0.

(4) If the above verification does not fail, the verifier checks the correctness of the composition aggregate signature as follows. In the case where the composition is fixed, h_{ijk} includes the hash value of the edited partial content of other contents and v_{ij} is the verification key of aID of the partial contents. The start and last signatures are verified using the key of the author decided from content ID.

$$e(g, \delta_{ij}) = \prod \prod e(v_{ij}, h_{ijk}) \quad (32)$$

(5) If the content is proper in composition, the verifier checks if each content is proper in diversion using the key of aID as follows:

$$e(g, \chi_{ij}) = \prod \prod e(v_{ij}, h_{ijk}) \quad (33)$$

(6) If the content is proper in diversion, the verifier checks if the content is proper in the edit about change, deletion, and addition. First, he/she checks if the empty data has the permission {00} or {11} with respect to change and deletion. Next, the verifier generates the hash value of each partial content for each edit. If the real data does not have a change control signature, the verifier checks by matching the generated hash value and the attached hash value for change. If an empty data does not have a change control signature, the verifier checks by matching the generated hash value and the attached hash value for deletion. The verifier prepares the key of aID and the generated hash value for each partial content with the signature, and the key of bID and the attached hash value for each partial contents with no signature. He/she verifies the following equations for change and deletion. If all checks are proper, the content is accepted as being valid.

$$e(g, \sigma_{ij}) = \prod \prod e(v_{ij}, h_{ijk}) \quad (34)$$

$$e(g, \tau_{ij}) = \prod \prod e(v_{ij}, h_{ijk}) \quad (35)$$

4 SECURITY ANALYSIS AND PRACTICALITY

The practicality of our scheme is guaranteed by the trusted CAC and trusted verifying machine. If the CAC and verifying machine are trusted, the security of our scheme can be shown as follows:

Our proposal is not of a new signature scheme. The security of the signature used in our proposed scheme is based on the security of the aggregate signature using the BLS signature shown in 2.1.

Our proposal is the edit control scheme using the above-mentioned signature. Namely, the security of our scheme is determined by whether a violation of the edit is detectable by our scheme. Therefore, under the premise that the signature scheme is secure and forgery of the signature is impossible, we consider the security of our scheme against following attacks.

(1) An attack that falsifies the author of partial content

The author of partial content is guaranteed by the administration signature from the CAC. CAC generates the signature only if it accepts the original content. The originality of the partial content is given by another means. For example, image similarity searches for a still image. Even if an attacker claims that the author of a partial content is himself, when the partial content does not have an administration signature including his ID and the hash value of the partial content, he is not accepted as author of the partial content. Therefore, in the proposed scheme the attacker cannot falsify the author of the partial content, if the CAC is trusted. CAC and the administration signature are not proposed in (Inamura et al., 2013) and (Koga et al., 2015). In other words, (Inamura et al., 2013) and (Koga et al., 2015) have the premise that the key for every partial content has is known for some means. This paper shows the means and the structure of partial content required to verify concretely.

(2) An attack that fakes the content ID of contents

The diversion control signature of partial content for which diversion is not permitted includes the content ID of the content. If the partial contents allow change or deletion, the attacker can change or delete them, add new partial contents with a different content ID, and make different content with an aggregate signature corresponding to the new content ID. However, it is not violation processing, since it is equivalent to having created different contents combining new partial contents and the partial contents that allow diversion. On the other hand, if there remains partial content that does not permit diversion to another content, the new partial contents that are changed or added must be set the same content ID or special content ID for diversion in the signature. Therefore, the attacker cannot fake the content ID of content with partial content with no permission of diversion.

(3) An attack that divert partial contents with no permission on diversion

Since the diversion control signature is inspected with the verification key of aID which is the author ID of the partial content guaranteed by the administration signature, the attacker cannot be changed into a signature that can be diverted. (2) and (3) realize diversion control unrealizable in (Inamura et al., 2013) and (Koga et al., 2015).

(4) An attack that improperly changes real data1 into real data2

During the verification of change, malicious edit is detected by the consistency of the hash value of the real data2 and that of real data1 attached in the partial contents. In the case where the attached hash value of real data1 is rewritten to that of real data2, malicious change is detected by signature verification of change.

(5) An attack that improperly deletes real data1.

During the verification for deletion, malicious edit is detected by the consistency of the hash value of the empty data and that of real data1 attached in the partial contents. In the case where the attached hash value of real data1 is rewritten to that of the empty data, malicious deletion is detected by signature verification for deletion.

(6) An attack that improper changes real data1 into empty data.

In attack (4), if real data1 is used as empty data, malicious change will be detected for the same reason. The measures against attacks (4)(5)(6) and state control according to Figure 3 realize repeated change, deletion, and addition control, which unrealizable in (Inamura et al., 2013) and (Koga et al., 2015).

(7) An attack that changes the hidden edit control signature of one partial content in a content

Even if a content has only one partial content that hides the edit control signature, the edit control signature cannot be specified since the aggregate signature has the hidden start and last signatures. However, in the case where only one partial content is changed to a new partial content, the edit control signature of new partial content can be determined from the difference in equation (26)-(29) in (Inamura et al., 2013) and (Koga et al., 2015), since they assume the simultaneous edit of two or more partial contents. In our scheme, the hidden edit control signature is set to p=0. The signature with p=1 can be generated by only the author of the partial content. Therefore, the attacker cannot change the signature even if the hidden signature is known from the edit of only one partial content.

(8) An attack that compounds uncompoundable contents

Uncompoundable content includes an unknown hidden composition control signature. Therefore, the attacker cannot change the aggregate signature. (8) realizes composition control that is unrealizable in (Inamura et al., 2013) and (Koga et al., 2015).

5 CONCLUSIONS

In this paper, we propose an improved content protection scheme. Our new scheme can control edit such as diversion of partial contents to other contents, and it can also control the composition of contents. In other words, our proposed scheme enables the control of not only the edit in one content but the edit between two or more contents. In addition, we solve the problem about a repetition of edits on change, deletion, and addition which remains a problem in the conventional scheme. This scheme is a next generation content protection scheme suitable for CGM on the Internet.

In future, we aim to apply signatures using Identity-Based Encryption [13] in our scheme.

REFERENCES

YouTube, https://www.youtube.com/ (URL).

CLIP, http://www. clip-studio.com/clip.site/ (URL).

Association of Radio Industries and Businesses (2013). Conditional Access System Specifications For Digital Broadcasting (*ARIB STD-B25 ver6.0., 3rd ed*). Association of Radio Industries and Businesses, Tokyo.

Inamura, M., Saito, A., and Iwamura, K. (2013). A Pre-Control System to Edit Contents with an Extended Sanitizable Signature *IEEE Information and Systems Society. Japan*, 133(4), pp.802-815.

Boneh, D., Lynn, B., and Shacham, H. (2001). Short Signatures from the Weil Pairing. Advances in *Cryptology–ASIACRYPT 2001, LNCS2248*, pp.514–532, Springer.

Boneh, D., Gentry, C., Lynn, B., and Shacham, h., (2003). Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. *Advances in Cryptology–EUROCRYPT2003, LNCS2656*, pp.416–432, Springer.

Miyazaki, K., Susaki, S., Iwamura, M., Matsumoto, T., Sasaki, R., and Yoshiura, H., (2003). Digital Document Sanitizing Problem. *ISEC, 103(195),* pp.61-67.

Koga, K., Inamura, M., Kaneda, K., and Iwamura, K., (2015). Content Control Scheme to Realize Right Succession and Edit Control. *12th International Joint Conference on e-Business and Telecommunications (ICE-B2015)*, pp.249-257, Colmar.